Nexo Revista Científica
Vol. 34, No. 01, pp. 142-153/Marzo 2021

ISSN-E 1995-9516
Universidad Nacional de Ingeniería

http://revistas.uni.edu.ni/index.php/Nexo
https://doi.org/10.5377/nexo.v34i01.11293

Problems and trends of the information security systems in some countries of the Asian region

Problemas y tendencias de los sistemas de seguridad de la información en algunos países de la región Asiática

Vasyl H. Fatkhutdinov[1,*], Anatoliy Y. Frantsuz[2], Kseniia V. Khlabystova[3], Mykola M. Tereshchuk[4], Yana P. Arhat[5]

[1] Pension Fund of Ukraine in Kyiv Region. Main Department. Kyiv, Ukraine
[2] "KROK" University. Department of State and Legal Disciplines. Kyiv, Ukraine
[3] Kyiv University of Tourism, Economics and Law. Department of Constitutional Law. Kyiv, Ukraine
[4] Bila Tserkva National Agrarian University. Department of Constitutional Law and Theoretical and Legal Disciplines. Bila Tserkva, Ukraine
[5] Bila Tserkva National Agrarian University. Department of Civil Law Disciplines. Bila Tserkva, Ukraine
[*] v.fatkhutdinov6286@uohk.com.cn

(recibido/received: 17-November-2020; aceptado/accepted: 19-January-2021)

ABSTRACT

The article is devoted to the theoretical and legal analysis of information security systems in some countries of the Asian region. It is proposed to consider the information protection system as a set of interrelated elements and their interactions aimed at preventing and countering threats in the information sphere, as well as developing and improving the system itself. The system-structural approach allowed the author to highlight the following elements of the information security system: objects, subjects, scope, functions, conditions and directions of the system, principles and legal framework. The main trend in the field of information security of these countries is the strengthening of state regulation of their cyberspace. In particular, the legislation of these countries strictly regulates the rights, duties and responsibilities of the owners of information resources on the Internet, news aggregators, instant messengers and search engine operators.

Keywords: Information protection; Sovereign Internet; Data localization.

RESUMEN

El artículo está dedicado al análisis teórico y legal de los sistemas de seguridad de la información en algunos países de la región asiática. Se propone considerar el sistema de protección de la información como un conjunto de elementos interrelacionados y sus interacciones encaminadas a prevenir y contrarrestar las amenazas en el ámbito de la información, así como desarrollar y mejorar el propio sistema. El enfoque sistema-estructural permitió al autor destacar los siguientes elementos del sistema de seguridad de la información: objetos, sujetos, alcance, funciones, condiciones y direcciones del sistema, principios y marco legal. La principal tendencia en el campo de la seguridad de la información de estos países es el fortalecimiento de la regulación estatal de su ciberespacio. En particular, la legislación de estos países regula

estrictamente los derechos, deberes y responsabilidades de los propietarios de recursos de información en Internet, agregadores de noticias, mensajería instantánea y operadores de motores de búsqueda.

Palabras claves: Protección de la información; Internet soberano; localización de datos.

1. INTRODUCTION

In recent years, Russia has been repeatedly accused of conducting information attacks and campaigns against other States. For example, we can recall the Russian campaign to disrupt the presidential elections in the United States (Shane, 2017), the Expansion of Russian influence in Africa through the use of new tactics of disinformation in social networks (Alba and Frenkel, 2019). The EU recognizes Russia as one of the main sources of misinformation in Europe, and so it has created the East StratCom Task Force. The Task Force was set up to address Russia's ongoing disinformation campaigns. In March 2015, the European Council tasked the High Representative in cooperation with EU institutions and Member States to submit an action plan on strategic communication (Questions and Answers…, 2018). Information tools are widely used in the Russian-Ukrainian conflict against Ukraine. In particular, the Doctrine of information security of Ukraine notes the use of new technologies by the Russian Federation for the implementation of destructive information impact against Ukraine (Decree of the President…, 2017). It became apparent that Russia, more than any other nascent actor on the cyber stage, seems to have devised a way to integrate cyber warfare into a grand strategy capable of achieving political objectives (Wirtz, 2015).

