ORIGINAL PAPER

DOI: 10.26794/2587-5671-2022-26-6-52-71
UDC 338.242(045)
JEL G20, 21

Challenges and Threats of the Digital Economy to the Sustainability of the National Banking System

M.N. Dudin[a], S.V. Shkodinsky[b]
[a, b] Institute of Market Problems of the Russian Academy of Sciences, Moscow, Russia;
[b] Financial Research Institute, Ministry of Finance of Russia, Moscow, Russia

ABSTRACT

The **goal** of the study — development of specific methodical reasoned proposals on improvement of the mechanism for ensuring sustainable development of the national banking system and its security against external challenges and threats to cyberspace. The **scientific novelty** consists in a comprehensive analysis of the processes of ensuring the cyber stability of the Russian banking system in the context of escalation of external challenges and threats to the digital economy. The authors used the following **methods**: general scientific (observation, comparison, measurement, analysis and synthesis, logical reasoning method), specific scientific (static analysis, peer review, graphical method). In the article conducted a critical review of domestic and foreign scientific literature and practical recommendations to ensure the protection of the banking institution from cyber threats in the digital economy; presented a comparative analysis of the organization of the cybersecurity system in the Russian and foreign banking systems; done multidimensional statistical analysis of cyber threats for Russian banks; substantiated recommendations and proposals on organizational, economic and legal improvement of the system of protection of Russian banks from internal and external cyber threats. As a **result**, it is shown that the main problem points (zones) of the banking system, creating the prerequisites for the occurrence of cyber-risks are: 1) there is no exchange of information on cyber-attacks and their mechanisms; 2) banks interact inefficiently with the state regulator of Internet — Roskomnadzor; 3) low level of competence of bank employees who are responsible for cybersecurity; 4) limited budget of small and medium-sized banks that wouldn't allow them to care independent cyber-protection units; 5) growing popularity of new fintech services and new fintech companies. The author draws a **conclusion** that the following measures are necessary for organizational, economic and legal improvement of the system of protection of Russian banks from internal and external cyber threats: the processes of development of banking ecosystems should be intensified; a federal interbank register of cyber fraudsters must be created; a single banking "polygon" for testing cyber threats needs to be developed.

Keywords: banks; cyber resilience; digital economy; challenges and threats; vulnerabilities; hacker attacks; fintech; personal data; fraud

***For citation*: Dudin M.N., Shkodinsky S.V. Challenges and threats of the digital economy to the sustainability of the national banking system. *Finance: Theory and Practice*. 2022;26(6):52-71. DOI: 10.26794/2587-5671-2021-26-6-52-71**

INTRODUCTION

The banking system is one of the most receptive areas of the national economy of any country to innovation and the changing architecture of the socio-economic system. This is explained by the dualism of economic interests of the banking institution in the context of digitalization. On the one hand, the formation of the digital economy — is a powerful driver to the qualitative evolution of the product portfolio with the possibility of offering personalized products and services to retail and corporate customers. On the other hand, banks strive to reduce the cost of providing banking services and products to their customers. However, it should be understood that on these "scales of interests" it is still necessary to place the interests of the national state regulator — the Central Bank — and its strategic goals to ensure the safe and sustainable functioning of the banking system of the country as a whole.

The transition of humanity into a new phase of development, called Industry 4.0, carries a number of systemic contradictions and risks for the stable functioning of the banking system. One of the fundamental ones is the large-scale transfer of business processes from physical analogues to digital, the appearance of virtual constructs, which weakens the ability of banks to ensure sufficient control of all these links, which makes them more vulnerable to external challenges and threats to the digital environment.

This scientific article is the result of a structured review of domestic and foreign practice of organization of the system of cyber protection against challenges and threats of sustainable development of the banking system, multidimensional statistical analysis of cyber threats for Russian banks, and also substantiation of specific methodical reasoned proposals on improvement of the mechanism for ensuring the sustainable development of the Russian banking system.

MATERIALS AND METHODS

Theoretical and methodological basis of the study includes scientific works of domestic (A.S. Yablochkin, A.P. Koshkin [1]; I.N. Timonicheva, V.V. Yanovskiy, A.S. Berezhnoy [2]; P.V. Revenkov, A.A. Berdyugin [3]; L.A. Chaldaeva; A.A. Kilyachkov, A.A. Yakorev [4]; N.I. Bykanova, D.V. Gordya, D.V. Evdokimov [5]) and foreign (N.A.-D. Khalifa [6]; Aguayo F. Zabala, B. Ślusarczyk [7]; A.W. Dorn, S. Webb [8]) academic community, also case studies and recommendations of leading consulting agencies (PT Security; PWC; Deloitte; Kaspersky Security Laboratory) and experts (N.N. Fedotov, J.S. Ashmanov; P. Singer, A. Friedman; V. Snyder; B. Tuscan; M. Hupponen) in cybersecurity.

When writing the article general scientific methods of scientific research (observation, comparison, measurement, analysis and synthesis, method of logical reasoning) and specific scientific (static analysis, expert assessment, graphical method) were used. The validity and reliability of the results of scientific research is ensured by the correctness and severity of the construction of the logic and design of the research, as well as the use of verified statistical information from authoritative sources (analytical reports of the Center for monitoring and responding to computer attacks in the financial sphere, thematic reports "Cyber security. Trends and forecasts" PT Security, materials of consulting agencies PWC, Deloitte, Kaspersky Security Laboratory).

REVIEW OF THE LITERATURE AND RESEARCH

Security functioning of any business — is a strategic task of management, the solution of which guarantees its survival in the market conditions and ensuring the trust of customers (without not neglecting other factors of competitiveness). For banks, this postulate is particularly true, as customers provide them with their money for safekeeping or trust

management and use their infrastructure and services for various transactions.

A critical review of domestic and foreign scientific literature and practical recommendations to ensure the protection of the banking sector from cyber threats in the digital economy revealed the presence of significant differences in the cyber security apparatus of the banking system.

In the domestic scientific and practical communities, the conceptual apparatus focuses on the disclosure of the concept of "cybersecurity" and the desire to take into account as many potential points (zones) in the business processes of banks that may be attacked from outside. Note that the domestic practice of banks is defensive and characterized by the desire to accurately and fully explain the content of such concepts as "security of banking business processes in the digital economy", "banking cybersecurity", "cyberstability".

According to Art. 2 of Doctrine of information security of the Russian Federation, *information security* refers to the state of security of individuals, society and the State against internal and external information threats, which ensures the realization of constitutional human and civil rights and freedoms, decent quality and standard of living of citizens, sovereignty, territorial integrity and sustainable socio-economic development of the Russian Federation, defense and security of the State.[1] In our view, this definition contains a rather general approach, reflecting the political orientation of State regulators to prevent the occurrence of potential challenges and threats to the digital economy for the economic security of the country as a whole.

According to S. I. Lutsenko, the cybersecurity of the banking institution should be considered as a complex mechanism for the application of organizational, technological, personnel and administrative tools to counter the influence of external cyberattacks and prevent offences of the internal information circuit of the banking system with its adaptation to the changing information technology landscape of the digital economy.[2] In this definition there is an essential fact that the mechanism should be adaptive, i.e. dynamic and change (more precisely — adapt) to the evolving challenges and threats of the digital economy, thus ensuring the security of financial assets and information of the banking system.

A slightly different approach was presented in the works of A. S. Alpeev, M. M. Bezkorovainy and A. L. Tatuzov. According to them, the cybersecurity of the banking institution — is a proactive system of response to internal and external challenges and threats of cyberspace, which is based on the flexible methodology of Agile, which allows in the shortest possible time to transform banking business processes for new sources of cyber-threats [9, 10]. The value of this definition lies in the feasibility of achieving synergy in the case of the application of flexible methods of project management in the IT sphere (Agile methodology specializes in IT projects) and classic rules of information hygiene in banks. That is, this definition brings us to a new term that was mentioned earlier,— "cyberstability".

In addition, in the work of R.I. Zakharchenko and I.D. Korolev, cyberstability refers to the ability of a business process management system to perform its functions in a complex, sharply changing environment under the conditions of destructive information impacts [11]. This definition refers to the ability of the banking system to remain operational even in the event of a cyberattack, which brings the issue of sustainable development to the level

[1] Doctrine of information security of the Russian Federation: approved by the Decree of the President of the Russian Federation No. 646 from 05.12.2016. URL: https://www.garant.ru/products/ipo/prime/doc/71456224/#0 (accessed on 20.01.2022).

