Advances in Economics, Business and Management Research, volume 128
International Scientific Conference "Far East Con" (ISCFEC 2020)

Information Security Ensuring in the Financial Sector as Part of the Implementation of the National Program "Data Economy Russia 2024"

K Horian[1], E Gorian[2]

[1]HorianSis Studio, Vladivostok, 690014, Russian Federation
[2]Vladivostok State University of Economics and Service, 41, Gogol str., Vladivostok, 690014, Russian Federation

E-mail: kristina.gorian@gmail.com

Abstract. The object of the research is the relations arising from the implementation of the National Program "Data Economy Russia 2024" in the aspect of ensuring information security in the financial sector of Russia. The role of the state financial regulator in the implementation of this program is determined, taking into account the peculiarities of its legal status. The key documents that form the regulatory and legal mechanisms for ensuring the information security of the financial and banking sector of Russia are examined. The content of the activity of the center of competence of the federal project "Information Security" is determined and the need to determine the Bank of Russia as the center of competence is justified. Despite the serious constitutional and legal status and experience of practical management of processes to ensure the security of financial institutions, the potential of the financial regulator is not fully used in the National Program "Data Economy Russia 2024", although the tasks assigned to the center of competence in information security are of a public nature and accordingly must be performed by the relevant subject. As the confirmation and logical continuation of the main role declared by the legislation in ensuring the stability of the financial system the Bank of Russia should be maintained as the center of competence of the federal project, since the financial regulator has all the organizational and legal powers and material resources (FinCERT) for this words.

1. Introduction

In order to implement the Strategy for the Development of the Information Society in the Russian Federation for 2017–2030 [1], the national program "Data Economy Russia 2024" [2] (hereinafter - the Program) was approved in 2017. Its main goal was to create a digital environment that ensures the interaction of all participants in the public and private sectors in all spheres of life in sufficient and necessary institutional and infrastructural conditions for the development of high technologies used in both traditional and new sectors of the economy. The Program's Roadmap initially envisaged five areas for the development of the digital economy in Russia: 1) legal regulation; 2) human resources and education; 3) the formation of research competencies and technological groundwork; 4) information infrastructure; 5) information security [2]. However at the end of 2018 the Passport of the National Program "Data Economy Russia 2024" [3] was approved providing the implementation of six federal projects under the Program (paragraphs 4.1-4.6): a) legal regulation of the digital environment; b)

information infrastructure; c) frames for the digital economy; d) information security; e) digital technologies; e) digital public administration. To implement the Program a management system was developed, including among other things the so-called "centers of competence" (paragraph 4). Centers of competence are engaged in a) the collection of proposals and the preparation of draft passports for federal projects of the Program, including an explanatory note, a financial and economic justification, and requests for alternations to passports for federal projects of the Program; b) the submission of these projects to the appointed working group and other members of the management system; c) the consideration of final reports on the implementation of the Program and on the implementation of federal projects of the Program; d) the consideration of draft acts and draft amendments to draft laws, which may have an impact on the implementation of the Program and the implementation of federal projects of the Program, as well as draft official comments on such draft laws; e) the implementation of measures of federal projects of the Program within the framework of its competence including the preparation of draft acts (clause 12) [4].

