Genesis of Russian cyber security legal mechanism: an authentic or a trend alike model?

Ella Gorian[1]

[1] Vladivostok State University of Economics and Service, 41, Gogol str., Vladivostok, 690014, Russian Federation
ella.gorian@gmail.com

Abstract. The object of the research is the relationship within the improvement of the national legal mechanism for cybersecurity in the new conditions of emerging cyber threats. The features of the Russian legal mechanism for information security are being characterized, the role of the Russian Federation in the international system of information communication technologies security is determined. The autonomous Internet law and the data localization law are being reviewed and evaluated for the compliance with the international trends and information security standards. The general and the special legal methods of scientific knowledge (comparative legal and formal-legal methods) were used in the study. The elaboration of the Russian legal mechanism of cyber security has the common features with the other national mechanisms. The use of the "autonomous Internet" model is justified by the stated goals; possible law misuses are expected and are eliminated due to the available tools. The Russian data localization model is a natural response to cyber threats and helps to reduce the potential risks that occur within the globalization processes, and no state is insured from those risks even if its cybersecurity mechanism is considered as the best in the world (as in Singapore). The Russian legislator should consider setting similar technical requirements as the United States, Australia and the United Kingdom has made (for imported telecommunication equipment), especially in light of the 5G networks development.

Keywords: Cybersecurity, critical information infrastructure, information communication technologies, autonomous internet, data localization.

1 Introduction

The last decade's feature is the involvement of the private sector representatives in the national cybersecurity mechanisms and the simultaneous strengthening of the state control within it. The most striking example is the situation in the UK, whose government in 2010 created a joint center with one of the leading manufacturers of telecommunications equipment Huawei (PRC) - Huawei Cyber Security Evaluation Center (HCSEC). It was founded in November 2010 due to the agreement between Huawei and the UK government on elimination of all potential risks associated with the Huawei's participation in the elaboration of a critical information infrastructure (CII).

HCSEC provides an assessment of the safety of telecommunications equipment used in the country and submits annual reports on Huawei technologies and products to the government [1]. HCSEC activities are being controlled directly by the National Cyber Security Center of the United Kingdom (NCSC). In 2012 a special report for the US House of Representatives recognized the largest manufacturers of telecommunications equipment from China as a potential threat to national security [2] due to suspicion of communication between representatives of the private sector and the government of the PRC and the possible compromise of the supplied equipment and technologies.

In 2018 Australia conducted the cyber training and the possible consequences of attacks on CII networks that used the 5G technology were discovered. It raised the concerns of states and certain measures had been taken at the national level – starting from the total ban on the purchase of telecommunications equipment from PRC manufacturers (USA) and ending on the limitation of the spheres for its use (EU member states). Previous measures of some states were aimed at the "pinpoint" security ensuring mostly the personal data and CII. Potential risks associated with the implementation of new technologies force many states to tackle problems using non-standard methods, for example, by ensuring the "autonomous" mode (Russian Federation) or the isolation of information computer networks (PRC). The difficulty of evaluating the effectiveness of a national legal mechanism of cybersecurity lies in the impossibility [4] or unwillingness to consider this legal phenomenon without the political context [3]. All the above said determines the importance of our research.

2 Methodology and literature review

In this study we will use the general methods (system structural, formal logical and hermeneutic ones) as well as the special legal methods of scientific knowledge (comparative legal and formal legal methods).

The subject of the study comprises the legal acts in the sphere of information security at the national and international levels. The chosen topic is poorly represented in the Russian scientific literature. Institutional aspects of the Russian cybersecurity mechanism are discussed in the researches on the activities of the Federal Service for Technical and Export Control (FSTEC) [5] and the Federal Security Service of the Russian Federation (FSS) [6], the Federal Service for Supervision in the Field of Communications, Information Technology and Mass Communications (Roskomnadzor) [7]. Research on foreign mechanisms are very poorly represented [8].