[2] Lutsenko S.I. Policy of the Russian Federation in the field of cybersecurity. URL: http://digital-economy.ru/images/easyblog_articles/504/IB 777.pdf (accessed on 20.01.2022).

of the entire banking system of the country. There should be a complex mechanism of co-insurance of banks in case of cyberattacks from outside and an effective filter to prevent the formation of an aggressive information environment within the banking system.

In foreign practice, both in scientific and legislative works, the categorical apparatus is focused on revealing the essence of challenges and threats to the banking system from the standpoint of the concepts of "cyberattack", "cyberterrorism" and "cyberwar". This allows to make an assumption about the desire of foreign specialists to distinguish the above concepts, which is connected with the interest of state regulators (both financial and military) to consider the digital landscape and its infrastructure as a "theater of military operations". This assumption can be substantiated by the informative analysis of such documents as the "National cyber security strategy",[3] "Tallin Manual on International Law Applicable to Cyber Warfare"[4] (2017) and "Cybersecurity Act"[5] (2019).

Highlight the approach presented by the International Telecommunication Union, which presents cybersecurity as "technologies, concepts, public policies, procedures and practices aimed at protecting assets (computers, infrastructure, applications, services, communication and information systems) and cyberspace from attacks, damage and unauthorized access".[6] The definition makes the orientation of all actors in cyberspace quite clear and implies retaliation against the aggressor (although it is not explicitly declared).

In accordance with Art. 1 The EU Cybersecurity Act defines "cybersecurity" as "activities necessary for the protection of networks and information, users of information networks and other parties that may be affected by cyber threats".[7] However, the Law itself specifies (somewhat diluted) that the activity can be understood as active actions by authorized EU authorities aimed at preventive protection against possible cyberattacks.[8] We consider that the EU Act is oriented towards a possible active offensive policy.

A reference to the perception of cyberspace as an object of EU political and economic interests can be found in EU Directive 2016/1148 on cybersecurity: in particular, articles 9, 11, 13 indicate that, if necessary, authorized state regulators and members of PPP-agreements — owners of critical infrastructure — can participate in organizing active actions aimed at leveling the influence of the source of cyber threats by breaking diplomatic relations with them, blocking financial transactions, exclusion of intermediary institutions from international agreements of exchange of information or corresponding relations in financial (banking) spheres.

In the US National Cyber Security Strategy is a reference to the supplement to the law — Cloud Act, which contains permission to participate American IT-companies of FAMGA Group and separate intelligence Agency in collecting information on potential sources

[3] US New Cyber Security Strategy: Brief Analysis of the New Edition (16.10.2018). URL: http://csef.ru/ru/oborona-i-bezopasnost/272/novaya-strategiya-kiberbezopasnosti-ssha-kratkij-analiz-novoj-redakczii-8665 (accessed on 21.01.2022).

[4] Tallinn Manual 2.0 and Capture Cyberspace (06.02.2017). URL: https://www.geopolitica.ru/article/tallinskoe-rukovodstvo-20-i-zahvat-kiberprostranstva (accessed on 21.01.2022).

[5] Cybersecurity Act (17.12.2019). URL: https://medium.com/lawgeek-by-aurum/eu-cybersecurity-act-review-aurum-law-firm-d588db539e75 (accessed on 21.01.2022).

[6] International Telecommunications Union (ITU) (2008). Overview of Cybersecurity, Recommendation ITU– T X. 1205. URL: https://www.itu.int/rec/T-REC–X.1205–200804-I (accessed on 21.01.2022).

[7] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No. 526/2013 (Cybersecurity Act). Official Journal of the European Union, L 151/1. URL: http://data.europa.eu/eli/reg/2019/881/oj (accessed on 22.01.2022).

[8] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32016L1148 (accessed on 22.01.2022).

of cyber threats and deciding on preventive impact on them up to destruction in order to mitigate the risks of destructive influence on critical infrastructure.

Foreign academic community has a softer view on the disclosure of challenges and threats to the banking system, but generally maintain solidarity to take active action against the source of the threat. Thus, N.A.-D. Khalifa consider that the concept of cyberstability of the banking system should necessarily include a "mechanism of retaliation", which can be implemented both by the victims of the attack and by the principle of solidarity, by other banks — parties to agreements on cyber protection of corporate interests [6, p. 43–44]. In addition, A.W. Dorn and S. Webb consider that banking cybersecurity is a holistic system not only the protection of financial assets and the sustainable functioning of the national financial infrastructure, but also a preventive influence on the world hotspots of cyber-threats and potential cyber-attacks [8, p. 24].

RESULTS AND DISCUSSION

We consider that the presented critical review of domestic and foreign viewpoints on the essence of challenges and threats to the banking system is characterized by an appealing approach. In this regard, we consider it necessary to present a table of results of comparative analysis of the organization of the cybersecurity system in the Russian and foreign banking systems (*Table 1*).

According to the above comparative analysis, in domestic practice banks have sufficient autonomy to organize the cybersecurity system of their own activities. It is also important to note the fact that there are no special programmes for the development of security infrastructure for banks, financed by public sources (extrabudgetary funds, special-purpose budgets of the largest participants of the cybersecurity market of the state form of ownership, for example GC "RosTech"). This makes the banking system more vulnerable, as, with the exception of a group of systemically important banks and included in the top-100, most banks cannot afford such expenses due to their long payback and implicit commercial effect.

Studying the situation of the banking system of Russia from the standpoint of its sustainability before the cyber-threats of the digital economy, we consider appropriate to start with quantitative and qualitative analysis of cyberattacks, which allows to understand their scale and target orientation (*Fig. 1 and 2*).

According to the given data in *Fig. 1*, there is a steady growth in cyberattacks on the Russian banking system, and when analyzing a section of functional levels, it is evident that the main interest of attackers is focused on banks of 2 levels (738 attacks were committed during the research period) and significantly less — on non-bank credit organization (283 attacks). When analyzing the reasons for the increase in attacks on the Russian banking sector, the following was established:

- *first*, the Bank of Russia has seen a steady growth in non-cash settlements in retail banking: so, for 2020 the share of non-cash payments in retail turnover was 70.3% (64.7% — in 2019),[9] which outpaces the development of the remote banking services in most Western European countries and even the US and objectively attracts hacker groups;
- *second,* Russia is in the top three countries with the most active digital transformation of banking services — according to E&Y, in 2019, the share of active digital banking users was 82.0% (for comparison — the world average is 64%).[10] It is important to note that digital transformation in Russian banks comes down from above, i.e. banks' customers motivate them to introduce

[9] Results of the Bank of Russia: briefly about the main thing, 2020. URL: https://cbr.ru/about_br/publ/annrep2020short/platezhnaya-sistema/ (accessed on 26.01.2022).

[10] Global FinTech Adoption Index 2021. URL: https://www.ey.com/en_gl/ey-global-fintech-adoption-index (accessed on 26.01.2022).

the latest digital financial services, and banks often do not have sufficiently reliable systems of protection against external cyber threats, which together increases the interest of hacker groups in attacks;

• *third,* in the Russian banking system the following segments are developing most actively: digital banking (online lending, unsecured deposits, currency exchange, less often — investment products) — this service is developing in 78.7% of all banks and a group of payment and settlement services (money transfers, e-money, P2P-loans), is actually an extended continuation of digital banking for interaction of banks and, for example, telecom operators, manufacturers of gadgets for communication and exchange of financial information — more than 18.0%.[11] This fact of development also contributes to the vulnerability of the Russian banking system, as the rapid development of virtual payment services is not harmonized with financial literacy and digital hygiene of customers while working on the Internet, which multiplies the vulnerability of both sides.

Based on the features of the development of the Russian market of banking services, consider the composition and structure of objects exposed to cyberattacks in 2016–2021 (QI–QIII). At the same time, it should be noted that during this period cyberattacks on the banking system became complex, i.e. their objectives were more than one object, which indicates an increase in risks to the cyberstability of the Russian banking system (*Fig. 2*).

Fig. 2 data suggest that key object of hackers' criminal interests is the banking infrastructure — on average, this facility accounts for 57.5% of all recorded cyberattacks. In the second place — retail clients — a little more than 31.0%, the third place with a significant lag is occupied by the group "ATMs, POS-terminals, mobile devices" — 18.5%. At first glance, it may seem that hackers deliberately choose the safest link — banking infrastructure, but in fact a large number of customers do not declare that they have been attacked, or their gadgets were used as a point of entry, including damage to banking infrastructure.

With the onset of the COVID-19 pandemic, attacks on retail customers, as well as the use of their gadgets for hacker attacks significantly increased due to objective reasons: Introduction of quarantine measures, popularization of non-contact delivery tools and orders of products and services through online shopping, which, together with insufficient digital culture of the population, led to an increase in cyberattacks on these groups of objects.