In these conditions, based on the principle of fas est et ab hoste doceri, the study of the experience of ensuring the security of the Russian Federation's own information space is very relevant. The purpose of the article is to analyze legislative acts and program strategic documents of the Russian Federation in the field of information security, taking into account the peculiarities of their implementation in practice. The novelty of the study is due to the consideration of recent changes in the legislation of the Russian Federation on the reform of its security system. The features and problems of interaction of state bodies with citizens and business representatives in the process of ensuring the security of cyberspace are analyzed. The author's definition of the information security system of the Russian Federation is proposed, and the main elements of this system are considered using the system-structural method.

Today, approaches to regulating its information space are changing in the Russian Federation, in particular by strengthening state control over this area. Such processes, on the one hand, are linked to the rapid development of information and communication technologies (hereinafter: ICT), which determines the informatization of all aspects of the life of society and the state, ensures the creation of a global information environment. On the other hand, these processes are a response to the risks and threats to national security, both domestically and internationally. In particular, nowadays the main threats to the national interests of the Russian Federation in the information sphere officially identify cybercrime, attacks on critical objects of the information infrastructure and information and psychological influence that are made to achieve military-political, terrorist and other goals (Decree of the President…, 2016). At the same time, information security of the Russian Federation refers to the state of protection of the individual, society and state from internal and external information threats, which ensure the implementation of constitutional rights and freedoms of man and citizen, decent quality and standard of living of citizens, sovereignty, territorial integrity, and sustainable socio-economic development Federation, defense and security of the state (Decree of the President…, 2016).

2. MATERIALS AND METHODS

The system-structural approach was used in the study, which is one of the main in the study of the essence of the legal phenomenon or process. It is based on the understanding of the system as a whole, consisting of elements uniting by a special feature, function. The set of elements that make up a single whole is the composition of the system, the relationship and interaction of the components of the system form its organization. The integration of components into the system is carried out based on organizational unity. This method provided consideration of the information security of the Russian Federation as a system that has structural links with all its components and the relevant functional areas. Consideration of the information security system allowed us to distinguish its structure: subjects, objects, scope, principles, directions, legal basis. Identifying the structure of the information security system of the Russian Federation helped to determine the place and role of all components in its functioning as a whole, provided that it maintains its integrity in interaction with the external environment. The main directions of the security system in the information space were identified, such as threat prevention and protection in the information sphere, development and improvement of the system itself. Also, within the information security system, legal mechanisms for regulating activities on the Internet have been identified, which can be considered as subsystems for ensuring the information security of the state. In particular, we are talking about regulating the placement of information on online resources, instant messaging services, dissemination of information by news aggregators etc. Besides, methods of analysis, synthesis, scientific comparison and formalization were used. The method of formalization allowed to formulate some definitions in the field of information security, in particular, the definition of the following categories: information security system, objects of information security system in a broad and narrow sense.

The peculiarities of the functioning of the information security system of the Russian Federation are analyzed. The general principles of regulation of access to information in the Russian Federation are defined. The method of synthesis is used when considering the mechanism of realization of the right to be forgotten on the Internet. The peculiarities of dissemination of information by news aggregators established by the Russian legislation are analyzed. The main directions of the introduction of the sovereign Internet are defined. The method of analysis was also used in establishing the criteria for inclusion of the news aggregators in the relevant state register. The powers of the committee in the field of communications, information technologies and mass communications are analyzed and its leading role in the information security system is established.

The list of subjects of the information security system of the Russian Federation is also considered and classified according to the following criteria: the principle of separation of powers (horizontal separation of powers), the principle of federalism (vertical separation of powers), and the nature of competence. Comparative is an important method for legal research, which contributes to the acquisition of new knowledge about approaches and concepts of legal phenomena and processes that are not inherent in national law. This method also makes it possible to establish common and distinctive features and characteristics for similar objects of law in the laws and practices of different states. In this study, the comparative law method allowed to establish common features in government approaches to the regulation of the Internet space of Russia and China, in particular the obligation to localize data in the state and cooperation of IT companies with its law enforcement agencies in terms of data disclosure.

Recently, in scientific works, the situational method has been singled out, the core of which is the analysis of specific situations, the study of situational circumstances that affect the general state of phenomena or processes. This method allowed us to consider the problems of implementing the obligation of organizers of information dissemination on the Internet to provide law enforcement with the keys to decrypt electronic messages of Internet users.

