Copyright © 2019 International Journal of Cyber Criminology – ISSN: 0974–2891
July – December 2019. Vol. 13(2): 255–269. DOI: 10.5281/zenodo.3698141
Publisher & Editor-in-Chief – K. Jaishankar / Open Access (Authors / Readers No Pay Journal).

Ensuring the Information Security of Information Communication Technology Users in Russia

Anna Zharova[1]
National Research University Higher School of Economics, Russia

Abstract

This paper studies information security for information communication technology (ICT) users in Russia. The study used dialectic, metaphysical and tabular methods. An analysis of the effectiveness of the legal regulation system of ICT security used in Russia starts with a presentation of the legal principles for ensuring the information security of those using ICT and the problem statement. Further, the paper analyzes federal laws; articles of the Russian Criminal Code related to the malicious use of ICT and the illegal receipt of personal information; the theoretical research in this area; the bill to provide consumers with the opportunity to use pre-installed Russian programs when selling certain types of technically complex goods; judicial practice, and the basic standards in this field. Legislative changes were studied for the period from 2015 to 2020. Using the example of these changes, the improvement of the field of ICT security in Russia was demonstrated. In conclusion, changes are proposed that will bring us closer to solving the problem of the emergence malicious ICT which collect user information, including confidential data.

Keywords: ICT security, confidential data, undeclared functionality, software.

Introduction

Artificial intelligence, cloud technologies, big data, the Internet of things, distributed computing and other information communication technologies (ICT) are developing rapidly. At the same time, the level of security in the digital environment remains too weak for the stable and progressive development of national information spheres.

The more devices are connected, the more difficult it is to ensure their integrity, accessibility and confidentiality, because, first, devices record and process restricted information (including personal data) often without the possibility of a person controlling the functioning of these technologies; second, to prevent delinquency, the state must have legal regulation which takes into account the specifics of the technologies used. In this regard, the problems of preventing the illegal collection of information are becoming more acute every year. Effective legal solutions to this problem are those that determine

[1] Director, Center for Cyberspace Research, National Research University Higher School of Economics, Associate Professor, Myasnitskaya Ulitsa, 20, Moscow, Russia, 101000.
Emails: ajarova@hse.ru; anna_jarova@mail.ru

state control of technology algorithms and that provide the user with control over their functioning and the actions they perform. For example, legal norms should contain requirements for developers of hardware and software for the mandatory presence of functions for the control of the processing of user data carried out by these technologies (Big data, artificial intelligence, 2017). Thus, the questions of the placement, storage rules and interaction of ICT, as well as information security need careful legal and technical regulation.

Harmful ICT creates the prerequisites for the formation of traditional and digital crime, for example, software containing viruses and "bookmarks" allows access to information about third parties without informing these persons, to carry out Internet fraud, to hack ICT systems and to disseminate harmful information. The information security of the state is ensured through the security of ICT, and in the era of internet enabled devices, the question arises as to how much a person is protected from the illegal collection of his personal information while using such devices?

In Russia, legal and technical regulation are independent fields and, in most situations, they do not interact with each other; Russian studies are mainly represented by the study of either legal or technical regulation. This paper proposes a comprehensive approach, reflecting the relations of legal and technical regulations to ensure effective information security.

Aim and Rationale of the Present Study

This study analyzes the legal norms and technical standards that form the legislative basis of ICT security, the strategic documents of the Russian Federation in this area and identifies gaps in the regulatory system. We include software and hardware in ICT. In order to best represent the state's policy in ICT security, it is necessary to understand the trends occurring at the level of legislative changes. The presentation of the regulatory system allows us to describe the general system of tools that the state gives to various actors to ensure their own safety or the safety of third parties, as well as punitive state instruments.

To achieve this goal, the following federal laws were examined:

1. "On Information, Information Technologies and Information Protection";
2. "On the Security of Critical Information Infrastructure of the Russian Federation";
3. "On the Protection of Personal Data"; "On the Protection of Consumer Rights";
4. The Criminal Code of the Russian Federation.

The following legal papers were also analyzed:

- the strategic planning documents of the Russian Federation;
- the main standards in the field of ensuring information security;
- the law enforcement practice,
- Bill No. 757423-7 "On providing consumers with the opportunity to use pre-installed Russian programs for electronic computers in the sale of certain types of technically complex goods" (Bill No. 757423-7).

The results of this study may be useful to foreign researchers in conducting a comparative analysis in the field of ICT security.

Literature Review

While using internet enabled devices a person may not suspect that his device is relaying information to a third party who may subsequently use this information illegally, including information regarding children (Choi, Lee & Ree lee, 2017). Such a device can be any technology that has Internet access. There are various vulnerabilities and risks associated with this technology, ratio of big data to personal data (Zharova & Elin, 2017), the risks of illegal collection of information (Marson, 2008). New generation of services are often characterized by high dynamism and untrustworthiness: "existing technologies for managing and applying data privacy policies could be unsuccessful ..." (Talreja & Dilip, 2017). The role of the state is to create legal conditions for limiting possible offenses.