Note that the fact of the active prevalence of attacks on the banking infrastructure directly indicates the participation of professional hackers of a very high level using powerful equipment (servers, Data-centers). This may indirectly indicate the carrying out of cyber-attacks sanctioned by the state regulators in order to find vulnerabilities in its architecture to obtain a new instrument of political pressure on Russia, at the worst — initiating cyberwarfare.[12]

The next step of this study is to study the tools of cyber-attacks, which is the information basis for developing specific proposals to improve the mechanism of cyber-attack protection and general increase of cyberstability of the Russian banking system (*Fig. 3*).

As follows from the diagram on *Fig. 3*, the key tool of cyber-attacks on the Russian banking system was software containing malicious code — on average, its use in

[11] Research of the market of technological entrepreneurship in Russia, 2020. (21.12.2020). URL: https://drive.google.com/file/d/1NsSN 3e_NkGS 1k2dfVb7cx6fXX8jHCNaA/view (accessed on 26.01.2022).

[12] The main types of computer attacks in the financial and credit sphere in 2019–2020 (2021). URL: https://cbr.ru/Collection/Collection/File/32122/Attack_2019–2020.pdf (accessed on 27.01.2022); Digital Threat: who might be behind cyberattacks on Russia (13.05.2021). URL: https://russian.rt.com/world/article/861272-rossiya-kiberataki-ssha-bezopasnost (accessed on 27.01.2022).

Table 1

Organization of cyber security in Russian and foreign banking systems: a comparative analysis

Criteria comparison	Russian banking system	Foreign banking systems
1. Sources of motivation/interest in developing cybersecurity	– increase in cyberattacks against the banking system from abroad; acute technological inequalities in the protection of banking services; – lack of unified national cyber security standards for banks; – increase the risks of cyberterrorism for EU and US political interests; – tightening international requirements for cybersecurity standards.	– political interests of using tools of cyberattacks on banking systems (USA, UK); – increase incidence of "leakage" of personal information about bank customers (EU, USA); – increase technological inequalities among partner banks (EU); – formation of precedents of sanctions pressure on the banking system and its individual banks (China) with a view to easing it in the world market.
2. Main stakeholders	– President of the Russian Federation – State regulators – Central Bank of the Russian Federation, Ministry of Digital Development, Communications and Mass Communications of the Russian Federation; – systemically significant credit organizations (13 banks).[a]	– European Banking Authority; – Committee on the Global Financial System BIS; – Society of World Interbank Financial Telecommunication (SWIFT); – Financial Industry Regulatory Authority [b]; – Country regulators as represented by Central Banks.
3. Summary of the implementation mechanism of the cybersecurity policy	Banks develop individual risk-strategies and maps of cyber threats, taking into account the specifics of the customer base, applied financial instruments and operating services. The main goal for banks – compliance with the criteria for safe operation established by the Central Bank of the Russian Federation and international regulatory institutions (when maintaining an active international activities). Minimum (thresholds) requirements for banking technology are contained in STO BR IBBS-1.0 "Information Security of Organizations of the Banking System of the Russian Federation. General Regulations".[c] General in GOST R 57580.1 – 2017 "Security of financial (banking) operations. Protection of information of financial organizations. Basic composition of organizational and technical measures".[d] A key expert accumulating information on cyberincidents in banks in the Central Bank Authority – Center for Monitoring and Response to Computer Attacks in the Financial Sphere (FinCERT) of the Information Security Department of the Bank of Russia.[e]	In the *USA*, commercial banks develop a collective cybersecurity policy (Sheltered Harbor[f] project) based on correspondent relations or the composition of the financial group and agree it with the National Cyber Authority.[g] In the *EU*, country-level regulatory banks develop State-wide cybersecurity strategies and coordinate them with the European Central Bank, which allows to harmonize the efforts of individual countries in ensuring the sustainable development of the EU banking system [12, 13]. In the *UK*, since 2014, the National Cyber Security Center, which is linked to all banks of the Kingdom and has the authority to make anti-crisis decisions in case of an attack and threats to destabilize the banking system.[h] In *China*, the cyber-protection system of banks is built on the principle of "soft power": bank system data transfer takes place through a dedicated autonomous network, to which clients are connected only during transactions or services. In addition, the State applies the model of "digital nationalism" – the introduction of special requirements on localization of all data within the jurisdiction of the State. This allows you to collect information about all network users and identify their personality, which is an additional protection against hacker attacks [14].

Table 1 (continued)

Criteria comparison	Russian banking system	Foreign banking systems
4. Sources of funding for cybersecurity projects and programmes	Banks individually set up special funds for financing cybersecurity projects within the framework of a development strategy for a period of 1, 3 or 5 years (forecast), or apply the method of regular contributions to a special fund.[i]	In the *USA*, banks are actively involved in Google and Microsoft-funded cybersecurity programs that test new cyber-attack protection products and then sell licenses to use them.[j] In the *EU*, banks and central banks in member states receive financial support from frameworks approved by the EU Parliament to ensure the cyber-sustainability of banks, and then at the level of regulators of individual countries, financing is distributed among banks. In the *UK*, banks actively engage with venture companies in the area of cybersecurity in the form of partnerships, including providing funding for startups in return for the latest solutions in the field of information protection (for example, the national technology partnership platform "Tech Nation", London Tech and North Tech city platforms to support the IT-community, universities and business schools engaged in cybersecurity research and development).[k] In *China*, in the period from 2020 to 2023, it is planned to spend the state funding in the amount of 40 billion USD for cybersecurity of the country[l], of which almost half are expected to be allocated to the banking sector. Funding will be directed to the development of IT group BAT, Huawei, ZTE.

Sources: compiled by the authors on the data [12–16]:

[a] Bank of Russia approved list of systemically significant credit organizations (11.10.2021). URL: https://cbr.ru/press/pr/?file=11102021_133500PR 2021–10–11T13_27_28.htm (accessed on 22.01.2022); [b] Regulatory overview of financial market (16.05.2016–15.07.2016). URL: https://cbr.ru/finmarkets/files/development/review_020916.pdf (accessed on 22.01.2022); [c] STO BR IBBS-1.0 "Information Security of Organizations of the Banking System of the Russian Federation. General Regulations". URL: https://cbr.ru/statichtml/file/59420/st-10–14.pdf (accessed on 23.01.2022); [d] GOST R 57580.1–2017 "Security of financial (banking) operations. Protection of information of financial organizations. Basic composition of organizational and technical measures": Order of the Federal Agency for Technical Regulation and Metrology No. 822 from 08.08.2017. URL: https://docs.cntd.ru/document/1200146534 (accessed on 23.01.2022); [e] Center for Monitoring and Response to Computer Attacks in the Financial Sphere (FinCERT) of the Information Security Department of the Bank of Russia. URL: https://cbr.ru/analytics/ib/fincert/ (accessed on 23.01.2022); [f] US Banks build system of defense against large-scale cyber-attacks (06.12.2017). URL: https://www.securitylab.ru/news/490069.php (accessed on 23.01.2022); [g] Karasev P. New US cybersecurity strategies (15.11.2018). URL: https://russiancouncil.ru/analytics-and-comments/analytics/novye-strategii-ssha-v-oblasti-kiberbezopasnosti/ (accessed on 23.01.2022); [h] United Kingdom cyberreadiness: a brief overview (October 2016). URL: https://analytica.digital.report/wp-content/uploads/2017/05/CRI-UK-RU.pdf (accessed on 23.01.2022); [i] Cyber security of the Russian economy and banking industry in general (17.02.2021). URL: https://plusworld.ru/professionals/kiberbezopasnost-rossijskoj-ekonomiki-i-bankovskoj-industrii-v-tselom/ (accessed on 23.01.2022); Cybersecurity 2021. Who is to blame and what to do? (12.11.2021). URL: https://plusworld.ru/journal/2021/plus-8–2021/kiberbezopasnost-2021-kto-vinovat-i-chto-delat/ (accessed on 23.01.2022); Revenkov P. Ensuring cyber security in the financial and credit sphere (06.11.2019). URL: https://www.secuteck.ru/articles/obespechenie-kiberbezopasnosti-v-kreditno-finansovoj-sfere (accessed on 23.01.2022); [j] Google and Microsoft has committed to invest in cybersecurity (26.08.2021). URL: https://www.forbes.ru/newsroom/tehnologii/438209-google-i-microsoft-vzyali-na-sebya-obyazatelstva-vlozhitsya-v (accessed on 24.01.2022); [k] Britain's economy tomorrow — the government's plan. URL: https://d-russia.ru/zavtrashnyaya-ekonomika-britanii-plan-pravitelstva.html (accessed on 24.01.2022); Britain's digital economy — state and development plans. URL: https://d-russia.ru/tsifrovaya-ekonomika-britanii-sostoyanie-i-plany-razvitiya.html (accessed on 24.01.2022); [l] Cybercrime and cyberconflict: China (14.07.2021). URL: https://www.tadviser.ru/index.php/Статья: Киберпреступность_и_киберконфликты:_Китай#. (accessed on 24.01.2022).

