Bank of Russia

GUIDELINES FOR THE ADVANCEMENT OF INFORMATION SECURITY IN THE FINANCIAL SECTOR FOR 2019–2021

MOSCOW
2019

CONTENTS

This publication was prepared by the Information Security Department.
Cover photo: Shutterstock/FOTODOM
12 Neglinnaya Street, 107016 Moscow
Bank of Russia website: www.cbr.ru

INTRODUCTION

The Guidelines for the Advancement of Information Security in the Financial Sector for 2019–2021 (hereinafter, the Guidelines) set priority goals and objectives for improving information security and cyber resilience, including the following:

- information security and cyber resilience to enhance the financial stability of each financial market organisation;
- operational reliability and business continuity of credit and financial institutions;
- countering cyber attacks, including with the use of innovative financial technologies; and
- protection of financial service consumers' rights.

The Guidelines describe the prerequisites for and trends in the development of information security in the Russian financial sector, the Bank of Russia's objectives and priority activities in the area of information security and cyber resilience, as well as measures to be taken in this area.

The measures stipulated in the Guidelines were developed, among other things, to implement a range of particular objectives as part of the federal projects of the Digital Economy of the Russian Federation national programme approved by Minutes No. 8, dated 6 May 2019, of the meeting of the presidium of the Governmental Commission for Digital Development and Using Information Technology for Improving the Quality of Life and Conditions of Doing Business.

The Guidelines build on the following documents:

- Information Security Doctrine of the Russian Federation, approved by Decree of the Russian President No. 646, dated 5 December 2016;
- Strategy for the Development of the Information Society in the Russian Federation for 2017–2030, approved by Decree of the Russian President No. 203, dated 9 May 2017;
- Economic Security Strategy of the Russian Federation, approved by Decree of the Russian President No. 208, dated 13 May 2017;
- Guidelines for the Development of the Russian Financial Market in 2019–2021;
- Guidelines for Financial Technology Development in 2018–2020;
- Priority Areas of the Bank of Russia's International Activities in 2019–2021.

The Guidelines are in line with global experience and best practices applied in the area of financial market information security and information security risk (cyber risk) management. They were developed based on the experience of such institutions as the US National Institute of Standards and Technology (NIST), the Monetary Authority of Singapore (MAS), the European Banking Authority (EBA), the International Organization of Securities Commissions (IOSCO), the Committee on Payments and Market Infrastructures (CPMI) and the Basel Committee on Banking Supervision (BCBS).

PREREQUISITES AND TRENDS

Digital transformation creates multiple benefits for financial service consumers and, inherently increases the quality and speed of and the opportunities for interaction between financial service consumers and financial institutions, while causing additional risks.

The rise in cyber crime, primarily in the credit and financial sector, is a global trend that requires coordinated efforts by regulators, law enforcement agencies, credit and financial institutions and financial service consumers.

Large-scale cyber attacks inflict material economic damage, affect geopolitical relations and decrease the level of confidence in the internet.

Cyber attacks on digital financial systems can provoke a financial crisis.

The World Economic Forum's 2018 Global Risks Report defines cyber attacks as a type of global technological risk.

As a global trend, there has been an increase in financial losses from cyber attacks and a disruption of the integrity and continuity of operations, including in the financial market (17% of all cyber attacks occur in the financial sector). The elaborate methods, techniques and instruments used to commit cyber attacks demand that regulators take flexible and prompt action and use innovative digital technologies and work methods.

The USA, Canada, Singapore, Australia, Malaysia, New Zealand, Japan, the UK and Austria are the countries best prepared to counter cyber attacks, which makes them the most attractive to financial service consumers and accelerates their economic development.

The key risks in the credit and financial area are as follows:

- financial losses of clients (financial service consumers) undermining confidence in modern financial technologies;
- financial losses of individual financial institutions that may have a material negative (critical) impact on their financial standing;
- disruption of the operational reliability and continuity of financial services causing reputational damage and growing social tension;
- a potential systemic crisis in the case of information security incidents in institutions that are critical to the financial market.

The International Organization of Securities Commissions (IOSCO) set the following criteria for the proper functioning of critical financial market infrastructure:

- the capability to restore operations within two hours after disruption; and
- the capability to perform settlements on due dates and to ensure the completeness of transactions.

According to the Bank of Russia's Financial Sector Computer Emergency Response Team (Bank of Russia's FinCERT),[1] in 2018 unauthorised transactions in corporate accounts amounted to 1.469 billion rubles (vs nearly 1.57 billion rubles in 2017, nearly 1.89 billion rubles in 2016 and nearly 3.7 billion rubles in 2015).