One of the federal projects of the Program is the abovementioned "Information Security", which is to ensure information security based on domestic developments in the transmission, processing and storage of data, guaranteeing the protection of the interests of the individuals, business and the state (clause 4.4) [3]. The results of this task are follows: 1) the creation of conditions for global competitiveness for the domestic developments and information security technologies export; 2) the stability and security of the information infrastructure and data transfer, processing and storage services; 3) the protection of the rights and the legitimate interests of individuals, business and the state from cyber threats in a digital economy; 4) the use of domestic developments and technologies in the transfer, processing and storage of data. However, Sberbank of Russia was designated as the center of competence for this federal project of the Program, and N. Kasperskaya the president of the InfoWatch group of companies was appointed as the head of the working group in the Information Security tier [5]. At the same time, the function of the financial regulator in Russia is performed by the Central Bank of the Russian Federation (Bank of Russia), which has a special constitutional legal status and corresponding powers. The management of the Bank of Russia has repeatedly appealed to the Government of the Russian Federation with a request to reconsider the decision on the definition of Sberbank of Russia as a center of competence in favor of the Bank of Russia or at least to transfer some of its powers to it, but to no avail [6]. Their arguments were follows: firstly, the Bank of Russia successfully operates a center for monitoring and responding to computer attacks in the credit and financial sector (FinCERT); secondly, its participation "harmonizes the program with the strategic goals of financial market development and reduces the risks of a conflict of interest in the envisaging and execution of the program ... these functions are "exclusively state-owned and are not characteristic of commercial banks" [6]. After all, the financial regulator is responsible for the stable functioning of the financial market and the banking system of Russia (Art. 2) [7], it plays a coordinating role setting the rules for the implementation of financial institutions, including in the field of ensuring the safety of their operations [8, p. 26]. Therefore, a theoretical study and substantiation of the role of the Bank of Russia as a center of competence for the federal Information Security project of the National Program "Data Economy Russia 2024" is necessary. All of the above indicates the relevance of the research topic.

2. Methodology and literature review

The methodology for this study comprises of two groups of methods: the general scientific ones (system-structural, formal-logical and hermeneutical methods) and the special legal methods of cognition (comparative legal analyses and formal-legal method). In order to obtain the most reliable scientific results they were used in complex. The subject of the research is the main regulatory and legal acts defining the content of the Program and the powers of the Bank of Russia to ensure information security, as well as a number of scientific studies on the topic.

The topic chosen by us for research is poorly represented in the Russian scientific literature. Among domestic scientific research, one can single out works on the role of the Russian financial regulator in ensuring the information security of the banking and financial systems [9; 10], as well as

work on approaches to the development of the information-regulatory system of financial infrastructure [11].

3. Hypothesis

Ensuring the information security of the state is carried out by interacting institutions of the public and private sectors. In such a situation, representatives of the public sector are responsible for coordinating actions within a particular segment of the economy. The financial regulator performs the functions of coordinating and managing relations within the financial and banking sectors (Art. 3, 4) [7], therefore, determining its role in ensuring information security in the framework of the state program to create a digital environment that ensures the interaction of all participants in public and private sectors in all spheres of life, is scientifically and practically justified.

4. Results and discussion

Before determining the legal status of the Bank of Russia, it is necessary to dwell on the issue of the specifics of an object to which the powers of the financial regulator apply. We are talking about information systems of the banking and financial sectors that have the status of objects of critical information infrastructures (CII). Along with the information systems of the energy and transport sectors, they are the primary target of computer attacks from both the criminal community and the specialized public services of foreign countries. CII objects constitute a zone of responsibility of primarily specialized state institutions that perform functions to ensure national security [12, p. 55-57]. As we indicated above, the financial regulator is authorized by the state to establish rules for the activities of all financial institutions, including in the sphere of the safety of their operations [8, p. 26].

The special legal status of the Bank of Russia is established by the Constitution of the Russian Federation (Art. 75) [13], which entitles it as the sole subject of protection and ensuring the stability of the ruble as the monetary unit of the Russian Federation. It was established in 1990 as a successor of the Russian Republican Bank of the Soviet State Bank. The Federal Law of 10.07.2002 №86-FZ "On the Central Bank of Russian Federation (Bank of Russia)" (hereinafter - FZ-86) establishes the status of a financial regulator, indicating additionally such aims as the development and strengthening of the banking system of the Russian Federation; ensuring the stability and development of the national payment system; development and ensuring the stability of the financial market of the Russian Federation (Art. 3) [7]. Among the defined in Article 4 of the Federal Law-86 functions of the Bank of Russia those that are directly related to ensuring the security of the financial and banking sector should be mentioned: establishing rules for conducting banking operations and making settlements; currency regulation; currency control and banking supervision, as well as supervision in the national payment system; development and implementation of development policies and ensuring the stability of the financial market; analysis and forecasting of the state of the economy with the publication of relevant materials and statistical data; organization of the provision of services for the transmission of electronic messages on financial transactions.