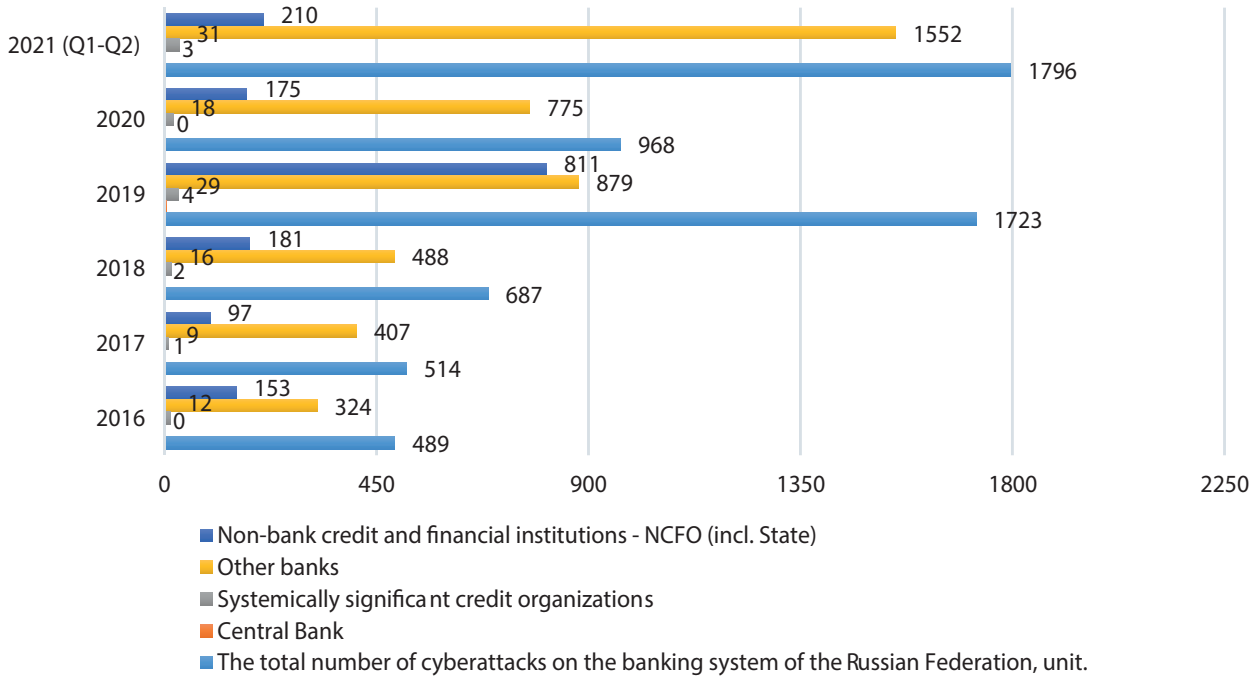

Fig. 1. **Number of Cyber Attacks on the Russian Banking System by Functional Level in 2016–2021 (Q1–Q3), units**

Sources: Overview of transactions made without the consent of clients of financial organizations in 2016: analytical report of the Information Security Department of the Bank of Russia (21.02.2017). URL: https://cbr.ru/Collection/Collection/File/32093/survey_transfers_16.pdf (accessed on 25.01.2022); Overview of transactions made without the consent of clients of financial organizations in 2017: analytical report of the Information Security Department of the Bank of Russia (15.10.2018) URL: https://cbr.ru/Collection/Collection/File/32094/survey_transfers_17.pdf (accessed on 25.01.2022); Overview of transactions made without the consent of clients of financial organizations for 2018: analytical report of the Information Security Department of the Bank of Russia (06.03.2019). URL: https://cbr.ru/Collection/Collection/File/32091/gubzi_18.pdf (accessed on 25.01.2022); Overview of transactions made without the consent of clients of financial organizations for 2019: analytical report of the Information Security Department of the Bank of Russia (19.02.2020). URL: https://cbr.ru/Collection/Collection/File/32189/Review_of_transactions_2019.pdf (accessed on 26.01.2022); Overview of operations performed without the consent of clients of financial organizations for 2020: analytical report of the Information Security Department of the Bank of Russia (12.06.2021). URL: https://cbr.ru/Collection/Collection/File/32190/Review_of_transactions_2020.pdf (accessed on 26.01.2022); Current Cyber Threats: Q3, 2021 (08.12.2021). URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q3/#id2 (accessed on 26.01.2022).

attacks was 53.7%. The prevalence of spyware software (in 2020, its share was more than 40.0%) for collecting personal data on customers and their accounts should be noted in its composition.

In second place is a tool of social engineering — 37,7%, which because of the pandemic COVID-19 sharply gained popularity. And its manifestation was both in the "familiar" form for cybersecurity professionals (phone scam), and new, complex formats integrated into customized service processes (for example, partner programs of the bank and representatives of retail, health centers). According to FinCert, in 2020, compared to 2019, the growth of this tool by 86.0%, which not only reduces the work of the security services of banks, but also significantly undermines customer confidence in the banking system as a whole.[13]

The third place is occupied by hacking — 21.8%, and it should be noted that its use was systematic

[13] The main types of computer attacks in the financial and credit sphere in 2019–2020 (2021). URL: https://cbr.ru/Collection/Collection/File/32122/Attack_2019–2020.pdf (accessed on 27.01.2022).

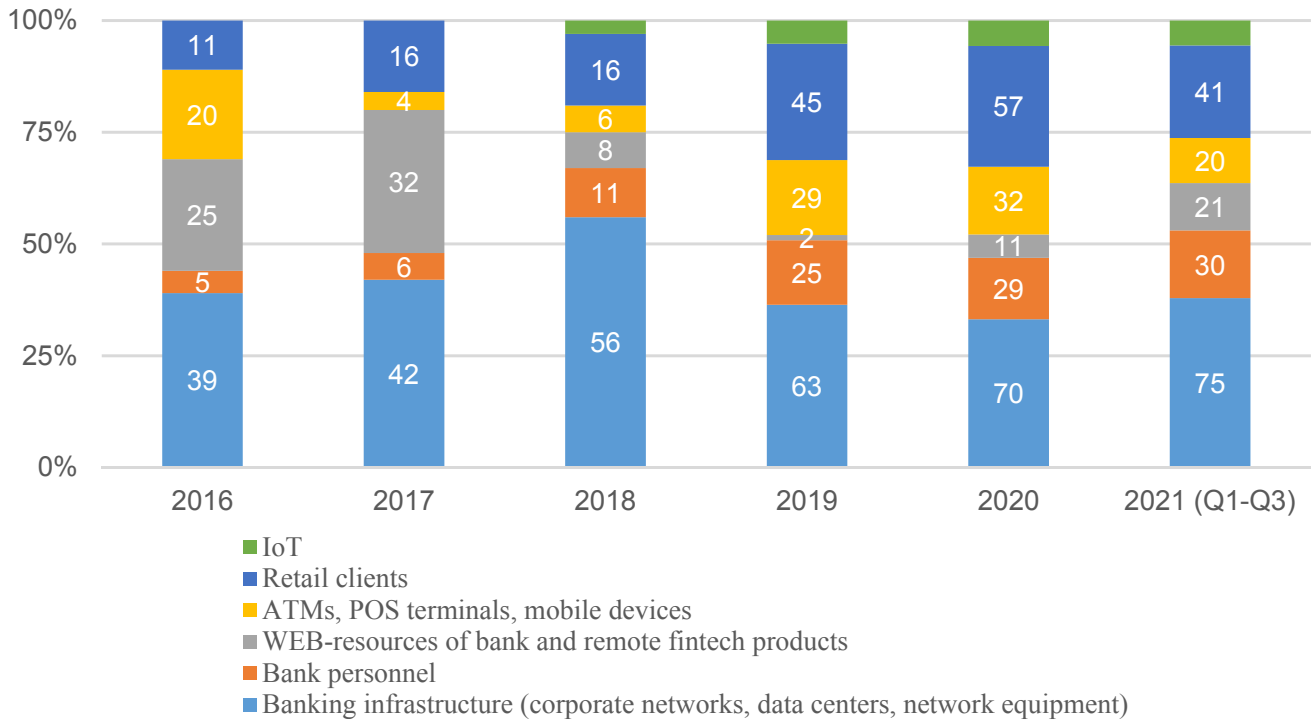

Fig. 2. **Composition and structure of banking system facilities exposed to cyber-attacks for 2016–2021 (Q1–Q3), in %**

Sources: Cybersecurity 2016–2017: from totals to forecasts (26.01.2017). URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-2016–2017-rus.pdf (accessed on 27.01.2022); Current cyber threats — 2017. Trends and forecasts (06.03.2017). URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2017-rus.pdf (accessed on 27.01.2022); Cybersecurity 2017–2018: figures, facts, forecasts (13.12.2017). URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2017–2018/ (accessed on 27.01.2022); Cybersecurity 2018–2019: figures, facts, forecasts (18.12.2018). URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2018–2019/ (accessed on 27.01.2022); Current cyber threats — 2018. Trends and forecasts (12.03.2019). URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Cybersecurity-threatscape-2018-rus.pdf (accessed on 27.01.2022); Cybersecurity 2019–2020. Trends and Forecasts (19.12.2019). URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-2019–2020/ (accessed on 27.01.2022).

and carefully organized: According to FinCert, 225 attacks by RTM hacker group in 2019–2020 there were[14] (acronym Remote Transaction Manager), the purpose of which was remote management of transactions of clients — owners of foreign currency deposits and investment deposits.