At the international level of research one should note the work on the Russian concept of cybersecurity in the international and national aspects [9], and also should mention the discussion regarding the elaboration of national mechanisms by the qualitative expanding of participants to include the private sector actors [10; 11]. It should be noted that for foreign researchers the Russian cybersecurity mechanism is primarily of interest in the foreign policy aspect [12].

3 Hypothesis

The measures taken by Russia to ensure information security both at the international and national levels are often criticized by the political opponents as well as the Internet users. The main arguments are follows: the restriction of users civil rights and freedoms as a form of censorship, the state monopolization of key positions on telecommunications - cross-border communication lines, technological communication networks, traffic exchange points, etc. The questions arise: how much does the cybersecurity mechanism used by Russia differ from the other ones? How are these measures justified from the point of view for ensuring public and national security?

4 Results and Discussion

The Russian Federation is the initiator of a system of international information security. Despite the fact that the problem of the sustainable development of the international community in the era of information and computer technologies has been the subject of discussion for several decades, nonetheless, since 1998 the Russian draft resolution of the UN General Assembly "Developments in the field of information and telecommunications in the context of international security" being supported by India and China has caused the debates with the US and the EU such key issues as digital sovereignty and human rights. However, as a result of these resolutions a Group of Governmental Experts (GGE) on cybersecurity was created and successfully has been working for many years (2004-2005, 2009-2010, 2012-2013, 2014- 2015, 2016-2017, 2018 - the present). In 2011 Russia and its associates in the Shanghai Cooperation Organisation proposed for consideration the International Code of Conduct for Information Security [14] in the form of a draft convention on international information security (Draft Convention on international information security), but a different West's approach to regulating cyberspace [9] was one of the reasons for the rejection of this document. Nevertheless, the launched process of active interaction of states within the framework of GGE followed by discussion of the annual reports of the UN Secretary General approved the multipolar nature of international security and brought Singapore, India and China to the opinion leaders. The result of the work of the GGE on Cybersecurity is the so-called states' code of conduct in the public sphere, covering 13 standards included in two resolutions of the UN General Assembly in 2018: 1) the principle of international cooperation in developing and implementing measures to strengthen stability and security of information communication technologies (ICT) and the prevention of the malicious acts in the sphere of ICT that are recognized as harmful or that may pose a threat to international peace and security; 2) the principle of the substantiation of accusations of organizing and implementing wrongful acts brought against States; 3) the prohibition of the use of its territory for internationally wrongful acts both by subjects of international law and non-state actors; 4) develop the best forms of cooperation in this area; 5) the integrity of information security with the protection of human rights; 6) the principle of renouncement from activities in the field of ICT which may be harmful to CII; 7) the duty to protect

CII in accordance to the international standards of a global culture of cybersecurity; 8) the duty to assist each other in the defense of CII; 9) the obligation to take reasonable measures to ensure the integrity of the information supply channels; 10) the duty to prevent the proliferation of malicious ICT software and hardware and the use of hidden malicious functions; 11) transparency of prevention actions and availability of information on ICT vulnerabilities; 12) the duty to refrain from carrying out and supporting activities to the detriment of computer incident preparedness groups and not to use them for malicious actions; 13) involvement of the private sector and civil society in the cybersecurity mechanism (paragraph 1) [15].

At the same time Russian Federation is making efforts to unify the rules of international information security at the regional and bilateral levels. At the regional level certain steps were taken within the framework of the Shanghai Cooperation Organization (signing the agreement in 2009 and the Dushanbe Declaration in 2014 in the field of ensuring international information security), the Commonwealth of Independent States (signing the concept in 2008, and agreements in 2012-2013) as well as the Collective Security Treaty Organization (the creation of the Center for Countering Cyber Threats in 2014). At the bilateral level, agreements were signed in the field of international information security between Russia and the Republic of Belarus (2013), Cuba (2014), People's Republic of China (2015), Vietnam (2018), etc.