In order to exercise its powers and to regulate the above mentioned relations, the Bank of Russia issues regulations that are binding on federal government bodies, state bodies of the constituent entities of the Russian Federation and local governments, all legal entities and individuals (Art. 7 of FZ-86). These acts take the form of instructions, provisions and notices.

Instructions determine the procedure for applying the provisions of federal laws and other regulatory legal acts (including regulatory acts of the Bank of Russia) on matters within the competence of the Bank of Russia, by establishing a set of rules governing the implementation of certain activities in a particular area of legal relations (clause 1.4.1) [14]. The provisions of the Bank of Russia establish the system-related rules on matters within the competence of the Bank of Russia (clause 1.4.2) [14]. Notice is a regulatory act issued to establish certain rules on issues falling within the competence of the Bank of Russia, as well as amending or declaring the regulatory acts or other acts of the Bank of Russia (clause 1.4.3) [14].

In addition to these regulations, the financial regulator may issue other non-regulatory acts: official clarifications; administrative acts; guidelines; regulations on structural divisions; acts containing exclusively technical formats and other technical requirements (clause 1.3) [14]. Some of them relate to ensuring the information security of the financial and banking sectors.

In order to ensure the exchange of electronic messages between the financial regulator and other entities conducting banking operations according to the law, the electronic information system of Bank of Russia was established that functions in accordance with the approved Regulation [15]. It includes the Bank's computing and technical centers equipped with hardware and software for the purpose of collecting, processing, storing and transferring administrative, economic, accounting, operating information, the payment information etc in accordance with the rules and conditions stipulated by the regulations and organizational and administrative documents of the Bank of Russia, and the agreements on exchange of information. The electronic information system of the Bank of Russia interacts with the telecommunications system of the Bank of Russia (clause 1.2) [15]. The information security of this system, along with the entire banking system of Russia, is ensured in accordance with the Bank of Russia Standard "Ensuring the Information Security of Organizations of the Banking System of the Russian Federation. General Provisions" [16], which consists of nine sections with the special sections devoted to 1) the initial conceptual scheme (paradigm) of the information security of organizations of the banking system; 2) the models of threats and violators of information security; 3) information security system; 4) information security management system; 4) verification and evaluation of information security.

In section 6 "Models of Threats and Violators of Information Security of Organizations of the Banking System of the Russian Federation" the standard defines the hierarchy of the main levels of information infrastructure that ensures the implementation of banking technologies: a) physical level (communication lines, hardware, etc.); b) network equipment (routers, switches, hubs, etc.); c) network applications and services; d) operating systems; e) database management systems; e) banking processes and applications; g) the organization's business processes (clause 6.2) [16].

There is also a list of the main sources of information security threats: 1) adverse events of a natural, technogenic and social nature; 2) terrorists and criminal entities; 3) dependence on suppliers / providers / partners / customers; 4) failures, destruction / damage of software and hardware; 5) employees of the organization of the banking system of Russia who implement threats to information security using the rights and powers legally granted to them (internal violators of information security); 6) employees of the organization of the banking system of Russia who implement threats to information security outside the rights and powers granted to them legally, as well as entities that are not employees of a bank institutions but who are attempting to grant an unauthorized access and to take unregulated actions within the framework of the powers granted (external violators of information security); 7) non-compliance with the requirements of supervisory and regulatory bodies, current legislation (clause 6.6) [16].

