State regulation of the IoT in the Russian Federation: Fundamentals and challenges

Zharova Anna[1], Elin Vladimir[2]
[1,2]High School of Economics, Russia
[1,2]The Institute of State and Law of the Russian Academy of Sciences, Russia

Article Info

Article history:

Received Sep 27, 2020
Revised Dec 19, 2020
Accepted Jan 13, 2021

Keywords:

Cyber-physical systems
Infrastructure systems
Protecting
Security
Standards

ABSTRACT

The purpose of this section is to study the problems with implementing technical and legal regulations for the development of public administration functions in the Russian Federation when using the internet of things (IoT). The introduction is based on an analysis of regulatory legal acts and presents the main strategic directions for the development of public administration functions in the Russian federation when using IoT. State reports, scientific literature, a system of technical and legal regulation are analyzed, and the main problems of implementing the IoT that impede the achievement of effective public administration are studied. The Russian practice of using IoT in various economic areas is investigated. Based on an analysis of the mechanisms for ensuring data safety of information technology users in the Russian federation, problems were investigated, such as the collecting data through IoT, including publicly available personal data in order to profile human activities, and creating of a digital twin of a person. The social constraints for introducing distributed registry technologies are users' distrust in the field of data privacy protection and mathematical algorithms that are used to establish trust in a digital environment instead of trusted centralized intermediaries; these problems were also analyzed. The Russian approach was analyzed in comparison to European experience in this field. To ensure information security and the possibility of its distribution, the IoT is revealed.

Corresponding Author:

Zharova Anna
Department of Information Law and International Information Security
The Institute of State and Law of the Russian Academy of Sciences
10 Znamenka st., Moscow, 119019, Russia
Phone: +7 (495) 691 3381
Fax: +7 (495) 691 85747
E-mail: anna_jarova@mail.ru

1. INTRODUCTION

In Russia, the use of the Internet of things (IoT) is typical for many sectors of the economy. Despite the fact that IoT technologies are still being tested, a commercially attractive number of IoT devices will appear on the market by 2023-2025. However, some devices for pilot projects were available as early as 2020.

Testing IoT technologies is carried out in the sphere, which includes cars with varying degrees of automation (in the future, autonomous cars), in medicine, logistics, and the entertainment industry based on augmented reality, as well as in certain types of state supervision [1], including in profiling human activities [2]. In Russia, as in the world, IoT is used to create a smart home and smart energy [3]. The development of this economic industry was confirmed by contracts concluded between IT leaders. For example, in 2018, mobile communication companies Megafon and MTS came to an agreement with Nokia to jointly test 5G networks in Russia [4].

The massive use of information technology to solve problems at the household and government levels pose challenges for developing a system of legal and technical regulation that reduces barriers to the use of these technologies, information security of information technologies, protecting privacy, compatibility, and protecting competition. Scientists believe that the use of new technologies will create serious problems and new risks to public safety and national security since they have a dual purpose and are inherently vulnerable to exploitation [5]. Achieving this result is possible by applying an integrated approach at the level of interdisciplinary knowledge. This requires, on the one hand, the joint work of state bodies, international and national organizations, and commercial structures. On the other hand, it is necessary to form a system of views on the complex problems regarding IoT security [6].

The digitalization of the economy and public administration requires a definition of a strategy for the creation and use of information technology, including introducing the IoT as a technology in which the state and business are interested. The Government of the Russian Federation defines as the main activity the need for “the formation and maintenance of state information resources, the definition of rules for the systematization of information in these resources, as well as the harmonization of information between various information resources of authorities” [7].

Between 2017 and 2019, a number of legal documents have been developed that introduced the IoT in the Russian federation [1], [8], [9]. By 2020, the structure of the Russian information technology market has increased the hardware and services market while reducing the software market [10].

Currently, the Russian federation is actively implementing and using the IoT in various areas of economic activity, which allows them to qualitatively strengthen the forecasting capabilities in various fields and to improve the quality of the services provided in the information sphere. Last year, the Government of the Russian Federation launched an experiment to create a digital profile of the infrastructure based on the unified identification and authentication system federal state information system. Since July 1, 2020, an experiment has been conducted to establish special regulations for implementing artificial intelligence technologies in Moscow.