Modern trends in the field of information security of the state are actively studied by scientists from different countries (Chan, 2019; Shemchuk, 2019; Weber, 2020; Wirtz, 2015). However, given the ongoing process of transforming Russia's information security system, comprehensive studies covering all aspects of this issue are not yet available. Therefore, we focused on the official assessment of the state of information security of the Russian Federation and the relevant legislation. The legal basis of the study was provided by the Federal Law No. 149-FZ "On Information, Information Technologies and Information Protection" (2006), which is a profile law on the security of the Russian information environment; The Doctrine of Information Security of the Russian Federation (2016), which sets out the official position on the state and prospects for improving the information security of the state. The information base of the study consists of statistical, sociological and other information on this topic.

3. RESULTS

The above legislative definition can be taken as the basis of a theoretical analysis of the structure of the information security system of the Russian Federation. So, from the above definition, we distinguish such elements of the information security system as the objects, scope, functions, and conditions of the system. The objects of the information security system can be viewed in a broad and narrow sense. According to the broad approach to understanding the objects of the information security system, such they are the individual, society and the state. Securing their rights and interests in the information space is the main purpose of the system. At the same time, in the process of information security of the individual, society and the state, the threats directly to information, information technologies or information infrastructures that act as objects of the information security system in a narrow sense are eliminated. The next element of the information security system is its scope, which includes the information space, which is formed by information systems, technologies, data, communication networks, actors and mechanisms of their interaction.

The functions of the information security system of the Russian Federation determined of necessity to protect the triad of objects of the system in its broad sense. The analysis of The Doctrine of Information Security of the Russian Federation (2016), which is the basic strategic document and the basis for the formation of the state policy of the Russian Federation in the field of national information security, allows us to identify the following main functions of Russian information security system:

- development and adoption of legislation in the field of information security;
- ensuring and protecting the constitutional rights and freedoms of the individual and the citizen in the part concerning obtaining and using information, privacy in the use of information technologies, providing information support to democratic institutions, mechanisms of interaction between the state and civil society, as well as the use of information technologies in the interests of preservation cultural, historical and spiritual and moral values of the multinational people of the Russian Federation (Decree of the President…, 2016);
- protection of information infrastructure;
- development and support of ICT and electronic industry;
- participation in the creation of the international security system and the achievement of equal partnership in it;
- informing the public, both inside and outside the Russian Federation, about the official positions of the state and its policies.

It should be noted that the function for the protection of human rights and freedoms in the information field, enshrined in The Doctrine of Information Security of the Russian Federation (2016) is quite declarative since its implementation is not detailed in the legislation. That is, there is a certain opposition of the interests of the state to the interests of the person, which allows speaking about the presence of information autarky. An important aspect that determines the peculiarities of the functioning of the information security system

of the Russian Federation is the conditions in which it exists. Among them are the state of the state information system and the threats that it faces.

According to The Doctrine of Information Security of the Russian Federation (2016), the threat to information security is a set of actions and factors that create a risk of harming national interests in the information sphere (Decree of the President…, 2016). The current system of information security of the Russian Federation is aimed at counteracting the threats to defense capabilities; state integrity; critical objects of information infrastructure; Russia's international image; management order; credit and financial sphere; rights and interests of the person in the sphere of information. A system in which one of the elements is an object usually has a subject in its structure as well. The subjects of the information security system of the Russian Federation per the law are determined by the President, and their list, in the general form, is enshrined in The Doctrine of Information Security of the Russian Federation (2016). We propose to consider them because of their classification according to the following criteria. On the principle of separation of powers (horizontal separation of powers):

- legislative bodies: The Federation Council of the Federal Assembly and the State Duma of the Federal Assembly of the Russian Federation;
- executive bodies: The President, the Government, the Security Council of the Russian Federation, federal executive bodies, the Central Bank of the Russian Federation, the Military-Industrial Commission of the Russian Federation, interagency bodies;
- judicial authorities.

According to the principle of federalism (vertical separation of powers):

- federal bodies of state power;
- bodies of state power of the subjects of the federation;
- local governments.