Consider the main motives of cyber-attacks on the banking system of the Russian Federation. The obtained results will determine the main points (zones) of attention of banks when assessing the cyberstability of their own business models (*Fig. 4*).

The data given on *Fig. 4* suggest that the key motive for cyber-attacks is to obtain financial benefits from the steal of money and its equivalents for enrichment — on average it accounted for 72.5%. However, it is important to note that its share in the structure of motives is gradually decreasing: This is due, on the one hand, to the increased work of banks on their own security against external and internal cyberrisks, and, on the other hand, to the more active work of the Central Bank on cyberincident reporting and bank tests for cyberstability.[15]

[14] See ibid.

[15] The Bank of Russia has summed up the results of the first anti-hacker teachings (10.02.2021). URL: https://www.mn.ru/smart/bank-rossii-podvel-itogi-pervyh-antihakerskih-uchenij-uchastie-v-nih-bylo-dobrovolnym (accessed on 28.01.2022).

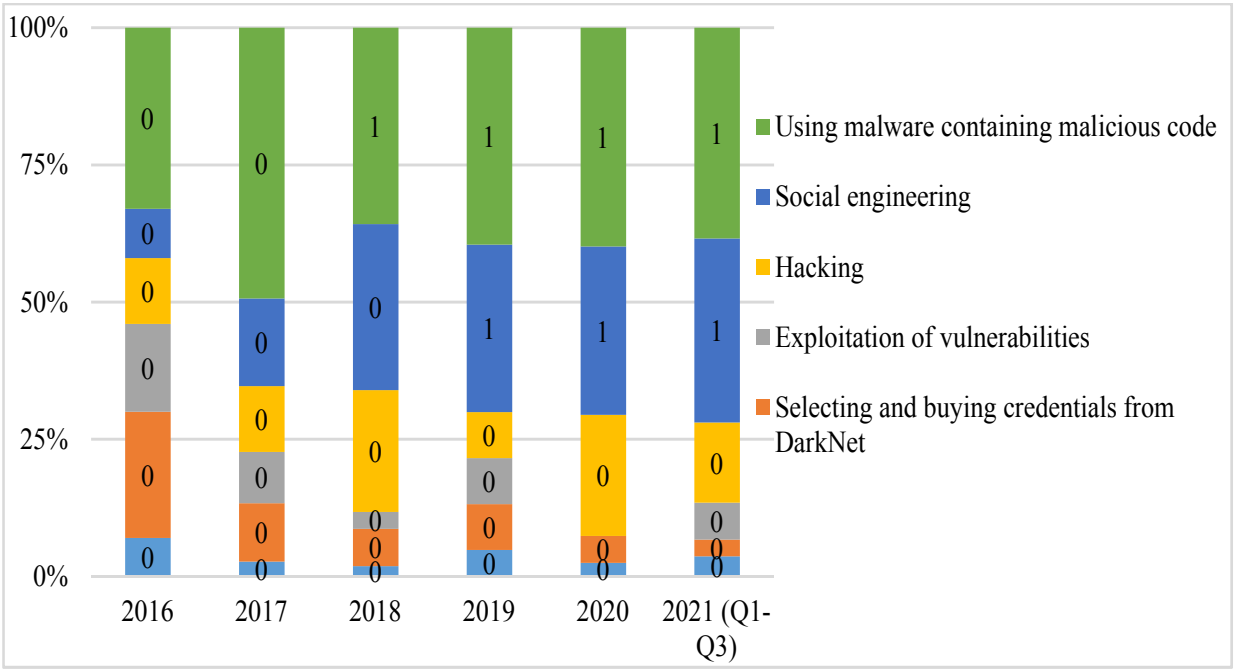

Fig. 3. **Cyberattack tools against members of the Russian banking system in 2016–2021 (Q1–Q3), %**

Sources: Penetration testing in credit sector organizations (20.02.2020). URL: https://www.ptsecurity.com/ru-ru/research/analytics/pentest-finance-2020/ (accessed on 28.01.2022); ART-attacks on the credit and financial sphere in Russia: a review of tactics and techniques (10.10.2019). URL: https://www.ptsecurity.com/ru-ru/research/analytics/apt-attacks-finance-2019/ (accessed on 28.01.2022); Credit and financial security, 2018 results. Positive Technologies Assessment (05.07.2020). URL: https://www.ptsecurity.com/ru-ru/research/analytics/credit-and-financial-security-2019/ (accessed on 28.01.2022); Vulnerabilities of online banks: summarizing the analysis (05.04.2019). URL: https://www.ptsecurity.com/ru-ru/research/analytics/vulnerabilities-rbo-2019/ (accessed on 28.01.2022); Vectors of hacker attacks on banks (05.06.2018). URL: https://www.ptsecurity.com/ru-ru/research/analytics/banks-attacks-2018/ (accessed on 28.01.2022); Financial application vulnerability statistics (24.04.2018). URL: https://www.ptsecurity.com/ru-ru/research/analytics/financial-application-vulnerabilities-2018/ (accessed on 28.01.2022); Current cyber threats: Q3, 2021 (08.12.2021). URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q3/#id2 (accessed on 27.01.2022).

At the same time, the share of such motivating factor as receipt and subsequent sale of personal data, blackmail and extortion — for QI–QIII in 2021, its share was 47.0%: the active development of social engineering practices and the popularization of virtual services have led to the development of models of the identity theft for the purpose of their sale to DarkNet-network or use for blackmail and extortion.

By the end of 2021, there was also an increase in such warning factors as hacktivism (popularization of hacker culture and cyberattacks) — 20.0% and the fixation of signs of organized and authorized by the State specialized regulators of cyber-attacks (4.0%).

These two tendencies have dangerous potential, as against the background of a pandemic and a decline in the real incomes of the population, there is an increase in social tension among the population, and the escalation of the military-political confrontation between Russia and NATO may well be supplemented by the conduct of massive cyber-attacks on banking infrastructure facilities.

At the same time, it is not easy to prove the existence of the threat of cyberwar: following rules of international humanitarian law, this means recognition of the State by the