The analysis of the studies makes it possible to identify the main lines of communication security, such as the independent security of smartphone users (Seyed at al., 2013; Sukeshini et al., 2015); ensuring the security by the state if defining the requirements for developers in field the safety of the information technologies, including the requirements of the development and application of standards (Schiller at al., 2017); also by imposing legal liability for the development and use of harmful technologies that violate the confidentiality of information (Dart at al. 2016; ENISA, 2016).

The importance of standards in terms of ensuring information security when using information technologies is that the standards contain a methodology for protecting information technologies and define the range of key issues that developers should be guided by. Legal norms determine the regulation of relationships and the responsibility for non-compliance with the rules of conduct determined by the state. In this regard, the harmonization of legal and technical standards will provide the greatest effect in the field of ICT security regulation. The effectiveness of ICT security can be considered as the coordination of national and international standards. Much research has been devoted to this topic affecting the problems of various states, for example, countries of the Southern African Development Community (Bande, 2018), EU countries (Szczepaniuk, et al., 2020), US (Alexander, et al., 2020), Portugal (Carvalho, et al, 2020), China (Li, 2015).

An analysis of articles on selected states (US, UK, EU, China, Russia) allows us to conclude that the problems of ensuring ICT security are relevant worldwide. The table 1 shows only some of the issues raised in such research.

Methods

To accomplish the aims stated above, court sentences were examined and statistics on criminal offenses in this area are presented. The research was based on the analysis and comparison of normative legal acts and the norms of technical regulation in Russia and the practices of ensuring information security in Europe and in Russia. The sources of normative legal acts were specialized information legal search systems are named "Consultant-Plus" and "Garant", in which all normative legal acts are presented in an actual form. The analysis of normative legal acts and standards allowed to determine the state approaches that are reflected in the functions of specialized state bodies in the field of ensuring information security, and that also revealed the shortcomings of such approaches. In addition, information was used that was posted on the official website of the State Duma of the Russian Federation.

Table 1. Some of the issues raised in Literature Review

States	Types of IT security problems	Research results
US, EU, UK, Russia, China.	The effectiveness of information security management in public administration;	Recommendations for improving information security mechanisms;
	the standardization of the most important information structures;	strengthening the regulation for protection against cyber threats at the regulatory and strategic levels;
	the development of cybersecurity rules and their impact on the business and technology sector.	the implementation of a systematic approach arising from the need for continuous improvement of state regulation.
US, China, UK, Russia.	Profiling cybersecurity risks; profiling human activity on the Internet; personal data in big data; the problem of ensuring cybersecurity with the increase in devices connected to the Internet; the lack of control and the inability to combat cyberthreats.	Establishing appropriate metadata for cybersecurity policies; improving legislation in the field of cybersecurity; the monitoring and analysis of risks and threats; the development of legislation ensuring the security of restricted information.
China, Russia.	The development of an information security policy, including the distinction between "information" and "cybersecurity"; the standardization of the most important information structures.	Identifying the main areas of information security policies; identifying the main implementation problems; reviewing and changing policies in a continuous cycle; developing a comprehensive risk management structure.

The study used dialectic, metaphysical and tabular methods. The dialectic method made it possible to critically examine the regulatory system for ensuring the state's ICT security and to conclude that the effectiveness of regulation can be ensured only through the interconnection of legal and technical norms. An analysis of the effectiveness of the legal regulation of ICT security in Russia begins with the legal principles for ensuring the security of ICT users, and the problem statement. Further in the paper, the main articles of the Criminal Code of the Russian Federation related to the malicious use of ICT and the illegal receipt of personal information were analyzed, as were theoretical studies and judicial practice.

The legislative changes for the period from 2015 to 2019 demonstrated the state turning towards the development of technical regulation and the use of national software.

The study and analysis of the practice, references in European studies, describing possible solutions to information security issues, made it possible to compare the Russian experience of standardization with the experience in Europe and come to the conclusion that the problems of ensuring the safety of communications are relevant worldwide.

In the development of standards in the field of information security of information technologies, European researchers have advanced further. This can be explained by the fact that a large number of information technologies (software and hardware) are developed by European manufacturers. However, it should be noted that Russian policy began to change from 2015. From 2015 to 2020, the Russian Federation adopted more than 2,000 acts at various levels to ensure information security in various areas. In 2019, amendments to 2 Federal laws were adopted that related to ensuring information security in the field of creating and using software and ensuring a safe communication environment in Russia. Since 2019, the government has been implementing, at the legislative level, the requirements for using predominantly domestic software for national and local government bodies and for organizations whose activities are related to critical information infrastructure. In the same year, in Art. 138.1 of the Criminal Code, amendments were adopted by which software can be recognized as special technical means.