[1] *According to the data of the mandatory reporting on information security incidents officially submitted by credit institutions to the Bank of Russia and the data obtained within the information exchange organised by the Bank of Russia's FinCERT.*

In 2018, unauthorised transactions with the use of payment cards[2] issued by Russian credit institutions carried out in Russia and abroad totalled 1.384 billion rubles (vs 0.961 billion rubles in 2017, 1.08 billion rubles in 2016 and 1.14 billion rubles in 2015).[3]

In 2018, such transactions accounted for 0.0018% of the total amount of transactions with the use of payment cards issued by Russian credit institutions[4] (1.8 kopecks per 1,000 rubles of money transferred).

Meanwhile, the maximum allowable percentage of unauthorised money transfers stipulated by the European Banking Authority (EBA) equals 0.005% (5 euro cents per 1,000 euros of money transferred).

No incidents leading to critical damage in systemically important credit and financial institutions have been registered in the Russian Federation. However, there was a number of incidents disrupting the continuity of financial services and, consequently, causing a growth in social tension. Information security incidents in small and medium-sized financial institutions may result in the termination of their business.

According to the findings of the analysis of attempted thefts of credit institutions' funds, the amount of funds exposed to the risk of theft is comparable to the average daily balance of a credit institution's correspondent account opened with the Bank of Russia, plus the average daily receipts into the given correspondent account.

For small and medium-sized financial institutions, this amount of funds is often comparable to their equity (capital).

Prerequisites for a greater importance of the development of information security in the Russian financial market are formed by the following trends:

- the development speed of the digital financial service sector for promoting the convenience and quality of such services in order to improve the competitiveness;
- the proactive stance of the country's leadership regarding the creation of a digital ecosystem promoting the development of financial technologies;
- the increased importance of the protection of financial service consumers' rights against financial losses and, consequently, a greater confidence in the Russian financial system;
- the integration of information security risk (cyber risk) indicators in the list of key risks of financial institutions; and
- the growing scale of cyber crime, primarily in credit and finance.

The development of the digital environment is inextricably linked to the application of continuously emerging breakthrough and advanced digital technologies.

The key digital technology-based infrastructure projects for which the Bank of Russia sets information security requirements in the first place are as follows:

- remote identification platform (Unified Biometric System);
- Faster Payments System;
- Marketplace platform;
- digital customer profile.

---

[2] *Hereinafter, payment cards comprise settlement, credit and prepaid cards.*

[3] *According to the data of the reporting on unauthorised payment card transactions submitted by credit institutions to the Bank of Russia. The increase in the amount of losses inflicted by unauthorised transactions was due to the higher reliability of the data provided in the reporting forms and the formation of an organisational and legal foundation for the prompt data exchange.*

[4] *According to the data of the reporting on payment cards and electronic funds submitted by credit institutions to the Bank of Russia.*

In the future, the digital transformation will cause major alterations in financial service technologies. Therefore, guided by the global development trends, the Bank of Russia should elaborate new approaches to ensuring the financial ecosystem's information security and cyber resilience in the following conditions:

- changes in the system architecture (use of distributed ledger technology);
- remote access to financial services and wide usage of mobile technologies;
- application of new advanced technologies for information security and cyber resilience purposes (Big Data, artificial intelligence);
- the Internet of Things as an element of the payment space.

THE BANK OF RUSSIA'S OBJECTIVES AND PRIORITY ACTIVITIES IN INFORMATION SECURITY

- The Bank of Russia's Guidelines stipulate the following objectives in the information security and cyber resilience area.

1) Cyber resilience:
   - ensuring that the credit and financial sector can guarantee financial stability and operational reliability in the case of cyber attacks, including the operational reliability and continuity of financial and banking services;
   - controlling the levels of risk of information security incidents;
   - controlling the amount of unauthorised banking and financial transactions;
   - monitoring and prevention of and prompt response to cyber attacks against credit and financial institutions.
2) Protection of financial service consumers' rights by monitoring financial loss indicators.
3) Promoting the development of innovative financial technologies by controlling the levels of risk of information security incidents and ensuring adequate information security.

To achieve the above objectives, the Bank of Russia established its Information Security Department which, among other things, performs the functions of the Competence Centre for Information Security in Finance.

The Competence Centre elaborates the methodology for, and ensures the advancement of information security in the credit and financial sector with account for global trends in the following major areas:

1) Standardisation:
   - development of information security and cyber resilience standards (including GOST standards) and organisation of the work of Subcommittee No. 1 of Technical Committee No. 122 'Financial (Banking) Transaction Standards' of the Federal Agency on Technical Regulating and Metrology;
   - ensuring the participation of Bank of Russia standardisation experts in the work of international organisations.
2) Interdepartmental communications on information security issues.
3) National programme 'Digital Economy of the Russian Federation':
   - engagement of the Bank of Russia's Financial Sector Computer Emergency Response Team (FinCERT) as a leader in the implementation of the Digital Economy of the Russian Federation national programme in the Information Security domain and in countering cyber attacks;
   - participation in the integrated system for combating cyber threats and in preparations for countering cyber attacks in the credit and financial sector;
   - elaboration of information security requirements for innovative technologies;
   - engagement in the development of the import substitution programme and in the analysis of the risk associated with the usage of foreign-made infrastructure components.
4) Supervision over the information security risk (cyber risk) level in credit and non-bank financial institutions and national payment system participants.
5) Countering the dissemination in the credit and financial sector of information on illegal market players' operations and services.
6) Building an environment for promoting a culture of information security and cyber hygiene in credit and finance.