The standard also contains the lists of the most relevant threats at three main levels: 1) at the physical level, network equipment level and network application level (clause 6.7); 2) at the levels of operating systems, database management systems, banking technological processes (clause 6.8); 3) at the level of business processes (clause 6.9) [16].

Section 7 "Information Security System of Organizations of the Banking System of the Russian Federation" contains principles for the distribution of the rights of workers and clients to information assets of the organization of the banking system of Russia: a) "know your customer"; b) "know your employee"; c) "need to know"; d) "dual control" (clause 7.1.4). The standard establishes that within the framework of bank payment technological processes the following assets should be protected in the first place: 1) bank payment technological process; 2) billing information; 3) information related to the protected information in accordance with clause 2.1 of the Bank of Russia Regulation №362-P of June 09, 2000 "On the Requirements for Ensuring Information Security in Transfers of Funds and the Procedure for the Bank of Russia Ensuring Enforcement of Information Security Requirements for

Money Transfers" according to the Directive of the Bank of Russia of 05.06.2013 №3007-U (clause 7.1.9) [16].

The specified section of the standard contains general requirements for ensuring information security: a) when assigning and ensuring confidence in personnel (clause 7.2); b) automated banking systems at the stages of the life cycle (clause 7.3); c) in access and registration control (clause 7.4); d) anti-virus protection tools (clause 7.5); e) when using Internet resources (clause 7.6); e) when using tools for cryptographic protection of information (clause 7.7); g) banking payment processes (clause 7.8); h) banking information technology processes (clause 7.9); i) banking technological processes in which personal data are processed (clause 7.11), as well as general requirements for the processing of personal data in the organization of the banking system of the Russian Federation (paragraph 7.10) [16].

Section 8 "Information Security Management System of Organizations of the Banking System of the Russian Federation" sets out requirements for: 1) the organization and functioning of the information security service of an organization of the banking system of the Russian Federation (clause 8.2); 2) determining / correcting the scope of the information security system (clause 8.3); 3) selection / correction of the approach to risk assessment of information security breaches and conducting risk assessment of information security breaches (clause 8.4); 4) developing plans for processing information security breach risks (clause 8.5); 5) development / correction of internal documents regulating information security activities (clause 8.6); 6) the adoption by the management of the organization of the banking system of the Russian Federation of decisions on the implementation and operation of the information security system (clause 8.7); 7) the implementation of road maps for information security systems (clause 8.8); 8) development and organization of implementation of training and awareness-raising programs in the field of information security (clause 8.9); 9) the organization of detection and response to information security incidents (clause 8.10); 10) the organization of ensuring business continuity and its recovery after interruptions (clause 8.11); 11) monitoring information security and monitoring protective measures (clause 8.12); 12) conducting self-assessment of information security (clause 8.13); 13) conducting an information security audit (clause 8.14); 14) analysis of the functioning of the information security system (clause 8.15); 15) analysis of the information security system by the management of the organization of the banking system of the Russian Federation (clause 8.16); 16) making decisions on tactical improvements to the information security system (clause 8.17); 17) making decisions on strategic improvements to the information security system (clause 8.18) [16].

With regard to the verification and assessment of information security of organizations of the banking system of Russia, the following processes are provided and their characteristics are given: a) information security monitoring and protective measures control; b) self-assessment of information security; c) information security audit; d) analysis of the functioning of the information security system (including management) (clause 9.1) [16].

The Provisions on information protection requirements for money transfers and the procedure for the Bank of Russia to monitor compliance with information protection requirements when making money transfers №382-P is an another important tool for ensuring information security [17]. Its detailed analysis was conducted by O.A. Vasilenko in the research [10]. First of all one should note the key measures taken by the financial regulator such as the obligation of banks and money transfer operators to inform about hacker attacks, the obligation of banks to disclose financial damage from cyber attacks, mandatory certification of technical measures to protect information.