Legal conditions were created to attract investment in the Russian economy and improve the quality of goods, work, services. In addition, a bill was passed in third reading on requiring certain types of technically complex goods to have pre-installed Russian software, which should enter into force on July 1, 2020.

General Provisions for Communication Security

In Russia, the constitutional principle of non-interference in the private life of citizens has deep legal traditions. There are requirements for the protection of personal and family secrets, and the correspondence, telephone conversations, postal, telegraphic or other communications of citizens. In 1997, Presidential Decree No. 188 was signed, which defined confidential information as the facts, events and circumstances of a citizen's private life which allow him or her to be identified. In 2006, the Russian Federation adopted the Law on Personal Data, the implementation of which required the adoption of a set of organizational, technical and legal measures aimed at ensuring the security of personal data (Federal Law No 152-ФЗ).

Despite the legal norms for the security of personal data, technologies and malicious software has appeared in Russia, including undeclared functions to illegally collect information transmitted from internet enabled devices. This situation can be explained by the fact that information security when using IT should be provided not only by legal means, but also by a system of standards that supplements the legislative system.

Understanding the complexity of the standardization problem and the diversity of participants in this process, the government, on October 29, 2019, approved the following directions for the implementation of the federal project “Information Security” of the national program “Digital Economy of the Russian Federation” (Resolution of the Government of the Russian, No1382: “the development of requirements for operators of the industrial Internet, draft security standards for cyber-physical systems, and the registration of equipment networks of the IoT devices. The development and adoption of a set of information security standards to minimize risks and threats to the safe functioning of public communication networks, and national and international standards in the field of information security. […] The development of a model of information security threats for personal devices for collecting biometric data and the development of a roadmap for ensuring information security when citizens use this class of technical equipment in the Russian Federation".

Information systems can be associated with various areas of public life, the incapacitation of which can entail enormous economic damage. In order to ensure information security in the areas most important for the state, Federal Law "On the Security of Critical Information Infrastructure of the Russian Federation" entered into force on January 1, 2018 (Federal Law No. 31). Sectors, including communications and financial, are classified as areas of critical information infrastructure. Changes also affected the financial sector, in accordance with 2017 FATF methodology in the federal project "Information Security", (Passport of the federal project "Information Security") including tasks for increasing the technical compliance level with international FATF standards (Rosfinmonitoring, 2019). In their 2019 report, FATF noted that Rosfinmonitoring has achieved significant achievements and it entered the top five countries in terms of the effectiveness of the national anti-laundering system (Russia praised the compliance).

The availability of standards, their diversity, the developed and approved methodology for their application can help solve information security problems if there is a clear state strategy to reduce any threats and possible security risks and minimize new threats and risks. On October 14, 2019, the Ministry of Digital Development, Telecommunications and Mass Media developed a Roadmap for the development of end-to-end digital technology and wireless technology as a strategic public policy instrument that identifies priorities and prospects for the development of technologies in the Russian Federation by 2024 (Roadmap "end-to-end"). Also in 2019, the Federal Service for Supervision of Communications, Information Technologies and Mass Communications (Roskomnadzor) identified key goals for its activities for the year, which included ensuring a timely response and developing relevant measures to respond to challenges and threats associated with active technological changes, and the widespread dissemination of the IoT, big data processing systems, artificial intelligence and next generation communications networks. (Public declaration, 2019)

To understand the processes of ensuring information security in Russia, it must be borne in mind that the application of the requirements of technical regulation to ICT security and to confirm the compliance of IT with information security requirements are not defined as mandatory in Russian Federation (Federal Law of "On Technical Regulation"). Therefore, in the national program "The Digital Economy of the Russian Federation" a number of tasks are set to develop and adopt a national system of standards in this area.

In 2019, a serious change in the state policy in the field of legal regulation, standardization and the licensing of the activities of persons related to the creation and further introduction of ICT into civilian circulation can be noted. "The Digital Economy of the Russian Federation" defined the task of developing, by the end of 2021, requirements for ensuring the control of processing and access to personal, big user data, including in social networks and other means of social communication (Resolution of the Government of the Russian, No1382).

The Concept of "Undeclared Functionality" in Terms of Russian Legislation

Not only the general provisions for ensuring ICT security, but also the applied norms should be adopted for effective legal regulation. This is especially important in ensuring the safety of ICT users, who must be sure that the ICT introduced into civil circulation and legally acquired does not bear any risks. However, this is not always the case, since there is a possibility of "undeclared functionality".

