International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 3, June 2020, pp. 3184~3192
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i3.pp3184-3192

The protect mobile user data in Russia

Anna Zharova
Center for Cyberspace Research, Higher School of Economics National Research University, Russia
The Institute of State and Law of the Russian Academy of Sciences, Russia

Article Info

Article history:

Received Nov 20, 2019
Revised Dec 28, 2019
Accepted Jan 2, 2020

Keywords:

Information security
Mobile phone
Russia
Standards
Undeclared functionality

ABSTRACT

This paper studies the issue the information security for smartphone users in Russia. The report analyses the regulations the state uses to prevent undeclared functionality and malicious programs in mobile phones in Russia; the law enforcement practice in this area; the responsibility of legal entities, officials and persons for non-compliance with the requirements for standardization, ensuring information security and violation of declaration of conformity. The paper develops proposals to improve state regulation of undeclared functionality of mobile devices providing the collection of information, including confidential data. The report discusses specific ethical issues related to privacy, including matters relating to compensation for damage resulting from the leakage of personal information and develops proposals for legal ensuring the information security of mobile phone users. The report first outlines the main actors, terms and concepts used in the report. Second the standards for mobile phone developers, although there is no guarantee of complete information security. In this case, the peculiarity of Russia is that standards used in the field of information security are voluntary. Third how law enforcement agencies protect the user community. In this case there is a potential danger that this may entail uncontrolled access of government agencies to confidential data.

Corresponding Author:

Anna Zharova,
Center for Cyberspace Research,
Higher School of Economics National Research University,
Russia, Moscow, Shabolovka street, 26s3 119049.
Email: ajarova@hse.ru

1. INTRODUCTION

In the era of smartphones and other internet enabled devices, the question arises as to how much a person is protected from the illegal the collection of personal information while using such devices, "... small-scale IT users remain ill-served by existing cyber security practices" [1]. While using a mobile phone a person may not suspect that his device is relaying information to a third party who may subsequently use this information illegally. Alongside the development of this technology, other technologies are being developed to illegally collect personal information from smartphone users. The illegal collection of information is possible through the installation of a malicious program or through undeclared functions installed on the mobile phone by its developer, "95% of the tested apps have at least one vulnerability" [2]. There are various vulnerabilities and risks associated with the use of mobile devices[3], including the risks of illegal collection of information. New generation of services are often characterized by high dynamism and untrustworthiness: “existing technologies for managing and applying data privacy policies could be unsuccessful ...” [4] For the purpose of unifying the approaches to information security, states are developing standards for technical regulation. Although the application of standards in the development of mobile applications is not always effective [5]. The standards define the range of key issues that developers should be guided by (this depends on the demand of application the standards in the state). However, standards cannot provide all possible vulnerabilities.

Therefore, the effective information security is possible only with interoperability of standards with legal norms. However, despite the existing regulatory system, malicious software and technologies has used in Russia, including undeclared functions to illegally collect information transmitted from internet enabled devices. This problem is relevant for many states, however, the methods of struggle differ not only the methods included in the standards, and the severity of the punishment defined in the law, but also in the level of interoperability of standards and law norms . The analysis of the studies makes it possible to identify the main lines of communication security, such as the independent security of smartphone users if such capabilities are initially provided in the phone [6, 7]; ensuring the security by the state if defining the requirements for developers in field the safety of the mobile technologies, including the requirements of the development and application of standards [8]; also by imposing legal liability for the development and use of harmful technologies that violate the confidentiality of information. In the field of ICT, the development of legal norms without coordination with the norms of technical regulation does not lead to security.