By nature of competence:

- bodies of general competence: federal bodies of all branches of government and bodies of state power of subjects of the federation for which functions in the field of information security are not essential;
- bodies of special competence: Federal Service for Supervision in the Sphere of Communication, Information Technologies and Mass Communications (hereinafter: Roskomnadzor), Ministry of Digital Development, Communications and Mass Communications of the Russian Federation, Committee of the State Duma on Security, Federal Service for Technical and Export control, etc.
-

Besides, The Doctrine of Information Security of the Russian Federation (2016) differentiates between the subject and the participant of the system of information security. In particular, participants in the information security system are: owners of critical information infrastructure facilities and organizations operating such facilities, mass media, and communications, organizations of monetary, currency, banking and other spheres of the financial market, telecommunication operators, information systems operators, organizations engaged in the creation and operation of information systems and communication networks, the development, production and operation of information security tools safety, providing services in the field of information security, organizations engaged in educational activities in this field, associations, other organizations, and citizens following the laws of participating in the task of information security (Decree of the President…, 2016).

The legal basis of the system of information security is the Constitution, laws and regulations, generally recognized rules of international law and international treaties of the Russian Federation in the information field. The system of information security of the Russian Federation is based and operates on some general

and special principles. They are defined in the Doctrine of the Russian Federation, among them: constructive interaction between the state and citizens in the field of information security, the sufficiency of forces and means of ensuring information security, the principle of proportionality, legality, etc. (Decree of the President…, 2016). It is worth noting that Russian, as well as Ukrainian, legislative and judicial practices still take the principles of law purely formally. In law, the principles are enshrined in a template and have a moral and political significance rather than a regulatory one. Generally, courts do not analyze litigation through the lens of legal principles.

Based on the analysis of The Doctrine of Information Security of the Russian Federation (2016), we can also identify the main directions of security in the information space, such as prevention of threats and protection in the information sphere, the development, and improvement of the system itself (Decree of the President…, 2016). Therefore, the information security system is a set of interrelated elements and their interaction aimed at preventing and counteracting threats in the information sphere, as well as developing and improving the system itself. Features of the functioning of the information security system of the Russian Federation can be considered through the prism of the Federal Law No. 149-FZ "On information, information technologies and information protection" (2006) (hereinafter: Federal Law No. 149-FZ, 2006). It establishes the legal basis for the exercise of the right to receive, create and disseminate information, regulates the protection of information and determines the order of use of information technology in the territory of the Russian Federation.

Based on Russian legislation, it can be concluded that information is understood to mean data (messages) in any form (written, graphic, audio, etc.) and on any medium (paper or digital). It is an object of a legal relationship and can be divided into the following types on accessibility criteria: information that is open to free access; information that is in limited circulation; prohibited information. Depending on the distribution and dissemination order, the information may be such that: freely distributed; is distributed with the consent of the parties to the relevant legal relationship; is subject to mandatory distribution; restricted or prohibited (information for which administrative or criminal liability is provided). Restricting access to information is governed by federal law, and such information is required to be confidential (for example commercial, professional, business information). At the same time, the Russian Federation Law on Information (2006) provides for a list of types of information that cannot be restricted, namely:

1) regulatory acts affecting the rights, freedoms, and responsibilities of the individual and the citizen, as well as establishing the legal status of organizations and powers of state bodies, local self-government bodies;
2) information on the state of the environment;
3) information on the activity of state and local self-government bodies, as well as on the use of budgetary funds (except for information constituting state or official secret);
4) information accumulated in open-ended funds of libraries, museums, as well as in-state, municipal and other information systems created or intended to provide such information to citizens (individuals) and organizations;
4.1) information contained in archival documents of archival funds (except for information and documents, access to which is restricted by the legislation of the Russian Federation);
5) other information, the inadmissibility of restricting access to which is established by Federal laws (Federal Law No. 149-FZ, 2006).

Another area of regulation of the Internet in the context of information security is the dissemination of information by news aggregators. The law defines them as programs for electronic computers, a site and/or pages of a site on the Internet that are used to process and disseminate news information on the Internet in the official language of the Russian Federation, the state language of the subjects of the federation, or other languages of the peoples of the Russian Federation, which may be targeted at attracting the attention of consumers located in the territory of the Russian Federation and accessed by more than one million Internet

users within one day (Federal Law No. 149-FZ, 2006). The procedure for acquiring the status of a news aggregator by an information resource involves the following stages.