One of the problems in the development of the Russian data market is the lack of clear legal regulation for the interaction of participants in this market. This paper presents an analysis of the threats and risks of the IoT, analyzes the regulatory and technical regulation of the IoT, a number of organizational and legal aspects of ensuring the security of the IoT was revealed. The problems that impede the creation of an effective system for regulating the Russian IoT market were analyzed.

This paper presents an analysis of the threats and risks of the IoT, analyzes the regulatory and technical regulation of the IoT, a number of organizational and legal aspects of ensuring the security of the IoT was revealed. The problems that impede the creation of an effective system for regulating the Russian IoT market were analyzed..

2. RESEARCH METHOD

This research is based on a number of research methods-general scientific methods: deduction and induction and special research methods (comparative research, complex legal regulation, tabular method, and other methods of theoretical research). The use of these research methods seems to the authors to be the most justified for understanding both the objective laws of the field of research and the directions for further use of the results in practice. These methods are widely used when it is necessary to conduct a complex of interdisciplinary research [11].

The transition from general to specific in the process of reasoning allowed the authors to reveal the features of technological solutions used in the IoT. The analysis of the above definitions of IoT led the authors to the conclusion that information is involved in a continuous cycle of reception and transmission, decision making, and interaction of devices in the Internet of things. Accordingly, this allowed the authors to describe the technological methods of information protection.

The IoT reference model made it possible to represent the "points" of the organizational and legal impact that require information security. International standards ISO 27000 and ISO-13335 and national standards of Russia were considered as instruments of technical regulation. An analysis of the existing system of division of competences between Russian federal agencies allowed the authors to describe the area of responsibility, identify priorities, and competencies.

The induction method, which includes the movement of cognition from facts to general statements, made it possible to present the structure of IoT security objects, clusters of the basic threat model, a number of specific threats related to the functioning of embedded interconnected IoT devices. In the conclusion, the general conclusion of the study is made. ConsultantPlus, Scopus, Elsevier, SpringerLink, GoogleScholar were used to collect data and analyze the regulatory and scientific base related to data security in general and in the context of IoT.

3. TECHNOLOGICAL REGULATION: RISKS AND THREATS OF THE IOT

3.1. Different approaches to representing the IoT architecture

The features of the technological solutions used in the IoT determine the specificity of the technological solutions in IoT security. For example, it is proposed to use the splunk SIEM solution to identify and block traffic from compromised IoT devices [12]. To ensure secure aggregation of data, it is proposed to use the efficient-CSDA algorithm [13], and various methods to ensure the security of storing, receiving and transmitting data are being studied [5]-[15].

The concept of building the IoT belongs to Kevin Ashton, who in 1999 expressed the idea that comprehensively implementing RFID tags could modify the logistics chain management system. He proposed combining physical objects ("things") equipped with built-in technologies for interacting with each other or with the external environment into a single computer network (served by Internet protocols). There are currently a number of IoT definitions. For example, the European Union Agency for Cybersecurity ENISA defines IoT as "a cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision making" [14].

Stemming from the definition is the fact that information lies at the heart of IoT, feeding into a continuous cycle of sensing, decision-making, and actions. The IoT is tightly bound to cyber-physical systems and, in this respect, is an enabler of smart infrastructures (e.g., Industry 4.0, smart grid, smart transport) by enabling services of higher quality and facilitating the provision of advanced functionalities [15].

The IoT technologies are based on a set of requirements for measuring instruments that ensure the conversion of information into machine-readable data (sensors, devices, home systems, and measuring systems), means of automatic identification of objects of the physical world (RFID technologies, barcodes, data matrix, QR codes, means for determining location in real-time, and MAC address of a network adapter), and data communications using wireless and wired networks. The IoT requires the presence of basic components; their interconnection is carried out in the presence of its own IoT architecture and includes:

- The totality of the presence on the devices or systems of sensors or identification tags that allow for unique identification;
- Fully automatic execution of processes and functionality by devices or systems;
- Interaction between devices or systems through communication networks (infrared, wireless, power and low-current networks);
- The ability to transfer data in two directions over TCP/IP protocols via Internet channels without human intervention.

Of course, there are different approaches to representing the IoT architecture. For example, the National Institute of Standards and Technology (NIST) proposed dividing the IoT into five functional areas [16]: connected devices, consumer-grade IoT medical equipment, and devices used in healthcare, smart buildings, and "Smart" production (including industrial control system). The disadvantages of this approach include the need to develop standards that consider the specifics of the activity.