In the beginning of the year 2019 the financial regulator approved the Regulation on Information Protection Requirements in the Bank of Russia Payment System №672-P [18], which applies to information infrastructure facilities used to process the protected information listed in clause 2.1 of the Bank of Russia Regulation of June 9, 2012 №382-P: 1) on cash balances in bank accounts; 2) on electronic cash balances; 3) on completed transfers of funds, including information contained in notifications (confirmations) concerning the acceptance for execution of orders of participants of the payment system, as well as in notifications (confirmations) concerning execution of orders of participants of the payment system; the requirement to classify information on money transfers made to protected infor-

mation stored in operational centers of payment systems using payment cards or located outside the Russian Federation established by the payment system operator; 4) information that is contained in the cashless settlement of cash orders of the operators of money transfer operators, orders of the participants of the payment system, orders of the payment clearing center; 5) on payment clearing positions; 6) necessary for clients to certify the right to dispose of funds including information of holders of payment cards; 7) key information of the tools for cryptographic protection of information used in the transfer of funds (on cryptographic keys); 8) on the configuration that determines the parameters of the automated systems, software, computer equipment, telecommunications equipment, the operation of which is provided by the operator for the transfer of funds, the operator of payment infrastructure services, bank payment agent (subagent), and used to make money transfers, as well as information about the configuration that determines the parameters of the technical means of information protection; 9) restricted access information, including personal data and other information that is subject to mandatory protection in accordance with the legislation of the Russian Federation, processed when making money transfers [19].

As the additional cybersecurity instruments a number of standards should be noted [20; 21; 22] as well as the Bank of Russia Notice №3889-U on December 10, 2015 "On the Identification of Threats to the Security of Personal Data that are relevant to the processing of personal data in personal data information systems" [23].

It is necessary to highlight the special rules on outsourcing within the financial sector. The outsourcing is a transfer of performance of certain business functions on the basis of contractual relations to the external organizations providing relevant services (service providers). The financial regulator determines the following business functions for possible outsourcing: a) associated with the use of information technology, maintenance and administration of computer equipment, server and telecommunications equipment, self-service devices, and software development; b) administrative, including those related to financial activities, the functionality of the back-office, call-center, organizational and administrative support; c) associated with the storage and processing of information, including at external data centers and cloud services (cloud services); d) ensuring information security of the organization of the banking system of Russia; e) administrative ones [22]. The relevant standard consists of 12 sections and 3 annexes. The immediate requirements for outsourcing in terms of information security are contained in sections 5-12 (risk of breach of information security and basic requirements for managing such risk; risk assessment; task content and area of responsibility for the management of the organization of the banking system; requirements for assessing the service provider and outsourcing, monitoring and control of the risk of breach of information security in outsourcing, features of outsourcing information security processes).

Appendix 1 establishes the permissible types of international certification for information security: certification of the international association ISACA (Information Systems Audit and Control Association) and certification of the international information security consortium ISC (International Information Systems Security Certifications Consortium, Inc.). Appendix 2 contains a list of questions for evaluating the policy of the service provider regarding information security, and Appendix 3 contains examples of business functions that can be outsourced.

Direct operational management of information security is carried out through the Center for Monitoring and Responding to Computer Attacks in the Credit and Financial Sphere (FinCERT) - one of the structural units of the Information Security Department [24]. FinCERT carries out information interaction not only between the subjects of the financial system, but also the antivirus software developers, providers and telecom operators, as well as law enforcement and other government agencies in charge of the information security of the industry. In addition, FinCERT prepares analytical materials on the facts of cyber attacks and establishes recommendations in the field of information security in the implementation of money transfers [24] based on the provisions of a special standard on managing information security incidents [20].

The instruments issued by the Bank of Russia to regulate information security include its main aspects: protection of information systems, risk management, outsourcing, and contain not only a detailed list of organizational and legal measures but also a lot of technical regulations.

The aforementioned regulatory and institutional instruments define the financial regulator as the key, moreover, the only entity with broad powers to regulate financial relations.