In Russia, legal norms and regulatory standards are divided and inconsistent, that are lead to ineffective information security. The various ways of ensuring information security are offered, for example, by confirming each software change [9], flexible phone settings [10], testing installed applications on the phone [11], by checking the trust metric for each component of the mobile system [12]. Basically, regulation is provided at the level of technology development through the use of mandatory standards. In Russia, information security standards are optional. Some security models are used in Russian standards [12], 13[10] and etc. In this regard, the article analyzes the problems correlation of the legislative system with the norms of technical regulation, which, with the developed regulatory and technical system leads to the fact that mobile phones with undeclared functions and preinstalled malware are used in Russia. For this, methods of preventing the risks of leakage of confidential user information for such application levels as software and hardware were investigated.

The paper examines the following areas of information security for mobile phone users in Russia: first, the law enforcement agencies for the protection of the user community, the identification of the risks and vulnerabilities of mobile phone users, if the phone has "undeclared functionality". Second, the standards for mobile phone developers, although there is no guarantee of complete information security. In this case, the peculiarity of Russia is that legal standards used in the field of information security are voluntary. Third, how law enforcement agencies protect the user community. In this case there is a potential danger that this may entail uncontrolled access of government agencies to confidential data [14]. The paper develops proposals for ensuring the information security of mobile phone users in the territory of the Russian Federation, and paper also presents: the concept of combining legislative and technical norms to prevent risks and threats, and Russian and foreign practices of dealing with vulnerabilities and risks in this area. The problems of state management of information security of mobile phone users from the point of view of the system of interoperability information security standards and the legal regulations in Russia were demonstrated.

2. RESEARCH METHOD

The research was based on the analysis and comparison of normative legal acts and norms of technical regulation in Russia and practices of ensuring information security of mobile communications in Europe and in Russia. Normative acts define the necessary rules of behavior and regulation of relations in the field of ensuring the information security of mobile phone users. 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. The study and analysis of the practice of provision, reflected in European studies, describing possible solutions protection of personal data and information security, 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 mobile communications, European researchers have advanced further. This can be explained by the fact that a large number of mobile communication technologies (software and hardware) are developed by European manufacturers. However, Russia, using such technologies, should also ensure the security of communication and users of mobile telephones. For each person in developed countries, on average, there is more than one such phone. For example, on average, Russians have two mobile phone numbers [15].

To search for and formulate possible ways to develop regulatory regulation and eliminate gaps in Russian legislation, the forecasting and modeling method was used. In Russia, there is a lack of research in this field, in contrast to Europe. For this reason, at a meeting of an expert-consultative group called "On Legal Regulation of Limiting the Use of the Internet for Cryptographic Means and Means of Anonymization for Terrorist Purposes" which was being held under the direction of Roskomnadzor, 2017, this issue was made on the agenda. The author is a member of this expert group.

3. RESULTS AND ANALYSIS

3.1. The term “mobile phone” and “subscriber”

A smartphone is a personal computer with a mobile communication function. In this paper we will use smartphone and mobile phone as synonyms. UMTS mobile phones are subscriber terminals that are structurally and functionally complete devices that have controls and display and provide users with telephony, multimedia and data services for the UMTS mobile telephone system [16]. The definition of a subscriber of "mobile communication", was determined at the end of July 2017, by amending the Federal Law "On Communications". According to Art. 1 "mobile radiotelephone communication services are provided to a subscriber who is an individual or a subscriber who is a legal entity or a sole proprietor" [17].

3.2. The concept of "undeclared functionality" in terms of Russian legislation

"Undeclared functionality" is a specific term adopted in Russia. According to the guidance document, "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" [13]. 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 [18]. Software for mobile devices that has undeclared functionality is a malicious computer program. According to Art. 273 of the Criminal Code "malicious computer programs include programs that are deliberately designed to unauthorized destruction, blocking, modification, copying of computer information or neutralizing computer information protection facilities."

3.3. 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 smartphones. For example, to ensure information security, it is proposed that each update software should be signed (verified) [9]. 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 [10]. 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 [11]. 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 a 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" [19] "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, a mobile phone consists of hardware and software, and each may have vulnerabilities that can lead to the illegal collection of information stored or associated with the mobile phone. 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 mobile system [12]. The Russian approach described in the standards also uses this principle [13]. 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.