In this work, the reference architecture of the IoT, developed by the standardization sector of the International Telecommunication Union (ITU-T) Y.2060, details the physical components of the IoT ecosystem used. The IoT reference model is shown in Figure 1 and includes four levels (applications, service support, application support, and network devices), as well as management capabilities and security capabilities. Architecture layers must be connected, integrated, managed, and made available to applications [17]. Since Russia is a member of the ITU, the proposed IoT architecture is used by Russian developers.

3.2. Correlation of Russian and international approaches to information security of the IT sector

The problems of ensuring the safety of IoT are actively discussed in the scientific literature, various solutions are proposed. For example, ensuring safety by reducing the response time of data transfer protocols in IoT is proposed [18], [19]. To ensure the safety of IoT switching, new algorithms for optimizing things are proposed [20]. In addition to considering the threats and risks traditional for the IT sector, a number of specific problems, IoT has its own problems:

- Device management, remote activation and deactivation of devices, diagnostics, firmware and software updates, device operating state management;
- LAN topology management;
- Traffic and congestion management detection of network congestion and the implementation of resource reservation for urgent and/or vital traffic flow.

Technical regulations for the IoT has been carried out by the Institute of Electrical and Electronics Engineers (IEEE) and the International Electrotechnical Commission (IEC) since 2014 when the IEEE working group began the development of an “architectural framework for the IoT, which focused on the problem of ensuring the reliability and safety of devices. In December 2015, the Interagency Working Group International Cybersecurity Standardization for the IoT was created to describe the goals, risks and threats, and coordinate issues in the field of cybersecurity at the international level [17]. A number of international organizations (e.g., The European Union Agency for Network and information security and the industrial internet consortium) also deal with the issue of ensuring IoT security through the use of an integrated (organizational and legal) approach.

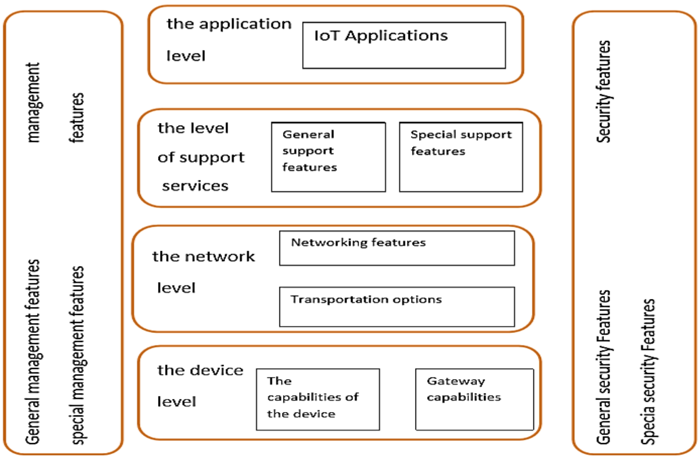

Figure 1. The IoT reference model

Russia takes part in the activities of these organizations both at the level of interstate cooperation and at the level of individual participation; Russian companies use the results from scientists in practice. To ensure information security in general, as well as to solve IoT security problems in the Russian Federation, both international standards ISO 27000 and ISO-13335, and national standards of legal and technical regulation are applied. The state standardization system of Russia allows various versions of the rules for applying international ISO standards by adopting an authentic text of an international standard as a state Russian regulatory document (GOST R) without any additions or with additions reflecting the peculiarities of Russian requirements for standardization. At the same time, the Russian federation is developing its own national standards. The relationship between international and national standards is shown in Table 1.

At the national level, IoT security is provided by the Federal Service for Technical and Export Control (FSTEC of Russia); they organize interdepartmental coordination and interaction and exercise special and control functions in the sphere of information security (applying non-cryptographic methods) in information and telecommunication infrastructure systems. The FSTEC cooperates with government agencies and companies in the field of cybersecurity and countering hacker attacks. The FSTEC created and updated a consolidated vulnerability database for information processing and transmission systems. Currently, the database contains 217 threats and more than 27 thousand vulnerabilities. These data are especially relevant for the protection of state information systems, personal data processing systems, and automated control systems for critical facilities.