The provisions of the Program that establish the scope and limits of Bank of Russia involvement in its federal projects are follows. The deputy heads of the following ministries were appointed as the project managers: Ministry of Economic Development of the Russian Federation - for the projects "Legal regulation of the digital environment" and "Human resources for the digital economy"; Ministry of Digital Development, Communications and Mass Communications of the Russian Federation - for the projects "Information Infrastructure", "Information Security", "Digital Technologies" and "Digital Public Administration" (Section 3) [3].

In the federal project "Legal regulation of the digital environment" the Bank of Russia is designated as the responsible executive body for the ensuring the legal conditions for the implementation and the use of innovative technologies in the financial market. As one of the results of this project the adoption of the federal law regulating the circulation of crypto currency and conducting ICO, determining the status of digital technologies used in the financial sphere and their concepts (clause 1.8) [3] by December, 31 2018 was indicated. To achieve this, the financial regulator interacted with the Ministry of Finance of Russia, the Ministry of Economic Development of Russia, the Ministry of Communications and Mass Media of Russia, the Skolkovo Foundation, the Autonomous non-profit organization "Digital Economy" and other interested federal executive bodies and organizations. The corresponding bill [25] was adopted by the State Duma of the Federal Assembly of the Russian Federation in the first reading on May 22, 2018, the expert opinion of the Presidential Council on the codification and improvement of civil legislation was delivered on November 29, 2018 and on March 20, 2019 the consideration of the draft bill was postponed by the State Duma of the Federal Assembly of the Russian Federation to another plenary session [26]. Another result within the framework of the federal project "Legal regulation of the digital environment" indicated the adoption of a federal law providing for the regulation of crowd funding activities (investment attraction activities using investment platforms) (clause 1.9) by December 31, 2018 [3]. The Ministry of Economic Development and Trade of the Russian Federation, the Ministry of Telecommunications and Mass Media, the Ministry of Finance of Russia, the Skolkovo Foundation, the Autonomous non-profit organization "Digital Economy" and other interested federal executive bodies and organizations were identified as co-executives with the Bank of Russia. The corresponding draft bill "On attracting investments using investment platforms" [27] was adopted in the first reading on May 22, 2018. The expert opinion of the Presidential Council on the codification and improvement of civil legislation on this draft bill was delivered on January 17, 2019 [28], [29].

The federal project "Information Infrastructure" maintains the Bank of Russia as a responsible body for the implementation of digital technologies and platform solutions in the sphere of government, business and society interactions. By December 31, 2023, the Bank of Russia together with Rostelecom to create a platform that provides for the exchange of information between the state, citizens, and commercial and non-profit organizations ("Digital Profile" infrastructure) (clause 1.66) [3].

It should be noted that representatives of the Bank of Russia are not involved in the work of the center of competence "Information Security", despite the fact that this center operates in 16 subgroups in the following areas: 1) stability and security of the unified telecommunication network of the Russian Federation (including the Russian segment of the Internet); 2) manageability and reliability of the network of the Russian segment of the Internet; 3) technological independence and security of the hardware and data processing infrastructure; 4) stability and security of the information systems and technologies; 5) the legal regime and technical tools for the functioning of services and the use of data; 6) the legal mode of machine-to-machine interaction for cyber-physical systems; 7) the legal mode of functioning of the machine and cognitive interfaces, including the Internet of things; 8) protection of the rights, freedoms and legitimate interests of the individuals in the digital economy; 9) technical