3.4. Interoperability of legal norm with norm of technical regulation for mobile data security

There are different position on whether the certification of the mobile phone software leads to the security of the confidential information of the mobile phone user. Security experts agree that standardized solutions and practices should be used in the first place [20], [21]. Standards help officers responsible for introducing new security measures to answer the questions regarding the choice of methods, the priorities and extent of implementation, or the sufficiency of the approach. On the other hand, it is impossible to envisage all situations in the standard, therefore vulnerabilities not covered by regulation will arise. Such vulnerabilities can be exploited. There is risk high is using of reeware routines and libraries that can contain known malware. Russia's approach to software standardization is different. The scope of the Federal Law On Technical Regulation “does not apply to [...] standards for the dissemination, provision or disclosure of information” (para. 3 of Art. 1). Consequently, computer programs are not subject to mandatory certification. When purchasing software, consumers should be assured that there are no functions allowing the illegal transfer of information. However, due to lack or mandatory standards, consumers cannot have such confidence.

According to the logic of the legislation, the voluntarily acceptance of standards means the company demonstrates the safety of its phones to the consumer, giving it a competitive advantage. The network operating system Microsoft Windows Server 2003 confirmed their compliance with the requirements of FSTEC in the certification of information security tools for information security requirements FSTEC of Russia, certifying the Russian version of Windows Server 2003 (Standard Edition and Enterprise Edition) and the R2 version. Microsoft also undertakes the monthly certification of new patches for these products. Given that the development of software is the result of intellectual activity, it is logical to assign responsibility to the software developer. However the part of Russian civil legislation devoted to intellectual activity and the means of individualization does not. According to the first and second part of the Civil Code, the imposition of liability is possible only on the general basis of Art. 15 and 1064 of the Civil Code. According to which a person whose right has been violated may claim full compensation for losses caused to him Part 1 and part 2 of Art. 1064 specifies that losses are understood as expenses that the person has or will have to perform to restore his violated right, as well as the unearned income that this person would have received under normal conditions of civil turnover, had his right not been violated.

The person who caused the harm is exempt from compensation for harm, if he can prove that the harm was not caused through his fault. However, the law may provide compensation for harm and in the absence of the fault of the harm-bearer. The mobile phone user can protect himself only by inclusion of conditions for the responsibility of the developer for errors in the software. However, such procedure for concluding a contract in most cases was not used, because practice follows the path of use agreement of accession. Seyed, et al. [6] believes that the losses to persons using computer programs in their economic activities lie in the contractual sphere. The Civil Code establishes a presumption of fault of the harm-bearer. In Art. 1064, the presumption of the fault of the harm-bearer suggests that the absence of guilt should be presented by harm-bearer. However, the developer's fault does not arise, if the responsibility of the software developer is not determined by the contract and if all the terms that are specified in the contract are complied with.

In the fourth part of the Civil Code: para. 3 of Art. 1252 of the Civil Code determines that rightholder can the protection of his exclusive rights by exercised through a claim for compensation for damages to a person who illegally used the result of intellectual activity or a means of individualization of legal entities, commodities, labor and services, which are provided with legal protection. In this case, the proof of the amount of damages in accordance with the general rules is assigned to the right holder whose right is violated. According to Art. 1252 of the Civil Code, compensation for damages is connected only with the violation of this exclusive right and with the illegal use of the result of intellectual activity or by means of individualization, but not with the fact that the software itself can inflict property or moral harm to users of software. Judicial practice in cases of the protection of intellectual rights has determined that compensation for moral damage as a non-property right is not connected with exclusive rights, "an exclusive right is not subject to protection by recovering compensation for moral harm, as it is a property right" [22]. According Art. 1100 of the Civil Code, the right holder for a protection of his personal non-property rights can claimed on recognizing the right and restoring the situation that existed before the violation of the law; can claimed suppressing actions that violate the law or threaten its violation. According to the general grounds, compensation for moral harm is carried out regardless of the fault of the harm's causer.