The proposed threats can be divided into large clusters, as defined for the basic threat model [21]: an internal attacker, external attacker, built-in hardware bookmark, standalone hardware bookmark, software bookmark, program (e.g., a Trojan horse), software virus; Network malware (e.g., password guessing, remote access) [22]. Within the framework of the IoT, FSTEC has been identified a number of specific threats to the functioning of embedded interconnected devices: theft and use of confidential information and user credentials, ransomware and ransomware attacks, installation of unauthorized firmware, remote access and attacks via mobile devices, data interception, man-in-the-middle attacks, and exploitation of vulnerabilities in applications [22].

The most important role in ensuring wireless data transmission in the IoT is played by factors such as bandwidth resiliency, adaptability and compatibility, efficient data transmission at low speed, reconfiguration, and scalability when using and organizing a network [23]. At the same time, a number of problems have been identified for the IoT: Protection against the use of built-in backdoors and known vulnerabilities in firmware and the detection and blocking of attempts of unauthorized change of firmware.

Embedded devices must provide protection that works effectively in isolated networks without an Internet connection, with minimal impact on performance, and complies with legal and industry standards [24], [25].

Testing methods for smart devices relate to the functioning of the devices themselves, interaction with networks, and security. Testing issues go beyond the devices and sensors themselves, and other issues arise related to the processing of large amounts of data. To ensure information security, the Russian Federation since 2015 has defined a strategy for the development of its own economic industry in the development of domestic software and domestic technical standards.

FSTEC offers a set of organizational and technical measures aimed to counter threats to the IoT and ensure information security. A set of measures by the FSTEC was proposed to address information security [22]: identification and authentication of access subjects and access objects, access control of access subjects to access objects, limitation of the software environment, protection of machine media, check the security event, antivirus protection, intrusion detection (prevention), control (analysis) of data security, ensure the integrity of the information system and data, ensure the availability of data, protect the virtualization environment, protect technical means, protect the information system (i.e., its means, communication, and data transmission systems), identify incidents, and configuration management for the information s and data protection systems. Scientists and practitioners offer solutions to the above problems [10]-[18], [21], [26].

4. RUSSIA'S PARTICIPATION IN THE DEVELOPMENT OF INTERNATIONAL SOLUTIONS TO ENSURE THE SAFETY OF IOT

Currently, the scientific community is discussing the issue of conflict resolution when data analytics and confidentiality conflict with each other. It is believed that overcoming this contradiction is possible as a result of applying a wide range of methods that satisfy different degrees of confidentiality and still allow researchers to use different methods of data analysis [27]. As a practical result, one can imagine the activities of a number of Russian companies to ensure IoT security, such as: Kaspersky Lab, Entrust Datacard, Praetorian, Fujitsu, and Microsoft, in 2019, they prepared the practitioner’s guide for IoT Security maturity model [28]. This guide identifies gaps in specific configurations, products, scenarios, and technologies and prioritizes countermeasures accordingly. This practice aims at both revealing known and specific factors that may place the functioning of a given system at risk and accurately describes these factors. Practical activities to ensure the safety of the IoT in Russia is related to a number of factors and are presented in Table 1.

Table 1. IoT security directions

Security directions	Factors	Implementation method
Development of secure devices	Implementing a Safe Development Life Cycle	- Define a concept for creating secure software, threat modeling, secure coding, security testing and ensuring privacy - Consider and determine the main issues of security and confidentiality of the project, including regulatory requirements - The use of documented tools for the development, search and elimination of outdated software and analyze all the functions of the project - Inclusion of additional necessary security levels - Code verification for compliance with security and confidentiality requirements - Develop a plan for tracking security incidents and quickly respond to them
Secure Networking	Using secure cloud technologies to protect data (other than encryption)	- Protect of the Internet gateway - Perform a safe boot and check the system firmware before booting - Regular updates of cloud providers solutions - Introduce threat monitoring solutions that help detect data leaks from cloud accounts - Use a secure VPN connection to encrypt personal data from potential threats
Building a secure network	Access control to connect only authorized devices	- Set up a firewall - Store authentication keys in a safe place - Install antivirus software to ensure network security monitoring
Secure data storage	Eliminate the possibility of illegal access, distribution, blocking, destruction of information	- Flexible scanning - Flexible reporting - Warning systems - Proactive antivirus technology - An easy-to-use centralized management console

In Russia, as in a number of other countries, a public-private partnership (PPP) can act as a coordination platform for pooling financial resources of public authorities and the private sector. This approach is used for the implementation of expensive projects with long payback periods, has a high potential for attracting investments and a set of conditions necessary for the implementation of the project [29], [30].