"Undeclared functionality" is a specific term adopted in Russia. According to the guidance document[2], "undeclared capabilities are understood to mean any functionality of the software which is not described or not corresponding to functionality described in the documentation and which may violate the confidentiality, availability or integrity of the information being processed" (*The guidance document, 1999*). Through such undeclared functionality, third parties may illegally gain access to personal data or confidential information. Information security specialists from Perception Point warned of the existence of a dangerous vulnerability in the Linux kernel which gives the attacker full access to the Android operating system as an administrator. This dangerous vulnerability is called CVE-2016-0728 and had existed since 2012 (Shoshin, 2015).

The concept of a malicious computer program is directly related only to the Criminal Code. However, the concept of a "computer program" is defined in the Civil Code as commands to operate computers and other computer devices to obtain a certain result, including the preparatory materials obtained during the development of the computer program and also the audio-visual images generated by it. But the Civil Code considers software only from the point of view of property relations and as a result of intellectual activity.

Software for communication devices that has undeclared functionality is a malicious computer program. From July 26, 2019, amendments were made to Art. 138.1 of the Criminal Code. Currently, it covers special technical means intended for secretly obtaining information include software; other electronic devices for accessing information and (or) obtaining information from technical means for its storage, processing and (or) transmission, and the properties of which are the covert information acquisition or access to it (138.1 of the Criminal Code); and the circulation of these without an appropriate license and not for the needs of the authorities authorized to carry out the operational investigative activities. According to Art. 273 of the Criminal Code "malicious computer programs include programs that are deliberately designed to destroy, block, modify, copy computer information or neutralize computer information protection facilities without authorization."

The statistics presented on the official website for court decisions for the period from May 7, 2019 to August 29, 2019 show that there were 30 convictions under Art. 273 of the Criminal Code (Sentence No. 1-377 / 2019); and 36 convictions under Article 138.1

[2] The guidance document it is a normative branch act that is adopted by the State Technical Commission of Russia, the supervisory and control authority. This document outlines the system of views, the basic principles that form the basis of the problem of protecting information from unauthorized access.

of the Criminal Code (Judicial practice under Article 138.1). Thus, each month there are an average of 10 convictions for each of the above articles of the Criminal Code.

The analysis of the content of the sentences shows that crimes under Article 273 of the Criminal Code are mainly related to the use of counterfeit software, malicious computer programs and the use of such software to illegally access information. Under article 138.1, the crimes are associated with the illegal acquisition of special technical means and their further introduction into civil circulation.

Such a source of threats is the inability to control the ICT being developed and their subsequent use in Russia. The success of identifying such ICT entering Russia is largely associated with the presence of a state administrative system responsible for monitoring, supervising and implementing the national policy for the certification of such technologies. However, in Russia, the ICT certification system is optional.

Information security as a component of all state security cannot be ensured without creating its own ICT. Therefore, in 2019, the tasks of switching to domestic software and protecting information infrastructure were identified in two federal projects of "Digital Economy of the Russian Federation": "Information Infrastructure" and "Information Security".

However, the state policy of transition to Russian ICT has been implemented since 2015. By Order of the Ministry of Communications dated April 1, 2015 No. 96, a plan for the import substitution of software was approved (The order of the Ministry of Communications, 2015). To ensure this task, an autonomous non-profit organization must be created, which organizes collective software development for segments with a high level of dependence on foreign software (GOST R 54593-2011). In 2015, the Ministry of Economic Development issued a negative opinion on the project of the Ministry of Communications of Russia in this field (The Ministry of Communications has prepared a package).

Despite this, Order No. 96 has not been canceled. The non-profit organization has given grants to developers involved in the creation of local ICT.

In addition, the Government Decree of November 16, 2015, No 1236 (Decree of the government, No 1236) established a ban on the use of software originating from foreign states for the procurement of state and municipal needs. The purchase of foreign software is allowed only if there is a justification for the impossibility of observing the prohibition. This has been confirmed by judicial practice (The determination of the Supreme Court, No A65-25932). To determine whether the software is Russian or foreign, criteria for software classes defined which can be replaced by Russian software (Order of the Ministry of Communications, No 622).

Legal entities guilty of violating the laws of the Russian Federation and other regulatory legal acts on the contract system in procurement are charged under Art. 107 of the Law on the contract system.

There have been cases of the cancellation of the purchase of an operating system, which was part of the set of goods purchased by the customer, which falls under the ban on the admission of foreign software, established by Government Decree No. 1236 (Decree of the government 2015, No 1236).

Restrictions on the use of foreign ICT are also in force for the participation of state organizations and legal entities in the critical information infrastructure sectors. On October 1, 2019, the government submitted proposals on measures to ensure technological independence and the security of critical information infrastructure through the use of predominantly domestic software (Putin instructed the Government). Art. 12.1 of the Federal Law "On Information, Information Technologies and the Protection of Information" defines the specifics of state regulation in using Russian software and databases and defines the procedure for creating a unified register of Russian software and databases.