Therefore, if the software harms the licensee, then only on the basis of general provisions of the Civil Code, can the licensee demand compensation from the licensor. The licensor must provide evidence that the damage was not his fault. If it is established that the damage was caused through the fault of the licensor, then the licensor will have to satisfy the damage in full, unless the law or the contract provides for compensation of losses in a smaller amount. For example, the European Commission in 2009 proposed a bill to protect software users from errors inherent in the software which provides for the liability of software vendors for the shortcomings of the software product and compensation for damage caused to the consumer as a result of its use [23]. In 2017, EC reconsidered the Directive 85/374/EEC. “The purpose of this evaluation is to assess the functioning and the performance of Council Directive 85/374/EEC concerning Liability for Defective Products (LDP) as modified by Directive 1999/34/EC of the European Parliament and of the Council. A key issue is to reflect whether Directive 85/374/EEC is fit for purpose vis-à-vis new technological developments and whether it covers cases of malfunctioning apps and non-embedded software” [24]. Russia also wants to implement the idea that software should be developed according to security rules.

The Council of the Eurasian Economic Commission determined that "independent software is considered an active medical device [...] and the safety of a medical device is defined as the absence of unacceptable risk associated with causing harm to life, human health and the environment." [25]. Companies are trying to solve these problems by developing the Declaration of Information Security. For example, MTS has developed a Declaration on the Protection of Subscribers from Cyberthreats (MTS), banks are also developing their own Information Security Declarations [26]. Currently, Russian civil law does not directly determine the persons responsible for possible damage caused by software. There are no current standards that determine the security rules of the software being developed. According to Chapter 19 of the Russian Administrative Code, administrative liability is established only for violations of technical regulations, state standards, certification rules, and regulatory documents on ensuring the uniformity of measurements; general purpose hardware and software do not fall into these categories. A way out of such a situation could be the introduction of a practice which would include in license agreements the person responsible for possible harm from the software.

According to Art. 5 of the Civil Code "standard business practice are the established rule of conduct that is prevalent and widely applied in any area of entrepreneurial or other activity, not the rule of conduct provided by law". Standard business practice are sources of law. For example, in ISO/IEC 19770-2: 2009 which was put into effect in Russia in 2016, section “h” defines the requirement "to reflect in the tag of software identification data and the requirements of various subjects, including software developers, software licensors, packers, distributors of software, all subjects which are external to the consumer." [27]. We propose supplementing section “h” of this standard with a provision to include in the software tags identification of who is responsible for any harm caused by the software. This will make it possible to uniquely identify the person in charge and extend responsibility According to the general grounds of the Civil Code. For the legal regulation of the use and certification of mobile devices, it is necessary to amend Art. 2 "Basic Concepts" of the Law "On Communications", adding a definition of "mobile device". In addition, it is necessary to develop a set of legal proposals for the protection of software users from any inherent errors. For this, Art. 1235 of the Civil Code on the license agreement should be supplemented with provisions about the liability of the licensor for errors.

In the preamble of law № 2300 "On the protection of consumer rights" [28] it is determined that the 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. However, neither Rospotrebnadzor nor the Roskomnadzor controls the information security of consumers of mobile communications. Ensuring information security is not a function of Rospotrebnadzor, although it is an agency that is empowered to control the observance and upholding the interests of citizens in a wide variety of industries. The basis for the work of the agency is the law "On the protection of consumer rights". In order for the provisions of the law "On the protection of consumer rights" to apply to the results of intellectual activity, it is necessary that such software (the provision and transfer of rights for the results of intellectual activity) be included in the preamble of this law.