GENERAL

The Bank of Russia's activities in the information security and cyber resilience area (area of regulation) encompass the following entities:[5]

- credit institutions conducting banking operations;
- financial institutions carrying out financial transactions in accordance with Article 76 of Federal Law No. 86-FZ, dated 10 July 2002, 'On the Central Bank of the Russian Federation (Bank of Russia)';
- national payment system participants carrying out money transfers,

as well as the following objects:

- innovative financial technologies.

The general principle for credit and financial institutions' information security and cyber resilience is to ensure information security at the following levels:

- security of infrastructure, or the infrastructure level,
- security of application software, or the application level,
- security of data processing technologies, or the data technology level,

as well as the logging of actions and operations (transactions).

The fundamental principles are to be implemented based on the following methodological approaches:

- at the infrastructure level – the application of the package of the state standards elaborated by Subcommittee No. 1 of Technical Committee No. 122 'Financial (Banking) Transaction Standards';
- at the application level – control for the absence of software vulnerabilities, including those associated with programming bugs;
- at the data technology level – ensuring the integrity and authenticity of information processed;
- action and operation logging to the extent sufficient for supervision purposes, data exchange for countering cyber attacks and follow-up activities of law enforcement authorities.

[5] *Except Bank of Russia divisions.*

LEGAL REGULATION

To ensure information security in the financial market, it is necessary to build a legal framework comprising, among other things, the Bank of Russia's powers to take part in organising information security and to establish regulatory requirements for financial market participants.

The legal framework for ensuring information security in the financial market shall guarantee the predictability of the exercise of the Bank of Russia's powers and the predictability of supervision over financial market participants' compliance with the requirements.

As of now, pursuant to the Information Security Doctrine of the Russian Federation approved by Decree of the Russian President No. 646, dated 5 December 2016, the Bank of Russia is the authority providing the organisational basis for the Russian information security system, and credit and financial institutions are participants in the system.

In accordance with Articles 57.4 and 76.4-1 of Federal Law No. 86-FZ, dated 10 July 2002, 'On the Central Bank of the Russian Federation (Bank of Russia)' (as amended) (hereinafter, the Law on the Bank of Russia), the Bank of Russia, upon coordination with the Federal Security Service of Russia and the Federal Service for Technical and Export Control of Russia, sets information protection requirements for:

- credit institutions in banking operations;
- non-bank financial institutions carrying out operations in financial markets provided for by Part 1, Article 76.1 of the Law on the Bank of Russia.

Article 27 of Federal Law No. 161-FZ dated 27 June 2011 'On the National Payment System' obliges money transfer operators, bank payment agents (subagents), payment system operators and payment infrastructure service operators to ensure information protection when they transfer funds.

The Law on the Bank of Russia establishes the regulatory powers of the Bank of Russia in the information security and information protection area, as regards:

- transferring funds and conducting banking and financial operations;
- maintaining a database on actual and attempted unauthorised money transfers;
- information exchange between credit and financial institutions and the Bank of Russia's FinCERT in accordance with Parts 6 and 7, Article 27 of Federal Law No. 161-FZ dated 27 June 2011 'On the National Payment System' (as amended).

Proportionate regulation in the information security and cyber resilience area is expected to be delivered as follows:

1) Detection on the internet of websites used to commit fraud in credit and finance and restriction of financial service consumers' access to such websites to the extent stipulated by the Constitution of the Russian Federation and federal laws, which requires the Bank of Russia to have the powers to:
   - Block on the internet:
     - phishing websites;
     - websites where financial services are offered and/or rendered by subjects not entitled to provide them according to the applicable laws;
     - websites used to disseminate information about financial pyramid schemes raising funds and other assets from individuals and legal entities.
     - Block malware websites on the internet through pre-judicial processes.

2) Countering fraud in finance through the creation of a single channel for telecommunications providers and banks and non-bank financial institutions, including microfinance organisations, to exchange data on mobile devices and mobile subscribers (which is important, for instance, when a SIM card or mobile number owner changes or when a mobile device is suspected to have been infected).