An example of a public-private partnership is a project of the IoT launched on July 23, 2020, by MegaFon, which will allow public and private medical institutions to offer patients a health monitoring service. At the moment, one solution has been launched for remote monitoring of the health status of patients with hypertension, in the future other solutions will be connected to the system, including the maintenance of measuring devices [31].

For its part, the Government of the Russian Federation must ensure regulatory of the safety of both devices and users. In this regard, the Government of Russia made a strategic decision to ensure information security through the priority use of domestic technological solutions using in various information infrastructures. So, for example, in 2019 the Ministry of Telecom and Mass Communications of Russia approved the Roadmap for the development of "end-to-end" digital technology "Wireless Communication Technologies", which provides for the development of terminal access equipment, collecting parameters by sensors/controlling actuators in communication networks of NB IoT/LTE-MTC using domestic cryptographic algorithms by 2021.

In addition, when creating and developing 5G/IMT-2020 networks on the territory of the Russian Federation, the use of domestic cryptographic algorithms, trusted software, and the electronic component base is also provided, and the introduction of Russian crypto algorithms in the specification of international standards is also proposed [32]. Despite the high security, cryptography has the disadvantage that it is a slower speed. This is noted by scientists and this is confirmed by mathematics [33]. This approach will allow to some extent eliminate the internal uncertainty associated with a large number of data sources, the anonymity of participants, and uncertainty of responsibilities [34], [35].

5. CONCLUSION

Thus, in ensuring the safety of the IoT, an integrated approach should ensure public-private partnerships at the national and international levels and use leading practices and techniques to ensure protection against threats and risks. IoT security is possible with the practical compatibility of legal and technical regulations. Coordination of legal and practical activities should take into account the autonomy and independence of the norms and the subjects of their application.

An additional problem is the lack of reliable standards, which is associated with the practical interaction of virtual and physical environments in the context of cyber-physical systems. Over a short period of time, the amount of information collected (including about users) has grown significantly, and the number and quality of heterogeneous devices have exponentially increased. This problem is relevant not only for the Russian Federation but also for other developed countries. At the same time, a characteristic threat to IoT security in Russia is the use of technologies, a significant part of which belongs to foreign developers. In the Russian Federation, information security is ensured by the development of domestic software and standards. Of course, one can agree with this position of the state, since the control and supervision of technologies that are created in accordance with domestic regulatory documents are easier to implement.

ACKNOWLEDGEMENTS

The reported study was funded by RFBR, project number 20-011-00077 "Legal regulation of the digital profile of a person on the Internet".

REFERENCES

[1] “Guidelines for the implementation and use of the industrial Internet of things to optimize control (supervisory) activities (approved by the minutes of the meeting of the project committee of 09.11.2017 no 73(13),” The Government of the Russian Federation, 2017. [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_284215/u.

[2] Draft Decree of the Government of the Russian Federation on amendments to some acts of the Government of the Russian Federation regarding the functioning and use of the federal state information system “Unified system of identification and authentication,” The Government of the Russian Federation, 2019. [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_284215/u.

[3] S. Kumar, P. Tiwari, and M. Zymbler, “Internet of Things is a revolutionary approach for future technology enhancement: A review,” *Journal of Big Data*, vol. 6, no. 111, pp. 1-21, 2019, doi: 10.1186/s40537-019-0268-2.

[4] Action Plan (roadmap) of the Avtonet National Technology Initiative, “(Appendix no 2 to the minutes of the meeting of the Presidium of the Presidential Council on Economic Modernization and Innovative Development of Russia of 04.24.2018 no1), The Project committee,” 2018. [Online]. Available: http://www.consultant.ru/document/cons_doc_LAW_309650.

[5] C. Kavanagh, “New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?,” Carnegie Endowment for International Peace, US, 2019. [Online]. Available:

https://carnegieendowment.org/2019/08/28/new-tech-new-threats-and-new-governance-challenges-opportunity-to-craft-smarter-responses-pub-79736.