At the national level the elaboration of a cybersecurity mechanism is comparable to the developed states. In particular in 2018 the Federal Law on Security of the CII came into force (hereinafter - FZ-187) [16], the criminal law established liability for wrongful acts against CII (article 274.1 of the Criminal Code).

It should be noted that according to the classification of the European Union Agency for Network and Information Security (ENISA) the Russian cybersecurity mechanism for CII protection corresponds to the fourth, the highest possible level [17, p. 6]. The legal instruments adopted in recent years allow not only to identify CII sectors, but also to establish their category to determine the necessary level of protection [18]. As a disadvantage that requires a prompt correction in this aspect is the lack of clear regulations on the procedure for identifying information networks as CII and the organizations as the subjects of CII [19, p. 55].

The institutional cyber security mechanism of Russia is represented by a number of public authorities of general and special competence. The President and the Government of the Russian Federation carry out the overall coordination of the activities of the special competence bodies - the FSS, the FSTEC and the National Computer Incident Coordination Center (hereinafter referred to as NCICC). The FSB performs legal regulation of the NCICC activity, which collects, accumulates, systematizes and analyzes information received from subjects of the CII and FSTEC, as well as organizes the exchange of this information between Russian CII subjects, foreign CII subjects and authorized bodies of foreign states, international and non-governmental organizations of domestic and foreign nature (clause 4.2) [20]. The FSTEC operates a register of significant CII facilities and establishes requirements for ensuring their safety, and also exercises federal control in this area. Ministry of Digital Development, Communications and Mass Media (hereinafter - the Ministry of Communications) approves the procedure and technical conditions of installation and operation of the hardware

designed to search for signs of computer attacks in telecommunication networks which organize the interaction of CII facilities (clause 5, article 6 of the FZ-187). A specific feature of the Russian mechanism is the active participation of the FSS, a governmental service with special forces and instruments, and also endowed with procedural competence to respond to cyber attacks [19, p. 58].

The legal characteristics of the Russian cyber security mechanism in comparison with the leading states was a subject of our previous research [19; 21]. We concluded that both the institutional and regulatory Russian cybersecurity mechanisms are not inferior to the international trends of the leading states (in particular, Singapore), and in some ways have even their advantages. The main goal of cybersecurity is to protect information systems (first of all, CII) and the data contained. Therefore the state should provide the protection of these two objects. To solve the first task, the state either limits its responsibility within the CII (the so-called "classical" model), or takes responsibility for the security of all information systems, using special organizational, legal and technical measures (the so-called "Chinese" model). The second task is being solved either by imposing responsibility for the safety of the data on the users and information system operators - the "liberal" model, or by introducing special requirements for localizing all data within the jurisdiction of the state - the data nationalism model.

The process of solving the above mentioned two tasks by Russian legislature is follows. In May 2019 the so-called "Autonomous Internet Law" [22] was adopted provoking harsh discussions among users and ICT actors. The aim of this act is to confront threats to the stability, security and integrity of the Internet and public communication networks within the territory of the Russian Federation. However, the text of the law does not indicate the types of such threats. To this end, a corresponding government decree is being developed, which contains a detailed description of the threats [23]. In particular, there are three types: 1) the threat to integrity; 2) the threat of sustainability; 3) the threat to the safety of the functioning of public communication networks.

The threat to the integrity of public communication networks is the threat of disruption of the ability of communication networks to interoperate, so it becomes impossible to establish a connection and (or) transfer information between users of communication services. The threat to the stability of common user communication networks means the threat in which the communication network's ability to preserve its integrity under the operating conditions of the technical communication equipment is violated if part of the communication network elements fails (reliability of the communication network), as well as under the conditions of external destabilizing effects of natural and man-made character (survivability of a communication network). The threat to the safety of the operation of public telecommunication networks means the threat of a violation of the operator's ability to resist unauthorized access to technical and software of the public telecommunications network and deliberate destabilizing internal or external information influences, which may result in disruption of the communication network (clauses 5-7 of section II) [23].