3) As part of the efforts aimed at improving the mechanisms of using enhanced certified digital signatures and the laws governing certification centres' activities, the Bank of Russia is developing comprehensive proposals for building a single system of certification centres in credit and finance where the Bank of Russia's certification centre will become the lead centre for the entire financial market.

4) Creating conditions for the safe turnover of digital financial assets through the establishment of proportionate requirements for information security and information protection in this area. The proportion of the information protection requirements set by the Bank of Russia will depend on the level of risks, the scope and nature of operations carried out by credit and financial institutions, and the level and combination of risks inherent in their business.

5) The coordination of financial market participants' activities for implementing the measures of the federal projects within the Digital Economy of the Russian Federation national programme aimed at elaborating approaches to regulating the requirements for the application of digital technologies in the financial market with account for safety requirements (e.g., digital financial assets, artificial intelligence, Big Data, cyber physical systems, distributed ledger platforms, etc.) are separate areas within the Digital Economy of the Russian Federation national programme.

ENSURING THE INFORMATION SECURITY AND CYBER RESILIENCE OF INFRASTRUCTURE

Ensuring the security and resilience of computing infrastructure is an infrastructure-related task which is intended to be addressed through applying the package of the state standards being elaborated by Subcommittee No. 1 of Technical Committee No. 122 'Financial (Banking) Transaction Standards'.[6]

The level of protection of credit and financial institutions' computing infrastructure (ecosystem) is planned to be assessed in a comprehensive way for each category of entities supervised by the Bank of Russia, with account for the type and scope (proportionate regulation) of their business.[7] In addition, it is planned to legally oblige financial institutions to submit to the Bank of Russia their data on the amount of unauthorised transactions as a ratio of the total amount of transactions. In calculating this figure, they shall not take into account transactions carried out without a client's consent in the cases provided for by federal laws or Bank of Russia regulations, nor by contract.

The Bank of Russia develops requirements for assessing the protection level within the elaboration of the information security methodology.

The methodological basis for information protection at the infrastructure level is the package of the following state standards:

- RM domain – 'Cyber Attack Risk Management';
- IP domain – 'Information Protection at Financial Institutions';
- IM&SA domain – 'Information Security Incident Management and Cyber Situation Awareness';
- OR domain – 'Ensuring Operational Reliability';
- MO domain – 'Cyber Attack Risk Management in Outsourcing and Outsourced Information Services'.

The methodology is being elaborated to enhance the set of the sectoral documents establishing the information security and cyber risk management requirements in order to build the fundamentals for the efforts of the Bank of Russia and credit and financial institutions in combating urgent information security threats, cyber attacks and cyber crime.

The core information security and information protection principles stipulated in the package of the state standards are as follows:

- mandatory application of the standardisation documents being drawn up by the Bank of Russia;
- implementation of a risk-focused approach to ensuring the compliance with the state standards;
- usage of the FinCERT's services to coordinate credit and financial institutions' activities and increase their cyber resilience.

The main instrument of the package of the sectoral documents on information security at the infrastructure level will be the GOST R Standard 'Security of Financial (Banking) Operations. Information Security Risk Management. General Provisions' that will stipulate:

---

[6] *Order of the Federal Agency on Technical Regulating and Metrology No. 1759, dated 21 August 2017, 'On Organising the Work of the Technical Standardisation Committee 'Financial (Banking) Transaction Standards'.*

[7] *In accordance with Bank of Russia Regulation No. 683-P, dated 17 April 2019, 'On Mandatory Requirements for Credit Institutions to Ensure Data Protection in Banking to Counter Unauthorised Funds Transfers' and Bank of Russia Regulation No. 684-P, dated 17 April 2019, 'On Mandatory Requirements for Non-bank Financial Institutions to Ensure Data Protection in Operations in Financial Markets to Counter Illegal Financial Transactions', credit institutions and non-bank financial institutions must comply with the mandatory requirements for information protection in accordance with National Standard of the Russian Federation GOST R 57580.1-2017 'Security of Financial (Banking) Operations. Information Protection of Financial Organisations. Basic Set of Organisational and Technical Measures' (approved by Order of the Federal Agency on Technical Regulating and Metrology No. 822-st, dated 8 August 2017) to come into force on 1 January 2021.*

- the corporate governance framework for ensuring information security and cyber resilience;
- the scope and content of processes and key activities for ensuring information security in all domains;
- a common (uniform) terminology to be used in all sectoral documents on information security;
- classification of information security levels (protection levels) – classification of the scope and content of the information security requirements and measures for their fulfilment.

Three protection levels are expected to be established – minimal, standard and increased. The protection level for a particular financial institution type is to be set with account for:

- the activity type of a financial institution, the range of its financial services, its business processes and/or technological processes;
- the amount of financial transactions;
- the importance of a financial institution for the financial market and the national payment system.

The target indicator for the accomplishment of the standardisation stages is the formalisation in 2021 of a complete package of the state standards.