tools to ensure the safe information interaction of individuals in the digital economy; 10) protection of the rights and legitimate interests of business in the digital economy; 11) organizational and legal protection of state interests in the digital economy; 12) creation of effective mechanisms of state regulation and support in the field of information security while integrating the national digital economy into the international economy; 13) laying the foundations for building a trusted Eurasian Economic Union environment providing collective information security; 14) Russia's participation in the preparation and implementation of international documents on information security related to the digital economy; 15) legal support of the implementation of information security direction; 16) human resources and the information security [5]. Representatives of both the public and private sectors take part in the activities of these groups, but the financial regulator is not represented in any of them, which is in no way correlated with its capabilities and powers. In other countries the financial regulator plays the leading role in such processes. For example since 2017 the Monetary Authority of Singapore (MAS) together with the Singapore Cyber Security Agency (the central executive body responsible for ensuring information security at the state level) launched a cyber risk management project [29], in which representatives of public and private sectors take part. The project is conducted on the base of the Nanyang Technological University and is aimed to the systematic data collection and modeling of cyber risks with the further development of cyber risk assessment tools and the use of cyber risks insurance tools. Among the objectives of the project, the following should be noted: 1) development of the classification of cyber risks and appropriate response options for each jurisdiction; 2) the creation of data packets (big data) on damages from cyber incidents with a further transfer to the estimated insurance claims on the basis of a "standardized" set of specific contract wordings; 3) development of a set of cyber-event scenarios for quantitative impact assessment and studying the risk of accumulation in system events; 4) development of standard loss models for different cyber attack scenarios for actuarial calculations; 5) development of a methodology for non-interference assessment of the cybersecurity level of financial institutions to maintain their rating and integration with the underwriting processes [30].

That year the financial regulation authority of Singapore has formed the Cyber Security Advisory Panel (CSAP), consisting of leading international experts in the field of cyber security, appointed for 2 years with the possibility of extending membership. CSAP is developing guidelines for MAS and financial institutions to enhance the security of the financial system of Singapore. The current members of the commission include heads of cybersecurity divisions in such companies of financial services industry as Accenture Security, IronNet Cybersecurity Inc., JP Morgan Chase & Co, London Stock Exchange Group, F-Secure, PricewaterhouseCoopers Risk Services Pte Ltd, FireEye Inc, Standard Chartered Bank, CyberArk, IBM Resilient, and the head of the Singapore Cyber Security Agency [31]. CSAP holds consulting meetings with the Cybersecurity Standing Committee of the Association of Banks of Singapore, as well as with representatives of the Life Insurance Association and the Singapore General Insurance Association [32].

5. Conclusions

The Bank of Russia supervises all financial institutions, forms the financial system by maintaining a stable corporate governance system and strict adherence to international accounting standards. In order to ensure information security of the banking and financial sectors the Bank of Russia is authorized to adopt regulations that cover such important aspects of banking and financial activities as the protection of information infrastructure facilities and money transfers information, personal data security, outsourcing services, and others. A special Center for Monitoring and Responding to Computer Attacks in the Credit and Financial Sphere (FinCERT) ensures the information security in interaction of the subjects from the public and private sectors. Despite the serious constitutional and legal status and experience of practical management of processes to ensure the security of financial institutions, the potential of the financial regulator is not fully used in the National Program "Data Economy Russia 2024" although the tasks assigned to the center of competence "Information Security" are of a public nature and accordingly must be performed by the relevant subject. In our opinion, the Bank of Russia

should be defined as the center of competence of this project (alone or together with Sberbank of Russia), which is a logical continuation of the powers granted to it by the state.