The Autonomous Internet Law moved amendments to the core federal laws: "On Communications" [24] and "On Information, Information Technologies and Informa-

tion Protection" [25]. A legal definition of the term "traffic exchange point" was implemented into the federal law "On Communications" and it means a combination of hardware and software, communication facilities that are used to connect and transfer traffic between communication networks, if the owner of communication networks has the autonomous system number (clause 28.5 article 2) [24]. The "autonomous system number" is also a new concept for the legislation and it means a unique identifier for the set of communications and other technical tools in the information and telecommunications network (clause 1 article 56.1) [24].

The key provision of the autonomous Internet law is a special technical measure to ensure cybersecurity i.e. to counter threats to the stability, security and integrity of the Internet. That measure is a mandatory requirement to install specific technical hardware in networks defined as "technical means of countering threats" (clause 5.1 article 46) [24]. This measure is associated with the organizational legal measure to impose additional responsibilities on telecom operators providing access to the Internet (hereinafter - providers). They are obliged to install the mentioned technical hardware and within three subsequent days to provide information about the actual place of its installation to the authorized body and to comply with the technical conditions of installation of these technical means and requirements for communication networks (clause 5.1 article 46) [24] . More detailed requirements for the installation and operation of technical means for countering threats as well as for upgrading communication networks by providers will be approved by the relevant regulation of the Government of the Russian Federation.

The very mechanism of the functioning of the "autonomous Internet" is described in chapter 7.1 "Ensuring the Sustainable, Safe and Integral Functioning of the Information and Telecommunication Network (Internet) in the Territory of the Russian Federation" amending the federal law "On Communications".

First, it is the providers (telecom operators, owners of technological communication networks, traffic exchange points, communication lines crossing the state border of the Russian Federation, as well as other persons having an autonomous system number) who are responsible for the sustainable and secure functioning of the Internet in Russia (clause 1 article 56.1) [24]. To fulfill this duty these actors must acquire practical skills gained at the special training (clause 3 article 56.1) [24]. The draft government regulation contains provisions on the types, aims, objectives and procedure of the training [26], [27]. In particular the trainings are planned to be held at the federal and regional levels (clause 2); in addition to providers it is planned to involve the Ministry of Communications, the FSS, the Ministry of Defense, the Federal Protective Service, the Ministry Civil Defense, Emergencies and Elimination of Consequences of Natural Disasters, Roskomnadzor, the Federal Agency for Communication as well as other government bodies and local governments by decision of the Ministry of Communications (clause 3). During the training it is planned to achieve the following aims: 1) to define and to implement measures to identify threats to information security, the integrity and sustainability of the Internet and to clarify the models of such threats; 2) to update the norms ensuring the specified safety; 3) to learn the use of techniques to ensure the sustainability of the Internet and public telecommunications