[6] Su-W. Park, J. D. Lim, J. N. Kim First, “A Secure Storage System for Sensitive Data Protection Based on Mobile Virtualization,” *International Journal of Distributed Sensor Networks*, vol. 2015, pp. 1-8, 2015, doi: 10.1155/2015/929380.

[7] The main activities of the Government of the Russian Federation for the period until 2024, The Government of the Russian Federation on September 29, 2018. [Online]. Available: http://government.ru/news/34168/.

[8] Order of the Ministry of Communications of Russia of 10.31.2019 no 637, “On approval of the Plan (roadmap) for the implementation of the Concept for the construction and development of narrow-band wireless networks of the Internet of Things in the Russian,” The Ministry of Communications of Russia, 2019. [Online]. Available: https://digital.gov.ru/ru/documents/7046/.

[9] Order of the Ministry of Communications of Russia of December 31, 2019 no. 932, “On approval of the list of federal executive bodies responsible for the development and approval of threat and violator models for various systems of narrow-band wireless network,” The Ministry of Communications of Russia, 2019. [Online]. Available: https://digital.gov.ru.

[10] “Forecast of the socio-economic development of the Russian Federation for 2018 and for the planning period of 2019 and 2020,” The Ministry of Economic Development of the Russian Federation, 2018. [Online]. Available: http://www.economy.gov.ru.

[11] L. Aggarwal, P. Goswami, S. Sachdeva, “Multi-criterion Intelligent Decision Support system for COVID-19,” Applied Soft Computing, vol. 101, 2021, doi: 10.1016/j.asoc.2020.107056.

[12] B. Al-Duwairi, W. Al-Kahla, Mhd A. AlRefai, Y. Abedalqader, A. Rawash, R. Fahmawi, “SIEM-based detection and mitigation of IoT-botnet DDoS attacks,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 2, pp. 2182-2191, 2020, doi: 10.11591/ijece.v10i2.pp2182-2191.

[13] S. Swathi and H. K. Yogish, “Secure data aggregation in IoT using Efficient-CSDA*,” International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 6, pp. 4889-4897, 2019, doi: 10.11591/ijece.v9i6.pp4889-4897.

[14] “IoT and Smart Infrastructures. Internet of Things (IoT),” The European Union Agency for Cybersecurity, 2020. [Online]. Available: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot2020.

[15] “Good practices for security of IOT,” The European Union Agency for Cybersecurity (ENISA), 2019. [Online]. Available: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures.

[16] Internet of Things, “NIST,” 2019. [Online]. Available: https://www.nist.gov/topics/internet-thingsiot.

[17] “Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT),” 2019. [Online]. Available: https://csrc.nist.gov/publications/detail/nistir/8200/draft.

[18] H. Qasim *et al.*, “Design and implementation home security system and monitoring by using wireless sensor networks WSN/internet of things IOT,” *International Journal of Electrical and Computer Engineering (IJECE),* vol. 10, no. 3. pp. 2617-2624, 2020, doi: 10.11591/ijece.v10i3.pp2617-2624.

[19] Y. Li, Y. Tu, J. Lu and Y. Wang, “A Security Transmission and Storage Solution about Sensing Image for Blockchain in the Internet of Things,” *Sensors*, vol. 20, no. 3, p. 916, 2020, doi: 10.3390/s20030916.

[20] Oh. Hayoung, “Security-aware fair transmission scheme for 802.11 based cognitive IoT,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 3, pp. 2589-2599, 2020, doi: 10.11591/ijece.v10i3.pp2589-2599.

[21] “Basic model of information security threats in key information infrastructure systems,” The Federal Service for Technical and Export Control of Russian, 2007. [Online]. Available: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/1585-informatsionnoe-soobshchenie.

[22] Order of the FSTEC of Russia dated February no. 17, "On approval of the requirements for the protection of information not constituting state secrets contained in state information systems," The Federal Service for Technical and Export Control of Russian, 2013. [Online]. Available: https://fstec.ru/normotvorcheskaya/akty/53.

[23] Order of the Ministry of Economic Development of Russia no. 603, "On approval of the procedure for the transfer of spatial data and materials by federal executive bodies for inclusion in the federal spatial data fund and departmental spatial,” The Ministry of Economic Development of Russia, 2017. [Online]. Available: http://www.pravo.gov.ru.