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 mobile devices; procedures for interaction between users of mobile devices and telecommunications operators, and Roskomnazdor with telecom operators, if the spread of harmful software via a mobile phone is confirmed. Interaction procedures should determine the procedure for lodging a complaint to a telecommunications operator or Roskomnadzor about checking a mobile phone if the owner of a mobile phone suspects the presence of harmful software on his device.

Russia provides information security by setting requirements in the standards for the process of working with specific information of limited access (for example, personal data, bank secrecy). However, the study showed that even though mobile operators work with information of limited access (personal user information), the process of ensuring the security of transmitted information and stored information on mobile phone users' phones is outside of the sphere of information security. In this regard, the state needs to reconsider its approaches to monitoring mobile software technologies in Russia, and to standardize the software for mobile phones. In both Europe and Russia, the approaches and models that form the basis for ensuring the information security of mobile users are close, this is because Russia is a member of the ISO international organization for the development of standards. However, most of the problems in Russia are connected with the principle of voluntary adoption of standards in the field of information security. This, in turn, allows technology developers not to certify their technologies, and state bodies do not have the responsibility to control the imported technologies of mobile communication and to supervise the use of such technologies in Russia. Accordingly, mobile phone users have a motivation to protect themselves with the possible technologies presented on the market, but this also leads to the emergence of unreliable technologies on the market that can work for third parties.

3.5. Standards in the field of mobile connection information security

Ambiguity in the certification requirements of mobile phone components increases the likelihood of mobile phones containing undeclared functionality. In Russia, the standards related to information technology security tools are united by the ISO 27000 series. In addition in 2016 Russia introduced State standards GOST R 56546-2015, for vulnerability detection of information systems and the classification of vulnerabilities of information systems. This is part of a set of standards establishing the classification of vulnerabilities, the rules for describing the vulnerabilities, and procedures for performing work to identify and assess the vulnerabilities of information systems. GOST R 56546-2015 classifies these vulnerabilities by their origin and by the type of deficiency. Section 5.2 includes "the ability to introduce commands into the operating system that allow attackers to remotely view directory structures, copy, delete files." The introduction of commands into the OS allows the profiling of a mobile client. An app may contain no malware, but may be programmed to transmit a user's address book, location, and any personally identifying information to a pre-determined location [5].

Since 2018 in Russia, the issue of preserving information has been solved by communication operators being required to store in Russia 1) information about voice data, text messages, images, sounds, video or other communications of users for three years; 2) text messages of users of communication services, voice information, images, sounds, video, other messages of users of communication services for six months [29]. Telecommunications operators are obliged to provide authorized state bodies information on users of communication services and on the communication services rendered to them, and other information necessary for the performance of the tasks assigned to these bodies, in cases established federal laws [29]. The cost of entry into force of these norms was assessed in different ways. A representative of MegaFon said that according to the most modest calculations, expenses for the whole country for all operators would exceed 1 trillion rubles. This will affect the cost of communication services. The head of the Ministry of Communications said that he does not see the threat of an increase in prices for mobile operators due to the adoption of amendments [30].

If confidential data is stored not on the phone but on the server of the mobile operator, then operative access to confidential data should be allowed only from the mobile phone using an application that does not have caching, since "caching is a vulnerability that allows the leaked confidential information stored on the phone" [31]. Although he believes that this risk can be reduced using artificial intelligence, that let add adaptability and error resistance when using high-speed computing [32]. This brings into question the reliability of operators. An evaluation of "reliability" can be carried out either by voluntary certification by the developer of his application, or by an open rating which is carried out by users of this application. The presence of a license will allow the developer to be considered "reliable" or "sufficiently reliable." In the case of an open vote, the class will be assigned according to the size of the received rating. The wide range of applications for mobile phones and mobile phones themselves which all have different requirements of information security makes it difficult for the user to ensure their information security. Governments assign citizens the responsibility of determining the safest model on which the application is based.