network in the state; 4) to research and to improve of techniques and methods to ensure the security of the Internet and public communication networks (clause 5) [26].
The draft regulation provides for the basis for organizing and conducting the training - an approved plan of the Ministry of Communications, which must be agreed with the FSS, the Ministry of Defense, the Federal Protective Service and the Ministry for Civil Defense, Emergencies and Elimination of Consequences of Natural Disasters (clause 6) [26]. Such a plan should include a) the curricula and the procedure of the training; b) the purpose of the training; c) the timing of the training and its schedule; d) the executive authorities involved in the preparation and conduct of the training, the management and composition board of the training; f) the scope of implementation - federal or regional level; g) networks or network segments, including emulated subscriber traffic, intended for conducting the training; h) a list of training activities; i) the procedure for monitoring the implementation of training exercises (clause 7) [26]. The management board and the list of the participants is determined by the order of the Ministry of Communications (clause 8) [26]. The responsibility for the preparation of the training is imposed on the Center for Monitoring and Management of the Public Communication Network (clause 10), created in February 2019 [26].
In addition to the obligations to install technical means of countering threats and participating in trainings, providers are obliged to 1) make agreements on the transfer to possession or use of a communication line crossing the state border of the Russian Federation, which contain the information on the purpose of use the specified communication line, as well as on communication facilities installed on the communication line (clause 1 article 56.2.) [24]; 2) to notify on the commencement of activities to ensure the functioning of the traffic exchange point (clause 2 article 56.2) [24].
It is necessary to note such an organizational legal measure of the information security mechanism as the establishment of a special registry of traffic exchange points (clause 3 article 56.2) [24].
If an autonomous system number is assigned to the provider, it has additional responsibilities (clauses 8-9 article 56.2) [24] related to the peculiarities of the legal regime of autonomous systems. For example, in a case of using the traffic exchange points to interact with autonomous system number provider one should send telecommunications messages using the traffic exchange points, details of which are contained in the registry of traffic exchange points (clause 8.2 article 56.2) [24]. It is necessary to emphasize the obligation of the provider to provide in a manner prescribed by law the following information: 1) on the number of their autonomous system and its network addresses; 2) on interaction with providers that have an autonomous system number; 3) on the places of connection of their communication facilities to communication lines crossing the state border of the Russian Federation, and hardware and software used for this purpose; 4) on the location of installation of their communications equipment connected to communication lines located outside the territory of the Russian Federation; 5) on telecommunication routes; 6) on the infrastructure of its communication network (clause 8.4 article 56.2) [24]. There is also an obligation of providers under the autonomous system number to cooperate and to assist the authorized state authorities carrying out operational investigative activities or ensuring the secu-

rity of the Russian Federation (clause 9.3 article 56.2) [24] in accordance with the law (clause 10 article 56.2) [24].

In the event of threats to the sustainability, security and integrity of the Russian Internet segment, a special procedure for responding to the elements of the institutional mechanism is provided for: 1) monitoring the functioning of networks; 2) the introduction of centralized management of a public telecommunications network (by transmitting binding instructions to providers participating in centralized management); 3) the provision to providers the technical facilities for countering threats with the subsequent regulation of the technical conditions of their installation and use on the free of charge basis (article 65.1) [24]. The procedure for centralized management of a public telecommunications network is established by the Government of the Russian Federation and includes: 1) the types of threats; 2) the procedure for identifying threats and measures to eliminate them; 3) requirements for organizational and technical cooperation in the framework of centralized management of a public telecommunications network; 4) methods for determining the technical feasibility of executing instructions transmitted within the framework of centralized management of a public telecommunications network; 5) the conditions and cases in which the provider has the right not to send traffic through technical means to counter threats (clause 5 article 65.1) [24]. Subjects of centralized management are obliged to comply with the established rules of telecommunication message routing (clause 6 article 65.1) [24]. The law also establishes a requirement for the localization of communication facilities used in centralized management (within the territory of the Russian Federation) (clause 8 article 65.1) [24]. After the autonomous Internet law comes into force (November 1, 2019), the ban of prohibited content will not be carried out by telecom operators as it is now but by Roskomnadzor itself.

The amendments to the federal law "On Information, Information Technologies and Information Protection" provide for a number of organizational, legal and technical measures to ensure the security of information and communication systems. In particular, Article 13 includes clause 2.1 which provides for the obligation of state and municipal providers (operators of state information systems, municipal information systems, information systems of legal entities carrying out the procurement in accordance with the federal law of July 18, 2011 №223-FZ "On procurement of goods, works, services by certain types of legal entities") in the operation of information systems to exclude the use of databases and technical facilities outside the territory of the Russian Federation which are not the part of such information systems [25]. Any interaction of public sector entities by themselves and with individuals should be carried out in accordance with the rules and principles established by the national standards of the Russian Federation in the field of cryptographic protection of information (clause 2.3 article 13) [25]. This provision will enter into force on January 1, 2021.

The autonomous Internet law provides for the creation of a national domain name system (a set of interrelated software and hardware designed to store and retrieve information about network addresses and domain names) (clause 1 article 14.2) [25]. The list of domain name groups constituting the Russian national domain zone will be

determined by Roskomnadzor (clause 3 article 14.2) [25]. The regulation acts are under development and the law comes into force on January 1, 2021.