[24] A. Zharova, “The protect mobile user data in Russia,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 3, pp. 3184-3192, 2020, doi: 10.11591/ijece.v10i3.pp. 3184-3192.

[25] A. Zharova and V. Elin, “The use of Big Data: A Russian perspective of personal data security,” *Computer Law and Security Review*, vol. 33, no. 4, pp. 482-501, 2017, doi: 10.1016/j.clsr.2017.03.025.

[26] N. A. Naraliev, “Review and analysis of standards and protocols in the field of the Internet of things. Modern testing methods and problems of information security IoT,” *International Journal of Open Information Technologies*, vol. 7, no. 8, pp. 94-102, 2019.

[27] J. Wieringa, P. K. Kannan, X. Ma, T. Reutterer, H. Risselada, B. Skiera, “Data analytics in a privacy-concerned world,” *Journal of Business Research*, vol. 122, pp. 915-925, 2021, doi: 10.1016/j.jbusres.2019.05.005.

[28] “Practitioner’s Guide for IoT Security Maturity Model,” Version 1.02019-02-25, 2019. [Online]. Available: https://iiconsortium.org/pdf/IoT_SMM_Practitioner_Guide_2019-02-25.pdf.

[29] I. N. Glukhikh, L. A. Tolstolesova, O. A. Arzikulov, “Systems engineering methodology for designing digital public-private partnership platforms,” Applied System Innovation, vol. 4, no. 1, pp. 1-13, 2021, doi: 10.3390/asi4010004.

[30] Y. Gu, T. Hao, D. Cheng, J. Wang, F. Cheng, “Consensus model with double feedback mechanism based on dynamic trust relationship in social network group decision-making,” *International Journal of Computational Intelligence Systems (IJCIS)*, vol. 14, no. 1, pp. 491-502, 2021, doi: 10.2991/ijcis.d.201228.001.

[31] Order of the Ministry of Telecom and Mass Communications of the Russian Federation of December 27, 2019 no 923, “On approval of the Concept for the creation and development of 5G / IMT-2020 networks in the Russian Federation,” The Ministry of Telecom and Mass Communications of the Russian Federation, 2019. [Online]. Available: http://www.pravo.gov.ru.

[32] Roadmap for the development of end-to-end" digital technology, “Wireless technologies,” Government of the Russian Federation, 2019. [Online]. Available: https://digital.gov.ru.

[33] X. Wang, F. Chen, H. Ye, J Yang, J. Zhu, Z. Zhang *et al.*, “Data Transmission and Access Protection of Community Medical Internet of Things,” *Journal of Sensors*, vol. 2017, no. 4, 2017, doi: 10.1155/2017/7862842.

[34] A. M., Evans, O. Stavrova, H. Rosenbusch, “Expressions of doubt and trust in online user reviews,” *Computers in Human Behavior*, vol. 114, 2021, Art. no. 106556, doi: 10.1016/j.chb.2020.106556.

[35] J. Wang, Y. Yu, Y. Li, C. Fan, S. Hao, “Design and implementation of virtual security function based on multiple enclaves,” *Future Internet*, vol. 13, no. 1, pp. 12-35, 2021, doi: 10.3390/fi13010012.

BIOGRAPHIES OF AUTHORS

Anna Zharova is lecturing since 2003 at the leading universities in Russia. Currently, Anna Zharova is Deputy Head of Department of Legal Security of the Fuel and Energy Complex, National University of Oil and Gas, Professor. Anna Zharova has over 100 publications including 9 books. Her professional interests are information law, intellectual property law. In 2003, the degree of Ph.D. in law was awarded. In 2013, the title of Associate professor has received. In 2020 Anna Zharova defended her doctoral dissertation on "Theoretical foundations of legal regulation of the creation and use of information infrastructures".

Vladimir M. Elin has been lecturing at leading Russian universities since 2003. Currently, Vladimir Elin is the Deputy head of the Department of integrated safety of critical objects at the National University of oil and gas. Vladimir Elin has more than 50 publications, including 5 books. His professional interests: Current problems of ensuring complex security of modern computer systems; Information security of critical information infrastructure; cybercrime and the fight against It. In 2004, he defended His Ph.D. thesis.