Creating a mandatory standardization of applications is of great importance, because applications will be easily recognizable by consumers. The responsibility of the developer will also be clear. For this, standardization bodies should develop mandatory standards for reliable online security and device security in terms of personal data processing. For example, the developers of the standard suggest that the level of security is confirmed by a valid digital signature. This allows a trusted source to create the code and that it does not contain malicious programs. If the signature is missing or the signature cannot be verified, the application should not execute it. Further to this, any mobile code in an app must not only be signed, but also be a mobile code that has already been categorized. Any uncategorized code, even though potentially safe, must not be used [5].

3.6. SIM-cards

An important component of the mobile phone is the Subscriber Identification Module card (SIM-card). This module is a microcomputer in the form of a plastic card with non-volatile memory and its own microprocessor, which provides access to information stored in the memory, and security functions. Through unauthorized access to a SIM-card, information about a person's personal data can be obtained. Technology developers are trying to overcome various vulnerabilities. To ensure the security of mobile business applications, a model of a secure SIM card, named PK-SIM card has been developed, which is a standard SIM card with additional PKI functionality. Developers present a security framework offering solutions for the development of secure mobile business applications using SMS as the bearer [33]. Standard № 03.48 provides end-to-end security services for a SMS message going to or coming from the SIM card [34]. Although there are standards that have some drawbacks, for example, those developed by the European Telecommunications Standards Institute (ETSI) which only addresses the mobile industry needs and does not consider the authentication and session key distribution for broader solutions.

In Russia, IPS\IDS, application firewalls, SIEM, security testing, anti DDoS, anti-fraud systems have been proposed for the protection and control of vulnerabilities. However, recent studies have suggested that IP-based security technologies are no longer effective, and for new solutions - a virtual network, software-defined network, network data naming, research is required because they are still at the initial stage. [35] In addition, the regulatory security of mobile phone users in Russia is related to the legislative requirements for the sale of only identified SIM cards. This practice was introduced only in 2016. The amendments to the Federal Law "On Communications" [29] to prohibit the distribution of SIM-cards without providing real subscriber data to mobile communications operators, established that mobile communications services are provided only to those subscribers who have provided reliable information about them. The verification of the information about the subscriber is carried out by establishing the full name and date of birth by the provision of an identity document; through a single system of identification and authentication; the use of an enhanced electronic signature; through a single portal of government services; and through the information systems of state bodies, if the operator has connections to such systems through a single system of inter-agency electronic interaction. Prior to the adoption of these provisions, SIM cards were sold without a contract.

Mobile operators are obliged to stop the provision of communication services within fifteen days upon receipt of a request from a body that carries out operational searches, or upon receipt of a request from Roskomnadzor, formed on the basis of the results of oversight measures, if the actual data about the users do not correspond with those stated in the subscriber agreements. A subscriber who is a legal entity or an individual entrepreneur, when using corporate tariffs, is obliged to provide the communication operator information about each actual user of the corporate tariff. The consent of such users for the transfer their personal data to the operator is not required. According to clause 4.1.5. GOST R 53732-2009 "the user of a mobile phone becomes the owner of the subscriber number and SIM-card, through which the identification of the subscriber device, its access to the operator's mobile network, as well as protection against unauthorized use of the subscriber number is ensured".

4. CONCLUSION

This paper demonstrates the problems of state management of information security of mobile phone users in Russia. We examined two points of view: the information security standards in Russia and the legal regulations. Possible practical solutions for ensuring the security of user data, both from the state and by the mobile phone user himself were suggested. Such solutions are changes: to the Russian standards; in key management scheme and the control of access to information stored on phones to eliminate problems caused by unauthorized third-party access; as well as empowering Roskomnadzor with the authority to control the spread of information technology with undeclared functionality, and expanding the scope of the law on consumer protection. The study of this problem of ensuring information security is carried out for the first time.