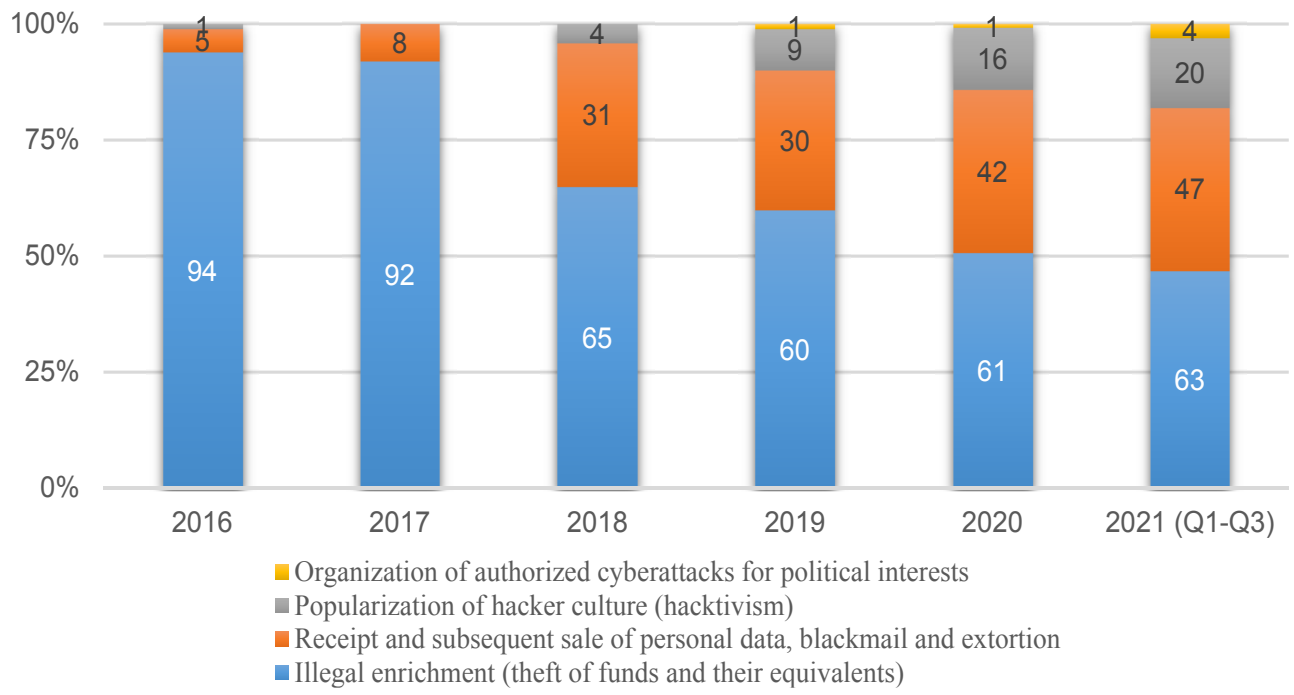

Fig. 4. **Composition and structure of motives for cyberattacks on the banking system in 2016–2021 (Q1–Q3), in %**

Sources: Penetration testing in credit sector organizations (20.02.2020). URL: https://www.ptsecurity.com/ru-ru/research/analytics/pentest-finance-2020/ (accessed on 29.01.2022); ART-attacks on the credit and financial sphere in Russia: a review of tactics and techniques (10.10.2019). URL: https://www.ptsecurity.com/ru-ru/research/analytics/apt-attacks-finance-2019/ (accessed on 29.01.2022); Credit and financial security, 2018 results. Positive Technologies Assessment (05.07.2020). URL: https://www.ptsecurity.com/ru-ru/research/analytics/credit-and-financial-security-2019/ (accessed on 29.01.2022); Vulnerabilities of online banks: summarizing the analysis (05.04.2019). URL: https://www.ptsecurity.com/ru-ru/research/analytics/vulnerabilities-rbo-2019/ (accessed on 29.01.2022); Vectors of hacker attacks on banks (05.06.2018). URL: https://www.ptsecurity.com/ru-ru/research/analytics/banks-attacks-2018/ (accessed on 29.01.2022); Financial application vulnerability statistics (24.04.2018). URL: https://www.ptsecurity.com/ru-ru/research/analytics/financial-application-vulnerabilities-2018/ (accessed on 29.01.2022); Current cyber threats: Q3, 2021 (08.12.2021). URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021-q3/#id2 (accessed on 29.01.2022).

aggressor with all the political and economic consequences for all participants.[16]

At the final stage of the study, an analysis of the security of Russian banks from cyberattacks for 2016–2021 (QI–QIII) was conducted (*Table 2*).

According to *Table 2*, despite an increase in the rate of successfully stopped cyber-attacks against banks (52.7% in 2020 compared to 39.5% in 2016), the volume of losses for the banking system is constantly increasing. In addition, there is a decrease in the index of stability of the national banking system in the category of commercial banks of the second group — in 2020 it was 3.4, whereas in 2016 it was 5.5.

Based on the above analysis, the authors identified the main problem points (zones) of influence on the cyberstability of the Russian banking system in the context of ongoing digital transformations (*Table 3*).

As a result of the description of points (zones) of influence on cyberstability of the

[16] The right tool for the job: how does international law apply to cyber operations? (06.10.2020). URL: https://blogs.icrc.org/law-and-policy/2020/10/06/international-law-cyber-operations/ (accessed on 28.01.2022); Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts (March 2021). URL: https://international-review.icrc.org/articles/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts-913 (accessed on 28.01.2022).

Table 2

Key indicators of Russian banks' protection against cyberattacks for 2016–2020

Indicators	2016	2017	2018	2019	2020
1. Indicator of successfully stopped cyberattacks, in% to the total	39.5	42.4	44.7	49.5	52.7
2. The volume of losses of the banking system from cyberattacks, mln rub.	1080	961.3	1384.7	5723.5	8757.2
3. Level of compensation by banks of losses from cyberattacks (amount of returned funds / amount of stolen funds * 100), in% to the total	18.3	17.2	16.2	15	11.3
4. Index of stability of the national banking system (ratio of reflected and successfully stopped cyberattacks) by categories of banking institutions:					
4.1. Central Bank	–	1	2	4	–
4.2. Systemically important credit institutions	7.9	7.2	6.8	8	7.7
4.3. Commercial banks of 2 groups	5.5	4.7	4.9	4.5	3.4
4.4. Non-credit financial organizations (NCFO)	6.2	5.8	5.5	4.9	4.1

Sources: Overview of transactions made without the consent of clients of financial organizations in 2016: analytical report of the Information Security Department of the Bank of Russia (21.02.2017). URL: https://cbr.ru/Collection/Collection/File/32093/survey_transfers_16.pdf (accessed on 17.05.2021); Overview of transactions made without the consent of clients of financial organizations in 2017: analytical report of the Information Security Department of the Bank of Russia (15.10.2018). URL: https://cbr.ru/Collection/Collection/File/32094/survey_transfers_17.pdf (accessed on 17.05.2021); Overview of transactions made without the consent of clients of financial organizations in 2018: analytical report of the Information Security Department of the Bank of Russia (06.03.2019). URL: https://cbr.ru/Collection/Collection/File/32091/gubzi_18.pdf (accessed on 17.05.2021); Overview of transactions made without the consent of clients of financial organizations in 2019: analytical report of the Information Security Department of the Bank of Russia (19.02.2020). URL: https://cbr.ru/Collection/Collection/File/32189/Review_of_transactions_2019.pdf (accessed on 17.05.2021); Overview of transactions made without the consent of clients of financial organizations in 2020: analytical report of the Information Security Department of the Bank of Russia (12.06.2021). URL: https://cbr.ru/Collection/Collection/File/32190/Review_of_transactions_2020.pdf (accessed on 17.05.2021).

Russian banking system in the final part of our research we present recommendations and proposals for organizational, economic and legal improvements of the system of protection of Russian banks from internal and external cyberthreats (*Table 4*).

We consider that ensuring the cyberstability of the banking system of the Russian Federation requires the application of systemic measures that include both administrative (improvement of legislation in the circulation of personal data, tightening of liability for their preservation and commission of cybercrimes), economic (formation by banks of targeted budgets of expenditures for information security) measures, and public education, aimed at developing the necessary competencies in the field of safe behavior of clients in the virtual space.

Table 3

Main problem points (zones) of influence on the cyber resilience of the Russian banking system

Problem Point (Zone)	Characteristics of the problem point (zone), assessment of its impact
1. Lack of market self-regulation and exchange of information on cyber-attacks and their mechanisms	*Characteristic of problem point (zone):* currently, in the Russian Federation there is no institution of market self-regulation of banks, NCFO and their clients (physical and legal), in terms of information exchange about cyberattacks and mechanisms of their commission due to risks of loss of business reputation, weakening of competitive positions in the market, corporate egoism management[a] *Impact assessment of problem point (zone)*: the information vacuum contributes to the scaling and replication of cyberattacks, as the experience of countering them is formed individually by each bank, i.e. the initiators of attacks have a temporary and technological advantage in cyber-attacks and maximization of damage
2. Low efficiency of cooperation of the e-commerce segment with the State regulator of the Internet — Roskomnadzor	*Characteristic of problem point (zone):* currently, between the e-commerce segment and Roskomnadzor, administrative measures prevail on violation of the rules of work with personal data of customers, lack of adequate protection during their processing, etc.[b] At the same time, the issue of preventive protection against cyber-attacks, the increase in cyber literacy of e-commerce management is extremely local and spot nature, which makes the e-commerce segment the point of intrusion of hackers to obtain subsequent access to banking products (cards, mobile banking, etc.) *Impact assessment of problem point (zone):* e-commerce segment is an essential source for the theft of customers' identity and their use to access banking products: according to FreightWave, the number of online e-commerce crime increased by 50% in 2020[c]
3. Insufficient professional training and competence of bank employees in detecting signs of cyber-attack	*Characteristic of problem point (zone):* according to the PWC report, only 16% of bank managers are performing systematic work on the formation of a team of cyber specialists in the security service and their integration into the business processes of all bank's departments, and 23% conduct regular training of the bank staff to identify cyber threats at workplaces[d] *Impact assessment of problem point (zone):* human factor is considered as an important vulnerability for cyberattacks as technical aspects of bank perimeter protection improve. Given the development of social engineering practices, exploiting vulnerability at the expense of the human factor becomes very effective: with a high-quality attack scheme its identification in operational business processes becomes extremely difficult to identify
4. Limited budget for small and medium-sized banks that wouldn't allow them to care independent cyber-protection units	*Characteristic of problem point (zone):* According to the Positive Technologies report, only 29.0% of banks have a regular budget to fund cyber defense programs, and 32.0% have one-time investments in the acquisition of new cybersecurity tools[e] *Impact assessment of problem point (zone):* Acute differentiation of cybersecurity costs affects the overall cyberstability of the banking system, as penetration of a secure perimeter of a malicious object is not only indicative of vulnerability, but given the exponential growth of correspondent accounts between banks multiplies risks of "infection" even the most protected banks