ENSURING THE INFORMATION SECURITY AND CYBER RESILIENCE OF APPLICATION SOFTWARE

To ensure control for the absence of software vulnerabilities, including those associated with programming bugs which may enable successful cyber attacks, it is critical to create organisational and technical conditions for financial institutions to analyse vulnerabilities in the software they use to transfer funds (or conduct other financial transactions) and to identify the software that should be analysed.

The methodological basis for ensuring software security comprises:

- the security profile currently being developed by the Bank of Russia for assessing vulnerabilities in banking applications used to transfer funds, which includes requirements for vulnerability analysis and control over undeclared features, within the methodology of National Standard of the Russian Federation GOST R ISO/MEK 15408-3-2013 'Information Technology. Security Techniques. Evaluation Criteria for IT Security. Part 3. Components of Confidence in Security' approved by Order of the Federal Agency on Technical Regulating and Metrology No. 1340-st, dated 8 November 2013 'On Approving the National Standard';
- the use of the certification system of the Federal Service for Technical and Export Control of Russia (test laboratories and certification authorities) to perform quality control of software provided by a credit institution or non-bank financial institution to its clients for conducting financial transactions and to analyse this software for vulnerabilities based on the provisions of the security profile;
- building an ecosystem to analyse the protection level of the information infrastructure used to transfer funds that comprises entities with the required competencies and developers.

The target indicators are as follows:

- the certification system of the Federal Service for Technical and Export Control of Russia shall be stipulated in laws and regulations as the system for performing software quality control;
- completion of the security profile development;
- creation of an ecosystem for analysing the information infrastructure protection level.

ENSURING THE INFORMATION SECURITY AND CYBER RESILIENCE OF DATA TECHNOLOGIES

The security of digital technology-enabled data processing is an objective that will be handled individually as applicable to each specific financial technology.

The implementation of the security requirements for data technologies shall ensure the integrity and authenticity of the information being processed.

The security requirements for data technologies used to transfer funds (or conduct other financial transactions) are as follows:

- ensuring the integrity and authenticity of information at each data processing stage;
- interaction with financial institutions' clients;
- logging of operations at all process stages, including for analysing data on risk levels at each process stage;
- maintaining databases on information security incidents, including based on complaint management.

The key technological measures for information security and information protection are as follows:

- using electronic signature (cryptographic) tools;
- implementing the dual control principle in processing protected information;
- multi-factor client authentication, which includes the use of data encryption tools;
- implementing mechanisms for clients to receive requests for additional confirmation of financial transactions.

The target indicator is the time period for developing data technology security requirements for each particular new financial technology (no more than 1 month), with account for the application of a proactive (preventive) model.

ENSURING THE INFORMATION SECURITY AND CYBER RESILIENCE OF FINANCIAL TECHNOLOGIES

Digital financial technologies promote the development of the financial market, better financial inclusion and higher competition, on the one hand, but they also involve new information security risks, on the other hand. As digital technologies evolve, new cyber threats emerge, requiring prompt and timely detection and assessment and the development of adequate measures to prevent them and mitigate potential consequences.

Taking into account foreign best practices, the Bank of Russia is elaborating information security and operational reliability requirements for financial technologies for the following key domains and objectives in accordance with the Guidelines for Financial Technology Development in 2018–2020:

1) Legal regulation on information security and operational reliability issues is established by the federal laws being drawn up.

2) Building and enhancing the following elements of secure and resilient financial infrastructure:
   - remote identification platform;
   - Faster Payments System;
   - Marketplace platform;
   - financial transaction registration platform;
   - Bank of Russia payment system;
   - national payment card system;
   - financial messaging system;
   - cloud service platform;
   - distributed ledger technology-based platform.

3) Scrutinising, analysing and developing information security requirements for the following financial technologies:
   - RegTech (regulatory technology), SupTech (supervision technology);
   - Big Data, Smart Data;
   - mobile technologies;
   - artificial intelligence, robotics and machine learning;
   - biometrics;
   - distributed ledger technology;
   - Open API.

4) Expert assessment of projects within the Bank of Russia's regulatory platform pursuant to Bank of Russia Order No. OD-846, dated 3 April 2018, 'On the Procedure for the Bank of Russia to Organise and Carry Out Modelling of Processes Related to the Provision (Application) of Innovative Products, Services and Technologies in Banking and Other Financial Market Areas'.

The Bank of Russia carries out the validation of innovative financial technologies, products and services within its regulatory platform, taking into account the comprehensive analysis of information security risk (cyber risk) and how threat models emerge when these innovations are used.