1. Roskomnadzor, on its initiative or as a result of the appeal of state bodies, local self-government bodies, citizens or organizations, discovers information resources in the information-communication systems with the features of news aggregators, recognizes them as such and includes them in the appropriate register. News resources that are registered as online publications are not recognized as news aggregators. It is important that the owner of the news aggregator can be only a Russian legal entity or a citizen of the Russian Federation.
2. Roskomnadzor shall establish a hosting provider or another person who provides the placement of the news aggregator on the Internet and sends them a message with the purpose of identifying the owner of the news aggregator. At the same time, the date and time of sending such a message in the information network are fixed.
3. These persons must provide the information within 3 days from the receipt of the notification.
4. After receiving the data and identifying the owner of the news aggregator, Roskomnadzor informs him about the inclusion of his information resource in the register of news aggregators, specifying the features of the right regulation of their activity.

Removal of an information resource from the register of news aggregators is possible: at the request of its owner if access to the news aggregator is within one month less than one million Internet users within a day; at the initiative of Roskomnadzor if the access to the news aggregator is less than one million Internet users within six months. The owner of a news aggregator is required by law to verify the accuracy of the publicly disseminated information before it is disseminated, and in the event of receiving an order from Roskomnadzor, immediately discontinue its dissemination.

At the same time, the law states that when information is a literal reproduction of messages and materials or fragments of them posted on an official web site of a public authority on the Internet or distributed by an identifiable media which, if necessary, can be held responsible, the owner of the news aggregator shall be exempted from the obligation to verify the accuracy of such information and shall not be responsible for its dissemination. Besides, the owner of a news aggregator undertakes: not to use its resource for unlawful purposes (disseminating forbidden information such as defaming a person's name or interfering with his or her private life, falsified or untrue publicly meaningful information); place contacts on your site to send him legally important information; install one of the Surveillance Programs offered by Roskomnadzor to determine the number of users of an information resource on the Internet; to retain, for six months, the information it disseminates, information about its sources and the timeframe for its dissemination, and to make the data available to the Roskomnadzor (Federal Law No. 149-FZ, 2006).

The termination of the dissemination of information by the owner of the news aggregator shall be made immediately upon receipt of the relevant order from Roskomnadzor. It should be noted that the owner of the news aggregator in the control of information interacts only with Roskomnadzor. This means that if the authorities establish facts of falsification of publicly relevant information on the news aggregator, dissemination of untrue publicly significant news information in the form of reliable messages, and dissemination of news information with other violations of the law, they must apply to the Roskomnadzor through a special electronic system.

An important aspect of ensuring a person's information security is the right to be forgotten on the Internet. The basis of the mechanism of the exercise of this right in the legislation of the Russian Federation was the Judgement of the Court of Justice of the European Union (hereinafter: CJEU) in Case C-131/12 “Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González” (2014). In this decision, the CJEU established that a search engine activity consisting of searching for information published or posted on the Internet by third parties, automatically indexing it, temporarily

storing it, and finally providing access to Internet users following a certain order, should be classified as "processing of personal data", and the search engine operator should be considered as the controller for this processing. The Court stated that individuals, under certain conditions, have the right to request search engines to remove inaccurate, inappropriate or outdated information that contains personal information about them. However, this rule is not universal, and the right to be forgotten is not absolute: decisions in similar cases will be made based on specific circumstances to eliminate their contradictions with fundamental human rights (freedom of speech and press) – a case-by-case assessment (Judgement of CJEU, 2014).

Russia has implemented this approach into its legislation in 2016. There was assigned to the law the obligation of the search engine operator on the Internet, at the request of an individual, to stop issuing a link to a site page in the search results that would allow access to information about the applicant. However, the information which is subject to forgotten must comply at least one of the following criteria:

- are distributed in violation of the law;
- irrelevant information, such that due to the subsequent actions of the applicant or certain events, it has lost its significance (except for the information about the criminal record which has not been withdrawn or not expired);
- false information.

To remove links to unwanted information from search results, an individual must submit to the search engine operator an appropriate request indicating the applicant's contact information, site information and the link to which it should be terminated, giving reasons for such termination and consent to the processing the applicant's data. The search engine operator shall, within ten days of receiving the request, suspend the issuing of links to the information specified in the applicant's request or reasonably refuse the applicant to satisfy his request. Besides, the law provides a procedure for clarifying the applicant's claims, which is also allocated ten days. In case of refusal of the search engine operator to fulfill the requirements of the applicant, he may apply to the court to terminate the issuance of links to the information specified in the request of the applicant.