REFERENCES

[1] E. Osborn, and A. Simpson, "On small-scale IT users' system architectures and cyber security: A UK case sudy," *Computers & Security*, vol. 70, pp. 27–50, 2017.
[2] J. Valcke, "Best practices in mobile security," *Biometric Technology Today*, vol. 3, pp. 9-11, Mar. 2016.
[3] A. Armando, *et al.*, "Security considerations related to the use of mobile devices in the operation of critical infrastructures," *International journal of critical infrastructure protection*, vol. 7, pp. 247–256, 2014.
[4] R. Talreja, M. Dilip, "User Privacy on Android Platform," *JAN 27-28, International conference on nascent technologies in engineering (ICNTE-2017)*, 2017.
[5] S. Dye and K. Scarfone, "A standard for developing secure mobile applications," *Computer Standards & Interfaces*, vol. 36, pp. 524–530, 2014.
[6] Y.V. Seyed, *et al*., "On the security of certain e-communication types: Risks, user awareness and recommendations," *Journal of Information Security and Applications*, vol. 18, no. 4, pp. 193-205, 2013.
[7] M.Turkanović, *et al.*, "Reconciling user privacy and implicit authentication for mobile devices," *Computers & Security*, vol. 53, pp. 215-233, 2015.
[8] E. Schiller, *et al.*, "Wireless Public Safety Networks," in *ICN/DTN for Public Safety in Mobile Networks*, vol. 11, pp. 231-247, 2017.
[9] C. Vijayakumaran *et al.*, "A reliable next generation cyber security architecture for industrial internet of things environment," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 1, pp. 387-395, 2020.
[10] Y. Zhou, *et al.*, "Taming Information-Stealing Smartphone Applications," in *Trust and Trustworthy Computing: 4th International Conference, TRUST 2011*, 2011.
[11] S. Schustera, *et al.*, "Mass surveillance and technological policy options: Improving security of private communications," *Computer Standards & Interfaces*, vol. 50, pp. 76–82, 2017.
[12] R. Weiss, *et al.*, "Trust Evaluation in Mobile Devices: An Empirical Study," *Trustcom/BigDataSE/ISPA, IEEE*, 2015.
[13] 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 of the State Telecommunications Commission of the Russian Federation*, vol. 114, 1999.
[14] P.B. Brandtzaeg, *et al.*, "A Mixed-Methods Approach to Mobile App Privacy," *Social Science Computer Review*, vol. 31, 2018.
[15] Decree of the President of the Russian Federation of 09.05.2017 No 203, "On the Strategy for the Development of the Information Society in the Russian Federation for 2017-2030," *Collection of Legislation of the Russian Federation*, no. 20, Art. 2901, 15.05.2017.
[16] Decree of the Government of the Russian Federation of June 30, 2004 No 320 "On approval of the Regulations on the Federal Communications Agency," *Collection of Legislation of the Russian Federation*, no. 27, Art. 2783.
[17] The Federal Law of 07.07.2003 N 126-FZ, "On Communications," *Collection of Legislation of the Russian Federation*, 14.07.2003. no. 28, Art. 2895, Jul 2004.
[18] P. Shoshin, "Why is it dangerous to use smartphones (tablets) with Android OS for remote banking services?," [Online], Available: http://www.banki.ru/blog/kamo4/7400.php.
[19] The Law of the Russian Federation "On State Secrets," no. 5485-1, 1993. *Collection of Legislation of the Russian Federation*, no. 41, pp. 8220-8235, 1997.
[20] H.F. Tipton and M. Krause, "Information Security Management," *Handbook, sixth ed*., 2007.
[21] R. Solms, "Information security management: why standards are important," *Computer Security*, vol. 7, no. 1, pp. 50–57, 1999. doi: 10.1108/09685229910255223.
[22] Review of judicial practice, "In cases related to the resolution of disputes on the protection of intellectual property rights," Approved by the Presidium of the Supreme Court of the Russian Federation on Sep. 23, 2015.
[23] Glyn Moody, "Should Software Developers Be Liable for their Code?," *Linux Journal*, 2009. [Online], Available: https://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0ahUKEwjm4YLgmbDTAhXiA5oKHRoNC3YQFggyMAI&url=http%3A%2F%2Fwww.linuxjournal.com%2Fcontent%2Fshould-software-developers-be-liable-their-code&usg=AFQjCNGMsLb9SMkrGQHYCvemveZ4nYB9Kw
[24] "Evaluation and fitness check(FC) roadmap," *European Commision*, [Online], Available: http://ec.europa.eu/smart-regulation/roadmaps/docs/2016_grow_027_evaluation_defective_products_en.pdf.
[25] The official website of the Eurasian Economic Union. Decision of the Council of the Eurasian Economic Commission "On Approval of the General Requirements for the Safety and Efficiency of Medical Products, Requirements for their Marking and Operational Documentation for them," (2016) [Online] Available: http://www.eaeunion.org/, 17.05.2016.
[26] Declaration of Security "TRUST," Security for Information, [Online], Available: http://www.trust.ru/upload/documents/about/docs/security/security_declaration.pdf.
[27] ISO/IEC 19770-2:2009 Information technology - Software asset management - Part 2: Software identification tag (IDT) GOST R ISO/IEC 19770-2-2014 approved and put into effect by the Order of the Federal Agency for Technical Regulation and Metrology of November 19, no. 1684-st, 2014.
[28] "The Federal Law of On the protection of consumer rights," *Collection of Legislation of the Russian Federation*, vol. 3, Art. 140, 1996.
[29] The Federal Law, "On Communications," *Collection of Legislation of the Russian Federation*, vol. 4383, Art. 2066, 2016.
[30] Acceptance of the "Yarovoy-Ozerov package," https://geektimes.ru/post/278532/.