As far as it can be concluded by the text of the law and the presented drafts of regulations for its implementation the Russian model of the "autonomous" Internet is not a "tracing paper" of the models of the PRC or the North Korea but it is an original model characterized by the state participation for the achieving the aim stated (protection from the certain types of threats). In contrast to the above mentioned states there is no rigid centralization and a state monopoly on the provision of information services in Russia. In China the state determines not only service providers, but also their content (in a form of the so-called censorship). Moreover, the "Chinese" model is characterized by outsourcing the censorship function to the private sector (for example, to a news aggregator such as Toutiao), turning the private sector into quasi-public corporations, but ensuring their commercial freedom [28]. Internet censorship in the PRC is established and regulated by three regulations. The Temporary Regulation for the Management of Computer Information Network International Connection 1996 provides for the licensing of providers and the obligatory transfer of Internet traffic through the one of the networks: ChinaNet (China Telecommunications Corporation), GBNet (Golden Bridge Network), CERNET (The China Education and Research Network) or CSTNET (China Science and Technology Network). The second source of regulation is the Ordinance for Security Protection of Computer Information Systems 1994, which delegates information security to the Ministry of Public Security and established such concepts as "harmful information" and "harmful activity" in relation to the Internet. The third source is the State Council Order №292, which establishes the general rules restricting the activities of Internet providers (licensing and separate permissions to transmit data from foreign media). The article 11 of this Order imposes the responsibility of providers on ensuring the legality of any information disseminated, and article 14 gives public officials full access to any confidential information they want from Internet service providers [29].

As we can observe the Russian model is significantly different from the Chinese one. Since a full comparison of these models is the object of a separate study, a comparison of general approaches allows us to conclude that these models are qualitatively different, despite the apparent similarity. The difference lies in both the goals and the means to achieve these goals. The Russian model is aimed at ensuring the security of the Russian segment of the Internet from external threats, while the Chinese model is to provide citizens of the country with "human wisdom" crystallized on the Internet (the internet is called as "a crystallization of human wisdom"), encouraging the use of the Internet in ways that promote economic and social security [30]. The Russian model provides for a situational response to threats defined by the law, while the Chinese model presents a permanent activity of authorized entities to generate content approved by the government.

Nevertheless, there may be problems associated with the abuse of the facilities of the autonomous Internet, both in private and state interests (this concerns fears of the liberal part of society that these tools will be used as means of censorship). However in the first case there are appropriate legal protection mechanisms and in the second case a balance between public and private interests is necessary, which may require

reforms of the state control (supervision) system, since Austria and Germany already have positive experience [7, p. 148]. Provided that the regulatory prescriptions (both the letter and the spirit of the law) are strictly observed, this mechanism can become an important structural component of the Russian cybersecurity mechanism.
With regard to data protection as it was mentioned above states follow the path of either imposing responsibility for data safety on the users and information system operators themselves, setting strict rules for providers (the "liberal" model) or by introducing special requirements for localizing all data within the state's jurisdiction (a data nationalism model). The idea of "data nationalism" is fulfilled in a Russian law that obliges personal data operators to collect personal data (including through the Internet), to record, systematize, accumulate, store, refine (update, change) and extract it using the databases located within the territory of Russia [31] and it is not a new one for the international community. Many states adopt the so-called data localization laws to a certain extent. For example, Nigerian law establishes the rule that all government data should be placed within its borders; Vietnam obliges Internet providers to store data on the territory of the state for possible state verification; Australia prohibits in some cases the transfer of data on health status abroad; and special European Union data protection directives encourage localization of data within it, setting strict requirements for the transfer of personal data to non-EU countries [32]. Protection of personal data became the object of close attention of the legislature of Singapore after its mass compromise in 2018 including the personal data of the head of state [33]. India's refusal to liberalize its data localization law in favor of the United States was the basis for the latter to apply countermeasures in the form of a tightening of the visa regime for specialists involved in information technology [34]. Therefore, it can be concluded that the elaboration of the Russian personal data protection model is a trend alike in international community to ensure national information security.