Table 3 (continued)

Problem Point (Zone)	Characteristics of the problem point (zone), assessment of its impact
5. Popularization and active growth of market presence of Fintech-services and companies	*Characteristic of problem point (zone):* Fintech-companies in the Russian Federation are mainly superstructures of banks and are subject to general security policy, but there is also a group of independent NCFO (according to 2022–71 units[f]), targeted use of which is mainly to organize money transfers in circumvention of the bank (anonymous wallets, P2P-transactions). Thus, from January to May 2020, there were 165 thousand fraudulent transactions totaling 1.6 billion rubles[g] *Impact assessment of problem point (zone):* business models of Fintech-companies are based on different principles from traditional banks and, importantly, do not comply with most of the bank safety standards set by the Central Bank. In addition, the unregulated development of Fintech-services threatens Russia's compliance with FATF standards (Financial Action Task Force on Money Laundering) [17]

Sources: developed by authors based on:

[a] The results of a study of the market opinions on the development of financial technologies for 2021–2023 (2020). URL: https://www.accenture.com/_acnmedia/PDF-163/Accenture-Result-Research-Market-Opinion-Russian.pdf (accessed on 28.01.2022); [b] Like war, shares of destruction. How Roskomnadzor fights social networks and what will happen next (06.12.2021). URL: https://skillbox.ru/media/business/kak-roskomnadzor-boretsya-s-sotssetyami/ (accessed on 29.01.2022); [c] E-commerce cybercrime jumped 50% in 2020. URL: https://www.freightwaves.com/news/e-commerce-cybercrime-jumped-50-in-2020 (accessed on 29.01.2022); [d] Global research "Trust in digital technologies" 2021. URL: https://www.pwc.ru/ru/publications/dti-2021/e-version-digital-trust-insights-2021-in-russian.pdf (accessed on 30.01.2022); [e] How much is security. Analysis of information security processes in Russian companies (2017). URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/IS-Cost-rus.pdf (accessed on 30.01.2022); Online security above all for banks (29.04.2021). URL: https://www.comnews.ru/content/214362/2021-04-29/2021-w17/onlayn-bezopasnost-prevyshe-vsego-dlya-bankov (accessed on 30.01.2022). [f] Fintech by the numbers Incumbents, startups, investors adapt to maturing ecosystem (2020). URL: https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/financial-services/fintech-by-the-numbers.pdf (accessed on 30.01.2022); Development of the fintech-market in Russia: neobanks and startups (11.12.2019). URL: https://www.finam.ru/analysis/forecasts/razvitie-fintex-rynka-v-rossii-neobanki-i-startapy-20191211-142048/ (accessed on 30.01.2022); [g] Financial regulator disclosed volume of fraudulent transactions in 2020 (23.06.2020). URL: (accessed on 22.07.2022).

CONCLUSION

Based on the results of the scientific research, it was found that, in general, there is a tendency to increase the threats to the sustainability of the national banking system and the growth of their qualitative, professional component, which indirectly indicates the likely presence of political interests of NATO member states in identifying potential vulnerabilities of the Russian banking perimeter.

In the analysis of the cyber-stability of the banking system of Russia, it was found that, despite the increase in the success of stopped cyberattacks, the losses of the national banking system increased. This is primarily due to an increase in attacks aimed at undermining public confidence in banks, as well as an increase in the use of "white spots" in national legislation by fintech companies in their own self-interest.

Note that the state regulator, represented by the Central Bank of Russia, carries out active and systematic work to reduce the number of sources of cyber-risks and actively improves the legislative base to prevent the use of legal collisions and unresolved issues to prosecute for the acts committed in the crime field using ICT.

The article makes a theoretical contribution to the development of the problems of ensuring the cyberstability of the banking system of Russia and the improvement of practices of the

Table 4

Recommendations and proposals for organizational, economic and legal improvements to the system of protection of Russian banks from internal and external cyberthreats

Recommendations/ suggestions	Contents of the recommendations/suggestions Assessment of the possible effect
1. Intensification of the development of the business model of banking ecosystems	*Content*. The ecosystem as a business model has as its core a strong and financially sustainable bank that is not only able to form a zone of attraction for partners, but is also interested in providing a safe space for transactions for customers and partners, which in fact guarantees the sustainability and economic value of the ecosystem for all its participants *Impact:* 1) formation of market centers for the accumulation of information on cyberthreats within the ecosystem and its circulation between the participants; 2) accumulation of experience against cyberattacks, and reducing their impact on members of the banking ecosystem; 3) scaling up and expansion of complex ICT solutions to secure banking infrastructure and client access devices *Examples of successful practices of applying:* CARTA (Continuous adaptive risk and trust assessment) methodology is implemented in the business model of the ecosystem headed by PJSC "Sberbank" — a special banking structure is constantly monitoring all risks arising in the ecosystem, and protective measures should be considered and implemented in each process, each participant, and the information interaction of the bank — heads of the ecosystem with partners is realized through multi-stage filter-system with implementation of OpenID Connect specification (framework OAuth 2.0) [a]
2. Establishment of a federal interbank registry of cybercriminal' accounts[b]	*Content*. Since 2018, an initiative on the creation of an interbank account register, with the help of which fraudsters withdraw stolen money, but until now its development remains at the level of private decisions of the country's largest banks, which does not allow a systematic approach to the problem *Impact:* 1) reduction of options for moving money abroad; 2) increased transparency and control of questionable transactions; 3) attraction of banks and fintech companies found to be complicit with hackers and fraudsters *Examples of successful practices of applying:* Saudi Arabia's banking regulator implements SOC–Center initiative, which holds the digital profile of each bank and Fintech-company, cyber-attack statistics, experience in their reflection and results of investigations into questionable transactions or bank and fintech fraud
3. Formation of a unified banking "polygon" to test software vulnerabilities	*Content*. Development of a joint infrastructure solution with the participation of the Bank of Russia, GC "Rostech" and the Association of Russian Banks — "testing sandbox" for testing of new software products and solutions in the field of cyber protection, as well as simulations of attacks on existing architecture of organization of protection business processes of banks by so-called "white hackers"[c] *Impact:* 1) formation of national methodology of software testing for vulnerabilities; 2) identification "back entrance" and spy codes in foreign software for banks and Fintech-services; 3) advanced training of specialists in the field of cybersecurity and the popularization of safe work; 4) conducting full-scale exercises of possible cyber-attacks of various scales *Impact assessment*. In the Russian Federation the formation of a testing platform for banking software vulnerabilities and information model architecture is regulated by the Federal Project "Information Security" (program "Digital Economy of the Russian Federation")[d] *Examples of successful practices of applying:* in the US in 2017 the concept of zero trust was adopted (zero trust even to users inside the perimeter of ICT-business architecture) and based on it, a commercial platform was created DataVisor Global Intelligence Network[e], allowing you to test bank software vulnerabilities for a fee, as well as design various scenarios of attacks

Table 4 (continued)