[31] P. Shasi, *et al.,* "Mobile cloud security: An adversary model for lightweight browser security," *Computer Standards & Interfaces*, vol. 49, pp. 71–78, 2016
[32] M. Aldwairi and L. Tawalbeh, "Security techniques for intelligent spam sensing and anomaly detection in online social platforms," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 10, no. 1, pp. 275-287, 2020.
[33] R. He, *et al.*, "A PK-SIM card based end-to-end security framework for SMS," *Computer Standards & Interfaces* vol. 31, pp. 629–641, 2009.
[34] M. Badra and P. Urien, "SSL integration in SIM SmartCards," *IEEE Wireless Communications and Networking Conference, IEEEWCNC, Atlanta, GA, USA*, 2004.
[35] M. Vidya, C.M. Patil, "Reviewing effectivity in security approaches towards strengthening internet architecture," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 5, pp. 3862-3871, 2019.

BIOGRAPHY OF AUTHOR

Anna Zharova was born in Tashkent 20/09/1972. On 1989 – 1994, she was in the Faculty of Automated Control Systems: Software and automation systems of Tashkent State Technical University named after A.R. Beruni. Also on 2001 – 2002, she studied in the Institute of State and Law of the Russian Academy of Sciences, Moscow, and on the year of 2013-2015, she took Law faculty of Academic International Institute, Qualification: Master of Law. Moscow. She got Academic degree of Candidate of Sciences and Academic title of Docent. For the present position, she becomes a Director of Cyberspace Research Center of National Research University Higher School of Economics (since June 2017). In the working field, she teachs in the Faculty of Business and Management/School of Business Informatics/Department of Innovation and Business in Information Technology, Higher School of Economics. Courses: Information law; Legal basis of high-tech business; Intellectual right (2007- to the present). She Experts of expert advisory group at the National Anti-Terrorism Committee "On the legal regulation of the restriction of the use of cryptographic tools and anonymization tools for terrorist purposes in the Internet." She gets 15 years of legal consulting experience in the area of legal aspects of computing; copyright and IT.