The key RegTech projects in the area of financial institutions' information security and cyber resilience are as follows:

- Creation of a system (environment of confidence) for the independent assessment of compliance with the information protection requirements in money transfers (compliance assessment) through the accreditation of compliance assessment organisations and control over the quality of their work, primarily by the Bank of Russia. Compliance assessment involves

an independent evaluation of the infrastructure and application protection level according to the universal package of the state standards.

- Implementation of initiatives for the wide use of cryptography in the financial market to ensure the security of digital technology-enabled data processing in collaboration with the competent security agency.[8]
- Exchanging data on cyber threats between credit and financial institutions by developing an information exchange with the Bank of Russia's Financial Sector Computer Emergency Response Team and supporting the operation of the payment and financial transaction monitoring system.
- Multi-factor authentication of financial institutions' clients, which includes the use of data encryption tools, when conducting and confirming payment and financial transactions formed in an untrusted environment (an environment beyond the control of a financial institution).

The key SupTech (supervision technology) projects in the area of financial institutions' information security and cyber resilience are as follows:

- Building the Bank of Russia's anti-fraud system to monitor transactions in the Bank of Russia payment system, detect signs of money transfers not authorised by Bank of Russia payment system participants, deliver confirmation to participants and reveal signs of withdrawal of funds.
- Supervision by the Bank of Russia over financial institutions' compliance with the information security and cyber resilience requirements. Within this area, it is planned to legally oblige financial institutions to submit to the Bank of Russia their data on the amount of unlawful transactions not authorised by clients as a ratio of the total amount of transactions. Data collection as part of the assessment of compliance with the information security and cyber resilience requirements and the proactive identification of operational and financial stability indicators are the basic approach to remote supervision and, accordingly, to the evaluation of the information security risk (cyber risk) level.

[8] *Within the implementation of the Information Security federal project, the Digital Economy of the Russian Federation national programme and Bank of Russia Regulation No. 382-P, dated 9 June 2012, 'On the Requirements to Protect Information Related to Funds Transfers and on the Procedures for the Bank of Russia to Control the Compliance with the Requirements to Protect Information Related to Funds Transfers'.*

STAFF TRAINING AND PROMOTION OF CONSUMER CONFIDENCE IN THE DIGITAL ENVIRONMENT

Competent specialists possessing relevant knowledge and skills are required to establish up-to-date information security requirements in the existing digital environment.

However, staff training programmes and the level of staff qualification do not meet credit and financial institutions' needs, and employees lack new basic digital competencies.

In view of the above, the Bank of Russia is going to act as a connecting link between universities and credit and financial institutions so as to create adequate conditions for training new-generation information security specialists.

Based on credit and financial institutions' proposals within the implementation of the Information Security federal project and the Digital Economy of the Russian Federation national programme, the Bank of Russia plans to work out training areas and develop respective training programmes, namely to:

- develop the professional standard 'Information Security Specialist for Credit and Financial Institutions';
- assess credit and financial institutions' needs for information security specialists;
- elaborate proposals on amending the state higher education standards as regards training of information security specialists for credit and financial institutions;
- develop the framework professional retraining programme 'Ensuring Information Security at Credit and Financial Institutions'.

In addition, the Bank of Russia intends to elaborate methodologies and programmes for certification of employees and heads of information security (cyber security) divisions both in-person at the Bank of Russia University and remotely (using web-based remote access technologies).

In order to raise the level of engagement of Bank of Russia security specialists and credit and financial institutions in the staff training process, the Bank of Russia plans to involve them in the educational process as lecturers of the specialised departments of leading higher education institutions.

People's confidence in the digital environment and personal cyber security in the digital world will be promoted as part of the improvement of financial literacy and basic cyber hygiene skills. The Bank of Russia is going to elaborate educational programmes for financial institutions' representatives, students of higher education institutions, schools and other training organisations.

Launching a cyber laboratory (cyber training ground) for on-site training of employees working in the credit and financial sector and the Bank of Russia. A cyber training ground is planned to be created as a platform for modelling credit and financial institutions' infrastructure for emulating cyber attacks in order to work out preventive and counter measures and to carry out cyber security trainings.

Consistent work aimed at improving people's financial literacy, in particular at raising consumers' awareness of the payment service security rules (hereinafter, digital financial literacy), is an objective of the Bank of Russia's Information Security Department (Clause 2.2.1.5 of the Regulation on the Information Security Department). People's insufficient knowledge and skills in the area of safe usage of electronic payment tools and continuously emerging new ways to defraud citizens by deceit or abuse of trust for stealing their funds (hereinafter, social engineering) that are employed by malefactors to unlawfully gain access to credit and financial institutions' client accounts are the main reasons for a growing number and amount of unauthorised transactions.

The Information Security Department is an information and coordination hub for the processes and measures aimed at enhancing people's digital financial literacy and, in order to address this task, it engages other Bank of Russia divisions and market players, as well as competent federal executive authorities in charge of awareness raising measures, social protection and law enforcement.