The government determined that by the end of 2019, standards for processing large data arrays, information security standards in systems implementing cloud, fog, quantum technologies, virtual and augmented reality systems, and artificial intelligence should be developed, adopted, harmonized and implemented. In addition, new interstate standards and amendments to existing standards in ICT security for the EAEU should be approved (Passport of the national project "National Program" Digital Economy).

In addition, from July 1, 2020, a law should come into force banning the sale of smartphones, laptops and other devices without pre-installed Russian software Bill No. 757423-7). On February 20, 2020, this bill was adopted by the State Duma in the third reading, so its entry into force is only a matter of time. The law provides for the creation of a list of required software that must be installed on all devices sold in Russia. Smartphones, tablets, computers and televisions with Smart TV are subject to restrictions. A list of such devices will be compiled and approved by the government.

Thus, it can be noted that the state policy in the field of ensuring information security has become focused on the need to ensure control over the ICT introduced into civil circulation and the priority use of national ICT. The first step in this policy is related to the development of a system of national standards for all ICT. A list of areas of economic activities in which the control and supervision of the ICT used must be drawn up, these areas are mainly related to the functioning of critical information infrastructure. For other ICT, used by entities in areas other than critical information infrastructure, legal regulation is still changing quite slowly.

However, information security can be ensured not only by controlling the introduction of software developments into civilian circulation, but also by monitoring the development of ICT algorithms. For example, in 2017, a paper prepared by the information commissioner indicates that it is possible to introduce “algorithmic responsibility”. In essence, this is the possibility of making sure that the machine learning algorithms are used do what we think and do not do what we do not want (Big data, artificial intelligence, 2017). However, neither the Russian scientific literature, nor government documents have yet reflected this.

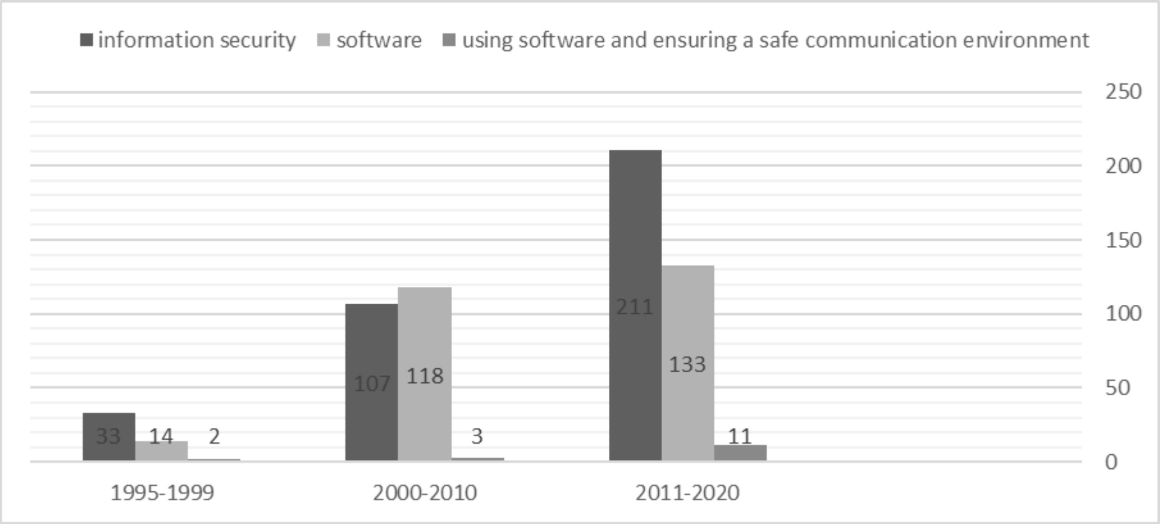
Such an innovation would be interesting, and it is quite possible that such a combination of legal and technical regulation could bring good results. Since the developers would be responsible for the development of inaccurate and opaque algorithms, and users would have the opportunity to legally control the results obtained in the processing of information related to their personal data. Difficulties are also likely in the implementation of such a decision, since this would require the formation of bodies responsible for monitoring and supervision in this area.

The figure 1 is presented allows us to see the dynamics of the development the directions of laws, including federal, in the field of information security of ICT. The selection of laws was made in the field of “information security”, “software” and “using software and ensuring a safe communication environment” for the periods: 1 January 1995

– 31 December 1999; 1 January 2000 – 31 December 2010; 1 January 2011 – 1 March 2020.

1995 was chosen as a conditional beginning, in which the first main Federal Law "On Information, Informatization and Information Protection" was adopted. Another law was passed in 2006, it is the Federal Law "On Information, Information Technologies and the Protection of Information" dated July 27, 2006.

Figure 1. Dynamics of the development the directions of laws, including federal, in the field of information security of ICT



Every year, the issues of regulation of relationships in these areas are becoming increasingly relevant.