As practice shows, in the Russian Federation, this mechanism is often tried to use public figures and officials, to delete information about their involvement in corruption scandals or about their criminal prosecutions (Osipov and Golunov, 2016). It is worth noting that sometimes such attempts lead to the opposite result – the interest in the information they are trying to terminate is increasing and the number of searches for it in the search engine is increasing (we are talking about the so-called "Streisand effect"). Therefore, the law imposes a duty on the search engine operator not to disclose information about the fact of the applicant's request to him to stop issuing references to information, except in cases established by federal laws. It is noteworthy that for the entire duration of this mechanism, search engines Google and Yandex only published statistics in the spring of 2016. At that time, Google in Russia received almost 1.5 thousand requests to remove 6.4 thousand URLs. Of these, the US Corporation satisfied 26.2%. Yandex received 3.600 applications, of which it satisfied 27% (Osipov and Sukharevskaia, 2016).

4. DISCUSSION

Since the dissemination of a significant amount of information is carried out through the Internet, the legislation of the Russian Federation establishes mandatory requirements for the placement of information on online resources, including the obligation to place data sufficient to identify the owner of the information or its disseminator, as well as the requirement for owners Internet sites to post their data and contacts to resolve situations related to copyright infringement. When launching resources and applications that are used to receive, store, and transmit instant messages by the Internet users, its owners must inform to Roskomnadzor about it getting started.

In 2016, some federal laws were amended in the Russian Federation, which the media called the "Yarovaya Law" (Kuzmin, 2016). These legislative novelties provided for the strengthening of the rules for the organizers of the dissemination of information on the Internet regarding the localization in the territory of the Russian Federation of the data obtained by them. In particular, information about the facts of acceptance, transmission, processing of electronic messages (in any form) of Internet users, as well as information about the users themselves, should be stored in the territory of the Russian Federation for a year from the moment of completion of such actions. At the same time, the content of such emails should be stored in the territory of the Russian Federation for up to six months from the moment of receipt, transmission, or processing (Federal Law No. 149-FZ, 2006). A lot of criticism and some difficulties in the implementation have been caused by the rule of the "Yarovaya Law" on the obligation of organizers of information dissemination on the Internet, if they carry out additional encryption or provide such services to their users, provide the Federal Security Service (hereinafter: FSB) with the information necessary for decryption e-mail messages from Internet users.

The stated provision of the law led to a confrontation between the Russian authorities and the developers of the Telegram messenger. The Telegram's refusal to provide the FSB with the keys to decrypt messages from 6 users accused of terrorism has led to a series of fines and an obligation on Telegram to provide technology for decrypting messages from users of this social network. In 2018, after a second Telegram refusal, Roskomnadzor moved to try to block the messenger. Some 20 million IP addresses that were used this social network were blocked, but its work was not stopped. Instead, third-party services such as Viber, Google, and others have been affected by this IP blocking (Sharikov and Stepanova, 2019).

At the end of 2019, the head of Roskomnadzor reported that his office is creating a new system to counteract the dissemination of prohibited information. It is it that makes it possible to completely block access to Telegram for users from the Russian Federation. According to the official, the messenger has a year left, after which it will be completely blocked in Russia. To do this, it has begun testing the Deep Traffic Filtering Equipment (DPI) in the Ural Federal District (Agajanov, 2019). The policy of the Russian Federation to localize data in its territory and the obligation to cooperate with law enforcement agencies are similar to the approaches applied in the PRC. According to article 41 of the China Cyber Security Act mandates network operators to collect and store personal information following the law, administrative regulations and their user agreements, within the PRC (Cybersecurity Law…, 2017). Foreign IT companies have several options for meeting these requirements. Thus, some international companies have decided to hire local data server vendors to store Chinese citizens' data following the rules. China's data center services are growing rapidly. Huawei, Tencent, and Alibaba are expanding and investing in data centers both locally and abroad, challenging companies like Microsoft, Google, and Amazon that do not have this home-based advantage (Chan, 2019). Other international companies have built their own data centers in China or leased data centers to host their servers and equipment (colocation). For example, Apple was outsourcing its Chinese iCloud operations to south China based Guizhou-Cloud Big Data. Soon after, they announced that they were investing in the building of 2 new data centers in China due to begin operation in 2020, to store their Chinese iCloud data with accordance to the Cybersecurity Law (Chan, 2019). In Russia, foreign IT companies are complying with the law on data localization through leasing servers in Russian data centers.