INTERNATIONAL COOPERATION

Global cyber security threats require nations to join their efforts as long as these threats are cross-border, disrupt existing business models and cause new challenges in international economic relations.

The Bank of Russia stipulates its competent participation in the development of an up-to-date agenda meeting Russia's interests as a key goal within the international cooperation in the area of information security and cyber resilience.

The main objectives comprise cyber threat data exchange, assistance in the implementation of uniform standardised approaches to ensuring cyber security, as well as sharing the experience in the regulation and deployment of financial technologies.

Despite geopolitical factors, the Bank of Russia takes part in the international cooperation enhancing and expanding it in the following domains:

1) Ensuring Bank of Russia experts' involvement in international organisations' cyber security efforts ('Multilateral Cooperation'). The key sites are the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), the International Telecommunication Union (ITU), the International Organization of Securities Commissions (IOSCO), the Financial Stability Board (FSB), the World Economic Forum (WEF), the Committee on Payments and Market Infrastructures (CPMI), the International Association of Insurance Supervisors (IAIS) and the Basel Committee on Banking Supervision (BIBS). The collaboration with the BRICS partners is also a promising area of cooperation.
2) Communication with foreign central (national) banks on the issues of sharing cyber threat information and enhancing the cyber security of financial services ('Bilateral Cooperation'). The key partners of the Bank of Russia are the Bank of Italy, the Bank of Spain, the Central Bank of the Republic of Turkey and the National Cooperative Bank of India.
3) Communication with the regulators of the Eurasian Economic Union member states ('Integration Cooperation') in order to coordinate the efforts of the regulators' security divisions in creating cyber incident response centres at the national banks of the EAEU member states and align the approaches to elaborating information security and cyber resilience requirements and developing the EAEU payment space and an environment of confidence.
4) Communication with international incident response teams, stress tests and cyber trainings (the global Forum of Incident Response and Security Teams, the European ATM Security Team, the Domain Name and IP Address Management Corporation, the global community of Computer Emergency Response Teams, the Computer Emergency Response Teams of Israel, Spain, the Nordic countries, Bulgaria, India, the Netherlands and Japan).

NATIONAL PROGRAMME 'DIGITAL ECONOMY OF THE RUSSIAN FEDERATION'

Efficient development of the financial market in the digital economy is only possible with mature infrastructure elements of the digital economy (information infrastructure and information security).

Information security is a key area of the Digital Economy of the Russian Federation national programme.

The main goal in this area is to ensure the appropriate protection of every person, the society and the country against internal and external information security threats.

The Bank of Russia is the connecting link on information security issues between credit and financial institutions and the competent information security authorities (the Federal Security Service of Russia and the Federal Service for Technical and Export Control of Russia) and takes part in the implementation of the Information Security federal project in the following domains:

- development of important payment systems and ensuring their information security and cyber resilience (including through using Russian cryptographic tools);
- elaboration of approaches to ensuring information security and cyber resilience of innovative technologies (artificial intelligence, Big Data, cyber physical systems, distributed ledgers, the Internet of Things, etc.);
- training of competent information security and cyber resilience specialists for credit and financial institutions.

The use of Russian cryptographic technologies within the development of important payment systems and ensuring their information security and cyber resilience are a priority for the Bank of Russia.[9]

For this purpose, the Bank of Russia, with the engagement of the Federal Security Service of Russia, credit institutions and national payment system participants, plans to:

- address legal and administrative barriers hindering the wide use of cryptographic tools in the Russian financial market;
- create money transfer process charts describing cryptographic algorithms, specifying cryptographic primitives, with account for the functioning of international payment systems;
- develop cryptographic algorithms;
- develop certified software and hardware according to the roadmap that enable the application of data encryption tools (DETs);
- carry out certification of software and hardware for the compliance with the requirements of international payment systems;
- establish a hardware and software testing centre.

The Bank of Russia intends to improve the mechanisms of legal regulation of information security and cyber resilience of advanced technologies that were developed as part of the Information Security federal project within the Legal Regulation of the Digital Environment federal project of the Digital Economy of the Russian Federation national programme.

[9] *In furtherance of Bank of Russia Ordinance No. 4793-U, dated 7 May 2018, 'On Amending Bank of Russia Ordinance No. 382-P, Dated 9 June 2012, 'On the Requirements to Protect Information Related to Funds Transfers and on the Procedures for the Bank of Russia to Control the Compliance with the Requirements to Protect Information Related to Funds Transfers'.*

COMPETENCE CENTRE FOR INFORMATION SECURITY AND COUNTERING CYBER ATTACKS IN CREDIT AND FINANCE

Pursuant to Resolution of the Security Council of the Russian Federation No. PR-73, dated 15 January 2015, the Bank of Russia established its Financial Sector Computer Emergency Response Team – FinCERT of the Bank of Russia's Information Security Department.