5 Conclusions

The elaboration of the Russian legal mechanism of cyber security follows the path of many states of the world. The use of the "autonomous Internet" model is justified by the stated goal; possible abuses are expected and eliminated by the available tools. The Russian data localization model within national jurisdiction is a natural response to cyber threats to reduce the potential risks that exist in the current situation of globalization and no state is safe from it, even if its cybersecurity mechanism is considered as the best in the world (Singapore). As for the future the Russian legislature should consider applying measures similar to those taken in recent years by the United States, Australia and the United Kingdom [35] in relation to stricter requirements for imported equipment, especially in light of the development of 5G generation networks.

References

1. Huawei cyber security evaluation centre oversight board: the fifth annual report for the Cabinet Secretary from the Huawei Cyber Security Evaluation Centre Oversight Board (2019). GOV.UK Homepage, https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019, last accessed 2019/06/25.
2. Investigation of the security threat posed by Chinese telecommunications companies Huawei and ZTE: Permanent Select Committee on Intelligence report for the United States House of Representatives (2012). U.S. House of Representatives Permanent Select Committee on Intelligence Homepage, http://intelligence.house.gov/hearing/investigation-security-threat-posed-chinesetelecommunications-companies-huawei-and-zte-0, last accessed 2019/06/25.
3. Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE: A report by Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger of the Permanent Select Committee on Intelligence (2012). Stanford Libraries Homepage, https://searchworks.stanford.edu/view/9762611, last accessed 2019/06/25.
4. Noor E. ASEAN Takes a Bold Cybersecurity Step (2018). The Diplomat Homepage, https://thediplomat.com/2018/10/asean-takes-a-boldcybersecurity-step/, last accessed 2019/06/25.
5. Portnova A.S. The analysis of modern regulative methodical documents of FSTEC in a sphere of intrusion detection system. In: 8th All-Russian Scientific and Technical Conference, pp. 340-346. Moscow State Technical University named after N.E. Bauman (National Research University), Moscow (2017).
6. Trufanov V.N., Shchavelev D.A., Demidov I.V., Sovalin S.V. Approach to the creation of personal data centers in organizations that protect the state information resources. Informatization and communication. 1, 56-62 (2018).
7. Ivanskyi V.P., Melnichuk G.V. State control (supervision) - a tool to counter threats to national security in the information sphere or a means of protecting privacy: the ratio of private and public interests. Bulletin of Russian University of People's Friendship. Series: Jurisprudence. 21(1), 136-152 (2017).
8. Ageev V.O., Shilov A.K. Ensuring the protection of SIS in foreign and domestic systems. Information countering the threat of terrorism. 24, 312-315 (2015).
9. Giles K. Russia's public stance on cyberspace issues. In: 4th International Conference on Cyber Conflict (CYCON 2012), pp. 1-13. NATO CCD COE Publications, Tallinn (2012).
10. Matania E., Yoffe L., Goldstein T. Structuring the national cyber defence: in evolution towards a Central Cyber Authority. Journal of Cyber Policy. 2(1), 16-25 (2017).
11. Farrand B., Carrapico H. Blurring Public and Private: Cybersecurity in the Age of Regulatory Capitalism. In: Security Privatization: How Non-Security-Related Private Businesses Shape Security Governance, pp. 197-217. Springer International Publishing AG, Basel (2018).
12. Grigsby A. Unpacking The Competing Russian and U.S. Cyberspace Resolutions at the United Nations (2018). Council on Foreign Relations Homepage, https://www.cfr.org/blog/unpacking-competing-russian-and-us-cyberspace-resolutions-united-nations, last accessed 2019/06/25.
13. International code of conduct for information security, Annex to the letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/66/359) (2011). United Nations Homepage,