The Risks of Leakage of Confidential User Information

The problem of preventing undeclared functionality is directly related to the problems trust evaluation which is still not fully resolved. Although developers are looking for and developing possible security solutions for gadgets. The market offers an information security system called TISSA, which implements Android privacy mode and which can allow users to flexibly control the settings of their phone (Zhou et al.) Defense Information Service Agency (DISA) developed a standard (the Mobile Applications Security Requirements Guide or the SRG) that may be used for developing new apps and testing, vetting, and assessing existing apps, providing a considerable degree of protection through applying controls and best practices in use throughout the industry to reduce vulnerabilities (Schustera, 2017). In China, the responsibility of service providers for infringement of information security is introduced (Li, 2015).

In Russia there is another approach. In 2002, the Federal Law "On Technical Regulation" was adopted to develop, adopt and apply mandatory requirements for products and design-related processes, including their application and execution on voluntary basis requirements to products, design processes, production, construction, installation, commissioning, operation, storage, transportation, sale and disposal, as well as to performing works or provide services for the purpose of voluntary certification.

The scope of this law does not include hardware or software information security. The declaration of conformity says that the products adhere to the requirements of technical regulations (TR). A determination of whether products meet the TR requirements can only be made on the basis of the declaration of conformity.

Further there is no legislative definition of computer information protection tools. In the law "On State Secrets", (*Law No 5485, 1993*) "information security includes technical, cryptographic, software and other means designed to protect information that constitutes state secrets, the means in which they are implemented, as well as means to control the effectiveness of information protection".

However, an information technology consists of hardware and software, and each may have vulnerabilities that can lead to the illegal collection of personal information. Risk can be assessed using a hierarchical method of trust assessment. This allows users to combine trust indicators and to check the metric of trust for each component of the information technology (Weiss, Reznik & Zhuang, 2015). The Russian approach described in the standards also uses this principle (*Guidance document, No 187, 2002).* Such an evaluation system is recognized as the most productive, because evaluates all the components of the system. In applying this methodology, the European and Russian approaches are close. However, despite the existence of a regulatory framework, the issue of preventing the illegal collection of confidential information remains. In this regard, we will consider regulatory acts to determine the requirements and conditions for the hardware and software complex to be introduced into civil circulation in Russia.

Discussion and Conclusion

This paper studies the regulatory problems leading to the failure to ensure ICT security. The work carries out a simultaneous review of legal and technical regulation, since the position of the author is that effective regulation of ICT can only be achieved by developing rules of legal regulation that take into account the specifics of the entire ICT life cycle.

The paper found that the creation and use of ICT that are not supported by mandatory technical regulations leads to such risks and threats as the use of undeclared functions in the hardware and software complex, the leakage of personal data, the unauthorized collection of information, which ultimately inflicts a legal blow ensuring information security. In turn, these negative risks and threats have become the engine for a change in state policy in the field of technical regulation. Only in 2019 were amendments to two federal laws in the field of information security when creating and using software and communication.

The government approved the main directions of information security related to the development of standards for various information technologies (Resolution of the Government, 2019). Two new standards have been developed and adopted to ensure the information security of software (GOST R 58412-2019, GOST R 8.964-2019). In 2018, a federal law was adopted to ensure the information security of critical information infrastructure.

However, despite the significant change in the state policy regarding ICT security, it is possible to note the presence of gaps in the organization of the legal regulation in Russia. It is necessary, therefore, to fix the monitoring and analysis of risks and threats associated with the introduction of new information technologies into civilian traffic for Roskomnadzor. Currently, this monitoring and analysis is carried out only for areas of economic relations related to critical information infrastructure. The results of the analysis should be taken into account in the regularly reviewed national policy of the state.

The list of Roskomnadzor functions does not include the collection of evidence for an offense committed within the "primary" collection of evidence (in the course of the pre-investigation) or the implementation of instructions from the investigator or the court on the performance of urgent investigative actions. The list of information that Roskomnadzor is authorized to block does not include harmful software. Therefore, the extension of the authority of Roskomnadzor will allow application directly to this state body. It is also necessary to extend the authority of Roskomnadzor on the primary collection of evidence. This information on the detected offenses, Roskomnadzor should consult with law enforcement agencies before making decisions. It is necessary to develop legal methods and criteria for identifying undeclared functionality of internet devices.

In addition, it is necessary to provide the relevant authorities with effective legal and technical mechanisms at the political and operational levels to prevent and limit possible risks and threats.

The effectiveness of the protection of users of information technologies introduced into civilian circulation will be promoted by amending in the preamble of law No. 2300 "On the protection of consumer rights". Now, it is determined that this law regulates relations that arise between consumers and manufacturers, sellers, importers when selling goods; establishes the rights of consumers to purchase goods of adequate quality and safety for the health, life and property of consumers and the environment; obtaining information about goods and their manufacturer; establishes state and social protection; and the mechanism to realize these rights. Currently, the law does not protect the rights of consumers of software technologies.