In 2017, the Russian Federation also established additional rules for organizers of instant messaging services regarding mandatory identification of users by subscriber number and storage of such identification data in the territory of the Russian Federation; providing technical facilities for users to block the receipt of unwanted messages and guaranteeing the confidentiality of transmitted electronic messages; cooperation with law enforcement agencies, in cases established by law, in providing information about users and the content of their communications; closely working with Roskomnadzor to block the transmission of prohibited information by users (Federal Law No. 149-FZ, 2006). An important event in the field of state regulation of Russian cyberspace was the adoption of the so-called Law "On sovereign Internet" (Federal

Law No. 90-FZ…, 2019). This piece of legislation has sparked debate in expert circles and led to mass street protests. This law provides the following innovations:

1. A national domain name system is being established and will begin to apply from 2021.
2. It is incumbent upon telecommunication operators that are providing Internet access services to install state technical means of counteracting threats and to notify Roskomnadzor of the actual location of the installation of such technical means.
3. The Roskomnadzor received the function of coordination and centralized management of the public communications network (if there are threats to the RuNet).
4. Roskomnadzor has been allowed to restrict access to sites that are prohibited in Russia using technical means of counteracting threats in the manner of centralized management of the public communications network.
5. It is provided the obligatory participation of telecommunication operators in training on ensuring sustainable, safe and holistic functioning Internet in the territory of the Russian Federation.

Critics of the "sovereign Internet" in the Russian Federation compare it with the Chinese project "Golden Shield", which provides Internet content filtering in China. This project includes a security management system, an offense reporting system, a traffic management system, a monitoring information system, and an exit and entry control system.

Of course, there are some parallels between the Russian model of regulation of the Internet space and the Great Chinese Firewall. Especially if we recall that in May 2015, the Agreement on Cooperation in the field of international information security was signed between the Russian Federation and the PRC, which provides for close cooperation on the protection of international cyberspace, technology sharing and experience, inter alia, in regulating the national segment of the Internet (Bevza and Khachatryan, 2015). Such cooperation and borrowing of the Chinese experience in government regulation of the Internet to increase the security of Russian Internet resources could have the opposite effect. In particular, experts note that there could be intelligence and national security risks. Copying the China model has meant the import of and dependence on Chinese technology, which could leave Russia exposed to Chinese spying. Second, Russia's influence in Central Asia, which is of vital security and economic importance to Moscow, is likely to recede. Although Russia used to have information control ideas and technology to offer Central Asia, China is becoming the security equipment supplier of choice in the region (Weber, 2020). In general, such trends in Russian-Chinese cooperation in the field of information security give grounds for classifying the Russian model of information security as an Asian type (Shemchuk, 2019).

In the aspect of information technology protection in Russia, the policy of developing modern ICTs and expanding the use of Russian programs for electronic computers and databases is being implemented. An important innovation in this area was the introduction from 02.12.2019 the mandatory installation of certain types of technically complex goods of Russian software. This legislative provision was adopted despite the reservations of the Russian Association of Trading Companies and Manufacturers of Electrical and Computer Equipment regarding its negative impact on the development of the industry and monopolization in the development of Russian software (Federal Law No. 425-FZ…, 2019).

5. CONCLUSIONS

Based on theoretical and legal analysis of the legislation of the Russian Federation in the field of information security, it is possible to formulate the definition of information security system as a set of interrelated elements and their interaction, aimed at preventing and countering threats in the information sphere, as well as developing and improving the system itself. In the structure of information security of the following elements can be distinguished: objects, subjects, scope, functions, conditions, and directions of operation of the system, principles and legal basis. We propose to consider the objects in a broad and narrow sense.

Entities can be classified according to the following criteria: the nature of competence, the principle of separation of powers and federalism. The information security system of the Russian Federation is at the stage of deep transformations, the main trend of which is to strengthen state control over the national segment of the Internet. Today already introduced mandatory data localization in Russia for organizers of information distribution on the Internet, it is provided obligatory installation for certain types of technically complex goods of the Russian software, expanded the powers of the Federal service for supervision in the sphere of Telecom, information technologies and mass communications and is launched a program of "sovereign Internet".