The Bank of Russia's FinCERT develops information security and cyber resilience as follows:

1) Performs the functions of a sectoral segment of the State System for Detecting, Preventing and Eliminating Consequences of Computer Attacks on Information Resources of the Russian Federation (GosSOPKA).

2) Organises and coordinates credit and financial institutions' activities as the Competence Centre for Countering Cyber Attacks:
   - automated collection of information on all incidents in supervised entities;
   - efficient technical analysis and expert assessment, including computer inspections and reviews of malware;
   - prompt dissemination of information on incidents and incident response rules.

3) Performs the functions of the Coordination Centre for Blocking Unauthorised Funds Transfers in the Bank of Russia payment system and in other payment systems.

4) Blocks phishing resources and resources distributing malware, telephone numbers and SMS mailing lists used for fraudulent purposes.

5) Collaborates with foreign central (national) banks (including of the EAEU member states) on cyber attack monitoring and response issues.

6) Cooperates with global cyber attack response centres.

7) Promotes financial literacy and cyber hygiene.

8) Interacts with operators conducting transfers of digital financial assets.

The target indicators are as follows:

Target indicator	2018	2020
Level of confidence*	60%	80%
Ratio (percentage) of unauthorised financial transactions**	0.005%	0.005%

** To evaluate the level of client confidence, in December 2018, the FinCERT carried out a survey of credit institutions and their clients (hereinafter, the Survey).*
Credit institutions and their clients filled in questionnaires.
Each credit institution filled in the questionnaire based on the data of at least 100 of its clients of the following categories:
– at least 20 questionnaires from legal entities;
– at least 20 questionnaires from individuals of all age groups (by age group: under 25 years old, 25–40 years old, 40–60 years old, and 60+ years old).
The questionnaire for clients also contained the following question: 'How confident are you (as a client of a credit institution) in the security of financial services you receive?'
As long as clients were polled directly by credit institutions, the level of client confidence was calculated using an adjustment factor.
The level of confidence in 2018 was 68.53%, which demonstrates a fairly high awareness of the security of applied electronic technologies and services and exceeds the target value for the indicator.
*** The ratio (percentage) of unauthorised financial operations (transactions) is calculated as the ratio of unauthorised payment card transactions in the total amount of payment card transactions.*

SUPERVISION

The Bank of Russia exercises its control and supervision powers with account for the best world experience accumulated by international organisations, including the Financial Stability Board (FSB).[10]

The general principles for control and supervision in the information security and cyber resilience area are as follows:

1) Obtaining objective data (metrics, indicators) characterising the level of information security risk (cyber risk) for managing information security risk (cyber risk) in every credit and financial institution:
   - implementation of a compliance assessment system (independent assessment of supervised institutions for their compliance with the state standards: information protection, business continuity, risk management and outsourcing);
   - a system for assessing the quality of fulfilment of the software security requirements. This assessment is to be based on the analysis of vulnerabilities in software where vulnerabilities are critical (certification of client applications and front-end applications);
   - organising the collection of primary data characterising the level of financial transaction risk within the data collection technology and the application of the Big Data technology to proactively detect risk concentration points;
   - developing the methodology for and subsequent stipulation in laws and regulations of stress testing (cyber training) practices for credit and financial institutions.
2) Developing the methodology for calculating minimum provisions for potential losses that might be caused by cyber risk incidents (e.g., additional requirements for credit institutions' capital, independent guarantees and insurance).
3) Obtaining objective data (metrics, indicators) on financial service consumers' financial losses and elaboration, on the basis of those data, of a strategy for financial consumer rights protection.
4) Assessing the financial stability of the Russian financial market in general based on the data on information security risks (cyber risks).

Another role of the Bank of Russia is the global promotion of advanced techniques and approaches to elaborating the control (supervision) methodology in the information security and cyber resilience area.

The target indicator is the compilation by 2021 of objective information on:
- risk levels of individual credit and financial institutions;
- the preparedness of individual credit and financial institutions to counteract cyber attacks (as regards addressing information security risk (cyber risk) and its financial coverage);
- the preparedness of the credit and financial sector to counteract cyber threats by aggregating the data on risk levels of individual credit and financial institutions and the preparedness of each of them to counteract cyber attacks.

[10] *Clauses 9 and 9.1, Article 4 of Federal Law No. 86-FZ, dated 10 July 2002, 'On the Central Bank of the Russian Federation (Bank of Russia)' (general banking supervision, control and supervision over non-bank financial institutions' activities); Part 11, Article 14.1 of Federal Law No. 149-FZ, dated 27 July 2006, 'On Information, Information Technology and Information Protection' (control and supervision over the implementation by banks of organisational and technical measures ensuring personal data security when using the unified biometric system).*