Acknowledgements

I appreciate all our participants who spared their time to be part of the study.

References

Alexander, A., Graham, P., Jackson, E., (2020). Williams, T., Park, J. An analysis of cybersecurity legislation and policy creation on the state level. *Advances in Intelligent Systems and Computing,* 2020.

Armando A., Merlo A., & Verderame, L. (2014). Security considerations related to the use of mobile devices in the operation of critical infrastructures. *International Journal of Critical Infrastructure Protection, 7,* 247 – 256.

Bande, L. C. (2018). Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities. *International Journal of Cyber Criminology. 12 (1),* 9-26.

Big data, artificial intelligence, machine learning and data protection. Retrieved from https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

Bill No. 757423-7 On Amending Article 4 of the Law of the Russian Federation "On Protection of Consumer Rights" (on providing consumers with the opportunity to use pre-installed Russian programs for electronic computers when selling certain types of technically complex goods). Retrieved from https://sozd.duma.gov.ru/bill/757423-7.

Carvalho, J.V., Carvalho, S., Rocha, Á. (2020). Uropean strategy and legislation for cybersecurity: implications for Portugal. *Cluster Computing*, 1216 -1223.

Choi Kyung-Shick, Lee Seong-Sik, & Jin Ree lee. (2017) Mobile Phone Technology and Online Sexual Harassment among Juveniles in South Korea: Effects of Self-control and Social Learning. *International Journal of Cyber Criminology, 11(1).* doi:10.5281/zenodo.56201

Dart E., Whipple H., Pasqua J., Furlow, C. M. (2016). Chapter 13 – Legal, Regulatory, and Ethical Issues in Telehealth Technology in book Computer-Assisted and Web-Based Innovations in Psychology, 339–363.

Decision of the Udmurtia OFAS Russia of 05.24.2018 N OP07-06 / 2018-1393, Retrieved from https://xn--80aahqcqybgko.xn--p1ai/141/13/16302/39291/39368/39372/50722.html.

Decree of the Government of the Russian Federation of November 16, 2015 No 1236, Retrieved from https://legalacts.ru/doc/postanovlenie-pravitelstva-rf-ot-16112015-n-1236/

ENISA. Information sharing and common taxonomies between CSIRTs and Law Enforcement (2016). Retrieved from https://www.enisa.europa.eu/publications/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement.

Federal Law "On the Security of Critical Information Infrastructure of the Russian Federation" No. 31. *Collection of Russian legislation,* July 31, 2017, Part I, 4736.

Federal Law No 152-ФЗ, July 27, 2006 "On Personal Data". *Collection of Legislation of the Russian Federation*, July 31, 2006, No. 31 (1 part), Art. 3451.

Federal Law of December 27, 2002 N 184-ФЗ "On Technical Regulation", *Collection of Legislation of the Russian Federation, December*. 2002, No. 52 (part 1), Art. 5140. Retrieved from https://ivprom.ru/lib/245/

GOST R 54593-2011. National standard of the Russian Federation. Information Technology. Free software. General Provisions. *Reference legal system "ConsultantPlus".*

GOST R 58412-2019. National standard of the Russian Federation. Protection of information. Secure software development. Threats to information security in the development of software. *Reference legal system "ConsultantPlus"*

GOST R 8.964-2019. National standard of the Russian Federation. State system for ensuring the uniformity of measurements. Verification technique. *Reference legal system "ConsultantPlus"*

Judicial practice under Article 138.1 of the Criminal Code of the Russian Federation. Retrieved from https://sudact.ru/law/uk-rf/osobennaia-chast/razdel-vii/glava-19/statia-138.1/?page=1.

Li, X. (2015). Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crime. *International Journal of Cyber Criminology*, 9(2) doi: 10.5281/zenodo.56225

Order of the Ministry of Communications of Russia of December 31, 2015 No 622 "On approval of the rules for using the classifier of programs for electronic computers and databases". Retrieved from https://legalacts.ru/doc/prikaz-minkomsvjazi-rossii-ot-31122015-n-622/

Passport of the National project "National Program Digital Economy of the Russian Federation " (approved by the Presidium of the Presidential Council for Strategic

Development and National Projects, Minutes dated 04.06.2019 No 7). Retrieved from https://legalacts.ru/doc/pasport-natsionalnogo-proekta-natsionalnaja-programma-tsifrovaja-ekonomika-rossiiskoi-federatsii/

Presidential Decree No. 188 of March 6, 1997 No 188 "On approval of the List of Confidential Information". *Collection of the legislation of the Russian Federation*. 1997, No 10, Art. 1127.

Public declaration of the goals and objectives of the federal service for supervision in the field of communication, information technologies and mass communications (Roskomnadzor), 2019. Retrieved from https: Rkn.gov.rn.