Features of the system ensuring security in the cyberspace of the Russian Federation are the following: the establishment of rules for dissemination information on online resources in terms of its reliability and verification of its disseminators; the obligatory cooperation of the organizers of information dissemination on the Internet with the security authorities regarding the transmission of data about Internet users, their messages, decryption technologies, etc.; regulation of the activity of organizers of instant messaging services, news aggregators, search engines; mandatory installation of state technical means to counter threats within the framework of the «sovereign Internet» program by Telecom operators that provide Internet access services; functioning of the mechanism for exercising the right to be forgotten on the Internet.

REFERENCES

Agajanov, M. (2019). Roskomnadzor called the deadlines for blocking Telegram in Russia. Russia. The Habr. 3, 15 p.

Alba, D., Frenkel, S. (2019). Russia tests new disinformation tactics in Africa to expand influence. The New York Times. 11, 2 p.

Bevza, D., Khachatryan, E. (2015). Russia and China launch cybersecurity partnership. Gazeta ru. 5, p. 1.

Chan, C. (2019). Understanding China's data security law: an intro for foreign businesses. Medium. 1, 7 p.

Creemers R., Triolo P. & Webster G. Cybersecurity. (2018). Law of the People's Republic of China. New America. 7, 11-12.

Federal Law No. 149-ФЗ "On Information, Information Technology and Information Protection". (2006). Russian Federation. Konsultant plyus. 107, 16-27.

Federal Law No. 425-FZ "On Amending Article 4 of the Law of the Russian Federation "On Protection of Consumer Rights"". (2019). Russian Federation. 304, 11-28.

Federal Law No. 90-FZ "On Amendments to the Federal Law "On Communications" and the Federal Law "On Information, Information Technologies and Information Protection"". (2019). Russian Federation. 352, 8-15.

Kuzmin, A. (2016). All cloud services and online stores fall under the Yarovaya law. Rusbase. 7, 16-17.

Osipov, I., Golunov, I. (2016). Businessman Sergei Mikhailov used the "right to be forgotten". RBK. 3, 5 p.

Osipov, I., Sukharevskaia, A. (2016). Yandex rejected two-thirds of requests under the "right to forgotten" law. RBK. 11, 4-5.

Shane, S. (2017). The fake Americans Russia created to influence the election. The New York Times. 8, 16-17.

Sharikov, P., Stepanova, N. (2019). Approaches of the USA, EU and Russia to the problem of information policy. Modern Europe, 2(87), 73-84. doi: http://dx.doi.org/10.15211/soveurope220197383.

Shemchuk, V. (2019). Asian model of ensuring the information security of modern states. Bulletin of Luhansk State University of Internal Affairs named after E.O. Didorenko, 4(88), 67-80. doi: https://doi.org/10.33766/2524-0323.88.67-80

The Doctrine of Information Security of the Russian Federation. (2016). Russian Federation. Rossiyskaya gazeta, 187, 15-24.

Weber, V. (2020). The sinicization of Russia's cyber sovereignty model. Council on foreign relations. 4, 13 p.

Wirtz, J.J. (2015). Cyber war and strategic culture: the Russian integration of cyber power into grand strategy. In Cyber War in Perspective: Russian Aggression against Ukraine. Tallinn, Estonia: NATO CCD COE Publications. 155-164.

SEMBLANCE OF THE AUTHORS

Vasyl H. Fatkhutdinov: Full Doctor in Law, Associate Professor, Hear of the Main Department of the Pension Fund of Ukraine in Kyiv Region. Research interests are a scientific and applied problem of administrative and legal support of public safety and the formation of the concept of public safety support.

Anatoliy Y. Frantsuz: Full Doctor in Law, Professor at the Department of State and Legal Disciplines of the "KROK" University**.** Research interests: administrative-legal regulation, occupational safety, industrial safety, public administration, administrative sanctions.

Kseniia V. Khlabystova: PhD in Law, Department of Constitutional Law of the Kyiv University of Tourism, Economics and Law. Scientific and research interests: administrative-legal regulation, public administration, administrative sanctions.

Mykola M. Tereshchuk: PhD in Law, Department of Constitutional Law and Theoretical and Legal Disciplines of the Bila Tserkva National Agrarian University. Research interests include forms of government, legal liability, public law.

Yana P. Arhat: PhD in Law, Department of Civil Law Disciplines of the Bila Tserkva National Agrarian University. Research interests: public administration, legal liability, public safety.