https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf, last accessed 2019/06/25.
14. Developments in the field of information and telecommunications in the context of international security resolution A/73/505 (2018). UN Homepage, https://undocs.org/en/A/73/505, last accessed 2019/06/25.
15. Federal Law on safety of critical information infrastructure of the Russian Federation (2017).
16. Mattioli R., Levy-Bencheton C.: Methodologies for the identification of Critical Information Infrastructure assets and services: Guidelines for charting electronic data communication networks. European Union Agency for Network and Information Security (ENISA), Heraklion (2014).
17. Regulation of Government of Russian Federation on approval of the Rules for the categorization of objects of critical information infrastructure of the Russian Federation, with a list of indicators of criteria for the significance of objects of critical information infrastructure of the Russian Federation and their values (2018).
18. Gorian E.: Institutional mechanisms of critical information infrastructure security in Russian Federation and Singapore: legal comparative aspect. Administrative and Municipal Law, 9, 49-60 (2018).
19. Order of FSS of Russian Federation on the National Computer Incident Coordination Center (with the Provision on the National Computer Incident Coordination Center) (2018).
20. Gorian E.: Identification of critical information infrastructure in Russian Federation and Singapore: legal comparative aspect. Administrative and Municipal Law, 11, 44-56 (2018).
21. Federal Law on Amendments to the Federal Law "On Communications" and the Federal Law "On Information, Information Technologies and Information Protection" (2019).
22. Draft regulation of Government of Russian Federation on approval of the procedure for centralized management of a public telecommunications network (2019).
23. Federal Law on Communications (2003).
24. Federal Law on Information, Information Technologies and Information Protection (2006).
25. Draft regulation of Government of Russian Federation on approval of the provisions on conducting training to ensure sustainable, safe and holistic functioning of the information and telecommunication network "Internet" and public communication network in the territory of the Russian Federation (2019).
26. Regulation of Government of Russian Federation on the Center for Monitoring and Management of a Public Communication Network (2019).
27. Alekseenko A.P. New Russian Model BIT and the Practice of Investment Arbitration. Manchester Journal of International Economic Law, 16(1), 79-93 (2019).
28. China has the world's most centralised internet system: a perfect example of a Hamiltonian internet for maximum control (2018). The Economist Homepage, https://www.economist.com/special-report/2018/06/28/china-has-the-worlds-most-centralised-internet-system, last accessed 2019/06/25.
29. Measures for the Administration of Internet Information Services (2000). CECC: Freedom of Expression – Laws and Regulations Homepage, http://webarchive.loc.gov/all/20040623205930/http://www.cecc.gov/pages/virtualAcad/exp/explaws.php, last accessed 2019/06/25.
30. White paper on the Internet in China (2010). China Daily Homepage, http://www.chinadaily.com.cn/china/2010-06/08/content_9950198_4.htm, last accessed 2019/06/25.

31. Federal Law on On Amendments to Certain Legislative Acts of the Russian Federation regarding the clarification of the procedure for processing personal data in information and telecommunication networks (2014).
32. Bowman C. Data Localization Laws: an Emerging Global Trend (2017). JURIST – Hotline Homepage, https://www.jurist.org/commentary/2017/01/Courtney-Bowman-data-localization/, last accessed 2019/06/25.
33. Tham I. Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack (2018). The Straits Times Singapore Homepage, https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most, last accessed 2019/06/25.
34. Dasgupta N., Kalra A. Exclusive: U.S. tells India it is mulling caps on H-1B visas to deter data rules – sources (2019). Reuters Homepage, https://www.reuters.com/article/us-usa-trade-india-exclusive-idUSKCN1TK2LG, last accessed 2019/06/25.
35. Botton N., Lee-Makiyama H. 5G and National Security After Australia's Telecom Sector Security Review (2018). ECIPE Policy Brief Homepage, https://ecipe.org/wp-content/uploads/2018/10/TSSR-final.pdf, last accessed 2019/06/25.