Putin instructed the Government to submit proposals on the implementation of Russian software. Retrieved from https://iz.ru/895234/2019-07-02/putin-poruchil-pravitelstvu-predstavit-predlozheniia-po-vnedreniiu-rossiiskogo-po

Resolution of the Government of the Russian Federation of October 29, 2019 No 1382 "The rules for granting subsidies from the federal budget to achieve the results of the federal project "Information Security" of the national program "Digital Economy of the Russian Federation"" Retrieved from http://www.pravo.gov.ru

Roadmap for the development of "end-to-end" digital technology "wireless technology" Retrieved from https://digital.gov.ru

Rosfinmonitoring activity report, 2019. Retrieved from fedsfm.ru/content/files/activity/annualreports/otchet_2018%20рус.pdf

Russia praised the compliance of the national "anti-laundering" system with FATF international standards Retrieved from http://www.fedsfm.ru/releases/4184

Schiller E., Kalogeiton, E., Braun, T., Gomes, A., & Nikaein (2017). No.11: ICN/DTN for Public Safety in Mobile Networks. Book Chapter-Wireless Public Safety Networks, 231-247.

Schustera S., van den Berg M., Larrucea X., Slewe T., Ide-Kostic P. (2017). Mass surveillance and technological policy options: Improving security of private communications, *Computer Standards & Interfaces 50,* 76–82.

Sentence No. 1-377 / 2019 of July 30, 2019 in case No. 1-377 / 2019 Egorievsky City Court (Moscow Region) – Criminal. Retrieved from https://sudact.ru/regular/doc/rjKpDrBPYSds/

Seyed Yahya Vaezpour, Rui Zhang, Kui Wu, Jianping Wang, Gholamali C. Shoja (2013). On the security of certain e-communication types: Risks, user awareness and recommendations, *Journal of Information Security and Applications, 18*(4), 193-205.

Shoshin P. Why is it dangerous to use smartphones (tablets) with Android OS for remote banking services? Retrieved from http://www.banki.ru/blog/kamo4/7400.php.

Stephen M. Marson. (2008) Crimes of the Internet - Frank Schmalleger & Michael Pittaro. *International Journal of Cyber Criminology*, *2*(1), 322–323.

Sukeshini A., Quentin J., (2015) Knock! who's there? Putting the user in control of managing interruptions. *International Journal of Human-Computer Studies, 79*, 35-50.

Szczepaniuk, E. Szczepaniuk, H., Rokicki, T. & Klepacki, B. (2020) Information security assessment in public administration. *Computers and Security. 90*, 234- 245.

Talreja, R., & Dilip M.,(2017) User Privacy on Android Platform, JAN 27-28, *International conference on nascent technologies in engineering (ICNTE-2017), 324-327.*

The determination of the Supreme Court of the Russian Federation (2018) No 306-KG17-22931, Retrieved from https://legalacts.ru/sud/opredelenie-verkhovnogo-suda-rf-ot-20022018-n-306-kg17-22931-po-delu-n-a65-259322016/

The guidance document "Protection against unauthorized access to information - Part 1: Information security software - Classification by the level of control of the absence of undeclared opportunities". Introduced by Order No. 114 of the State Telecommunications Commission of the Russian Federation of 04.06.1999. *Reference legal system "ConsultantPlus"*

The Law of the Russian Federation "On State Secrets" No. 5485-1 (1993). *Collection of laws of Russia, 13.10.1997, No 41,* 8220-8235.

The Ministry of Communications has prepared a package of documents to create an autonomous non-profit organization to support collective software development, Retrieved from https://www.computerra.ru/198623/minkomsvyazi-podgotovilo-paket-dokumentov-dlya-sozdaniya-avtonomnoy-nekommercheskoy-organizatsii-po-podderzhke-kollektivnoy-razrabotki-po/

The National Program "Digital Economy of the Russian Federation" (Approved by the Presidium of the Presidential Council for Strategic Development and National Projects, Minutes No. 7, June 4, 2019), Retrieved from https://digital.gov.ru/ru/activity/directions/858/

The order of the Ministry of Communications of Russia dated 04.04.2015 No 96 “On approval of the import substitution software plan”. *Reference legal system "ConsultantPlus"*

Weiss R., Reznik L., & Zhuang, Y. (2015). Trust Evaluation in Mobile Devices: An Empirical Study, Trustcom/BigDataSE/ISPA, *IEEE.*

Zharova, A. K., & Elin, V. (2017). The use of Big Data: A Russian perspective of personal data security. *Computer Law & Security Review, 33*(4), 482-501.

Zhou Y., Zhang X., Jiang, X., Ffeeh, V., & Zhou Y.et al., (2011) Taming Information-Stealing Smartphone Applications, *in Trust and Trustworthy Computing: 4th International Conference*, TRUST 2011.