References

[1] 2017 Strategy for the development of the information society in the Russian Federation for 2017-2030
[2] 2017 National program "Data Economy Russia 2024"
[3] 2018 Passport of the National Program "Data Economy Russia 2024"
[4] 2019 Regulation on the management system of the implementation of the national program "Data Economy Russia 2024"
[5] Information security 2019 Data Economy Russia 2024 Homepage https://data-economy.ru/security
[6] Razumnyi E 2018 Sberbank and the Central Bank argue over who is the main one in cybersecurity: the Central Bank wants some of the powers of Sberbank in the Data Economy Vedomosti Homepage https://www.vedomosti.ru/finance/articles/2018/10/31/785328-sberbank-i-tsb-sporyat
[7] 2002 Federal Law on the Central Bank of Russian Federation (Bank of Russia)
[8] Gorian E 2018 The role of the financial regulator in ensuring cybersecurity: Singapore's experience Financial Law and Management 2 25-38
[9] Aleksandrov V V, Malyi Yu V 2015 Application of the Bank of Russia Standard for Ensuring the Information Security of Organizations of the Banking System of the Russian Federation The Herald of Belgorod university of cooperation, economy and law **2(54)** 289-292
[10] Vasilenko O A 2018 Measures by the Central Bank of Russia to protect information in the financial sector *Science, techniques and education* **8(49)** 66-68
[11] Alekseev V N, Sharkov N N 2019 Approaches to the development of information and regulatory system of financial infrastructure Research Financial Institute *Financial Journal* **2(48)** 109-121
[12] Gorian E 2018 Institutional mechanisms of critical information infrastructure security in Russian Federation and Singapore: legal comparative aspect *Administrative and Municipal Law* **9** 49-60
[13] 1993 Constitution of Russian Federation
[14] 2017 Regulation of Bank of Russia on the rules of preparation of regulatory acts of Bank of Russia
[15] 2005 Regulation of Bank of Russia on the Electronic information system of Bank of Russia
[16] 2014 Standard of Bank of Russia "Ensuring the Information Security of Organizations of the Banking System of the Russian Federation General Provisions"
[17] 2012 Regulation of Bank of Russia on information protection requirements for money transfers and the procedure for the Bank of Russia to monitor compliance with information protection requirements when making money transfers
[18] 2019 Regulation of Bank of Russia on information protection requirements in the payment system of the Bank of Russia
[19] 2012 Regulation of Bank of Russia on the requirements for ensuring the protection of information during the transfer of funds and the procedure for the Bank of Russia to monitor compliance with the requirements for ensuring the protection of information during the transfer of funds
[20] 2018 Standard of Bank of Russia "Security of financial (banking) operations Information Security Incident Management About the forms and terms of interaction of the Bank of Russia with the participants of information exchange in identifying incidents related to the violation of requirements to ensure the protection of information"
[21] 2016 Standard of Bank of Russia "Ensuring information security organizations of the banking system of the Russian Federation Collection and analysis of technical data in response to

information security incidents in the implementation of money transfers"
[22] 2018 Standard of Bank of Russia "Ensuring information security organizations of the banking system of the Russian Federation Managing the risk of information security breaches in outsourcing"
[23] 2015 Notice of Bank of Russia "On the Identification of Threats to the Security of Personal Data that are relevant to the processing of personal data in personal data information systems"
[24] Center for Monitoring and Responding to Computer Attacks in the Credit and Financial Sphere (FinCERT) Bank of Russia Homepage https://www.cbr.ru/fincert/
[25] 2018 Draft federal bill №419059-7 "On digital financial assets"
[26] 2018 Passport of draft federal bill №419059-7 "On digital financial assets"
[27] 2018 Draft federal bill №419090-7 "On attracting investments using investment platforms"
[28] 2018 Passport of draft federal bill №419090-7 "On attracting investments using investment platforms"
[29] Alekseenko A P 2019 New Russian Model BIT and the Practice of Investment Arbitration Manchester *Journal of International Economic Law* **16(1)** 79-93
[30] Cyber Risk Management Project (CyRiM), Nanyang Technological University Homepage http://irfrc.ntu.edu.sg/Research/cyrim/Pages/Project-Brief.aspx
[31] MAS Sets Up International Advisory Panel for Cyber Security Monetary Authority of Singapore Homepage http://www.mas.gov.sg
[32] MAS' Cyber Security Advisory Panel Proposes Ways to Enhance Financial Sector Cyber Resilience Monetary Authority of Singapore Homepage http://www.mas.gov.sg