Recommendations/ suggestions	Contents of the recommendations/suggestions Assessment of the possible effect
4. Developing regulatory oversight of fintech services operations	*Content.* Currently, independent Fintech-companies operating outside of bank licenses are virtually unregulated in their operations. In particular, it should consider introducing regulation on such aspects as the introduction of the practice of screen scrapping (monitoring of operational risks), stricter rules of turnover and identification when using SIM-cards, phone numbers, service providers and hosts when renting servers *Impact:* 1) formation an open trust environment for exchanging information about unsafe customers and infrastructure; 2) formation of base of digital profiles of legal entities and individuals with assessment of risks of their financial behavior based on analysis of financial transactions and business operations *Examples of successful practices of applying:* Bank of England in 2015 initiated compulsory transition of banks to API (Application Programming Interface)[f], which will allow banks and the state regulator to identify at an early stage unsafe customers and telecom infrastructure facilities (for example, telecom providers) that provide implementation of potentially cyber-dangerous transactions
5. Development of practice of "cyber patronage" by banks — owners of ecosystems and administrators of super-services	*Content.* An alternative solution to ensure sufficient cybersecurity for small and medium-sized banks under the new cyberstability standards is to enter into a partnership agreement with the managers of ecosystem banks or super-service administrators to grant the right to use a secure infrastructure for a fee. In this case, the risks of attacks are distributed between the parties and both parties get synergistic effect from the interaction of granting the right to use the protected infrastructure for a fee: patrons — additional income, small banks — access to protected infrastructure and opportunity to develop new services and banking products on ecosystem landscape
6. Improvement of financial literacy of retail and corporate clients of banks and NCFO	*Content.* Russian Index of Financial Literacy (RIFL) in 2020 it was 54 points (in 2018–53, in 2017–52) [g], objectively not enough to create safe behavior in the context of the escalation of cyber threats. On this basis, a number of measures should be taken to promote safe behavior on the Internet in financial transactions, as well as to provide advice and education on current cyber threats in the form of TV-shows, podcasts on radio and popular social media forums, online meetings with cybersecurity professionals[h]

Sources: developed by authors based on [18–27]:

[a] Sberbank: ecosystem — new opportunities, new challenges to cybersecurity (11.01.2019). URL: https://www.it-world.ru/cionews/security/158287.html (accessed on 30.01.2022); [b] Cyberattacks on banks: trends, vulnerabilities and the role of regulator (27.07.2018). URL: https://plusworld.ru/professionals/kiberataki-na-banki-trendy-uyazvimosti-i-rol-regulyatora/ (accessed on 30.01.2022); [c] The results of a study of the market opinions on the development of financial technologies for 2021–2023 URL: https://www.accenture.com/_acnmedia/PDF-163/Accenture-Result-Research-Market-Opinion-Russian.pdf (accessed on 30.01.2022); [d] Execution of works on the creation of Cyber Range to training students, specialists and experts of various disciplines, managers in the field of information security and IT to modern security practices. URL: https://digital.gov.ru/uploaded/files/03kiberpoligontz.pdf) (accessed on 31.01.2022); [e] Gartner List: what technologies will help business in 2022 (18.11.2021). URL: https://habr.com/ru/company/netologyru/blog/590117/ (accessed on 31.01.2022); DataVisor. URL: https://www.weforum.org/organizations/datavisor (accessed on 31.01.2022); [f] Information and analytical review of "Russian Banking System Today" (September 2019). URL: https://asros.ru/upload/iblock/c30/20397_informatsionnoanaliticheskoeobozrenie sentyabr2019.pdf (accessed on 17.01.2022); [g] To measure the level of financial literacy: 3rd stage. URL: https://cbr.ru/analytics/szpp/fin_literacy/fin_ed_intro/ (accessed on 31.01.2022); [h] Strategy for improving financial literacy in the Russian Federation for 2017–2023. Order of the Government of the Russian Federation No. 2039 from 25.09.2017. URL: http://static.government.ru/media/files/uQZdLRrkPL AdEVdaBsQrk505szCcL4PA.pdf (accessed on 31.01.2022).

organization of the cyber-defense system in banks and NCFO. We consider that the article will be useful for all those who are interested in the issues of safe financial behavior, as well as those responsible for cyber security in banks, as well as the non-banking sphere, which has a close connection with the banking infrastructure (e-commerce segment, venture teams in the field of financial technologies, etc.).

ACKNOWLEDGEMENTS

The article was prepared within a state assignment of the Market Economy Institute of the Russian Academy of Sciences; the topic of research is "Institutional transformation of economic security in the solution of socioeconomic sustainable development problems of the national economy of Russia". Market Economy Institute, Russian Academy of Sciences, Moscow, Russia.

REFERENCES

1. Yablochkin A.S., Koshkin A.P. Current vectors of research in the area of information security strategies. *Natsional'naya bezopasnost' / nota bene = National Security / nota bene*. 2019;(5):34–47. (In Russ.). DOI: 10.7256/24540668.2019.5.31224 (In Russ.)
2. Timonicheva I.N., Yanovskiy V.V., Berezhnoy A.S. The level of confidence in the safety of financial technologies: A barrier or a point of growth. *Nauchnyi rezul'tat. Ekonomicheskie issledovaniya = Research Result. Economic Research*. 2021;7(3):81–88. DOI: 10.18413/2409–1634–2021–7–3–0–7 (In Russ.)
3. Revenkov P.V., Berdyugin A.A. Social engineering as a source of risks in online banking services. *Natsional'nye interesy: prioritety i bezopasnost' = National Interests: Priorities and Security*. 2017;13(9):1747–1760. DOI: 10.24891/ni.13.9.1747 (In Russ.)
4. Chaldaeva L.A., Kilyachkov A.A., Yakorev A.A. On the formation of state functions to ensure security in the virtual space of Russia. *Vlast' = The Authority*. 2020;28(3):37–46. (In Russ.). DOI: 10.31171/vlast.v28i3.7293 (In Russ.)
5. Bykanova N.I., Gordya D.V., Evdokimov D.V. Trends and patterns of the banking sector digitalization process. *Nauchnyi rezul'tat. Ekonomicheskie issledovaniya = Research Result. Economic Research*. 2020;6(2):42–51. DOI: 10.18413/2409–1634–2020–6–2–0–6 (In Russ.)
6. Khalifa N.A.-D. Cybercrime: theoretical determinants, criminal policies, prevention & control mechanisms. *International Journal of Technology and Systems*. 2020;5(1):34–63. DOI: 10.47604/ijts.1133
7. Zabala Aguayo F., Ślusarczyk B. Risks of banking services' digitalization: The practice of diversification and sustainable development goals. *Sustainability*. 2020;12(10):4040. DOI: 10.3390/SU 12104040
8. Dorn A.W., Webb S. Cyberpeacekeeping: New ways to prevent and manage cyberattacks. *International Journal of Cyber Warfare and Terrorism*. 2019;9(1):19–30. DOI: 10.4018/IJCWT.2019010102
9. Alpeev A. Terminology of security: Cybersecurity, information security. *Voprosy kiberbezopasnosti = Cybersecurity Issues*. 2014;(5):39–42. (In Russ.).
10. Bezkorovainy M., Tatuzov A. Cybersecurity — approaches to the definition. *Voprosy kiberbezopasnosti = Cybersecurity Issues*. 2014;(1):22–27. (In Russ.).
11. Zakharchenko R.I., Korolev I.D. Methods of estimation of stability of functioning of objects of critical information infrastructure operating in cyberspace. *Naukoemkie tekhnologii v kosmicheskikh issledovaniyakh Zemli = High Tech in Earth Space Research*. 2018;10(2):52–61. DOI: 10.24411/2409–5419–2018–10041 (In Russ.).
12. Carrapico H., Barrinha A. European Union cyber security as an emerging research and policy field. *European Politics and Society*. 2018;19(3):299–303. DOI: 10.1080/23745118.2018.1430712
13. Christou G. Cybersecurity in the European Union: Resilience and adaptability in governance policy. London: Palgrave Macmillan; 2016. 222 p. DOI: 10.1057/9781137400529
14. Gorian E. Cybersecurity law of the People's Republic of China as a key instrument for ensuring information security of the banking and finance system. *Administrativnoe i munitsipal'noe pravo = Administrative and Municipal Law*. 2020;(3):47–55. DOI: 10.7256/2454–0595.2020.3.32677 (In Russ.).

15. Najaf K., Mostafiz M.I., Najaf R. Fintech firms and banks sustainability: Why cybersecurity risk matters? *International Journal of Financial Engineering*. 2021;8(2):2150019. DOI: 10.1142/s2424786321500195
16. Uddin M.H., Mollah S., Ali M.H. Does cyber tech spending matter for bank stability? *International Review of Financial Analysis*. 2020;72:101587. DOI: 10.1016/j.irfa.2020.101587
17. Povetkina N.A., Ledneva Yu.V. Fintekh and redtekh: Boundaries of legal regulation. *Pravo. Zhurnal Vysshei shkoly ekonomiki = Law. Journal of the Higher School of Economics*. 2018;(2):46–67. (In Russ.). DOI: 10.17323/2072–8166.2018.2.46.67 (In Russ.).
18. Vakulyk O., Petrenko P., Kuzmenko I., Pochtovyi M., Orlovskyi R. Cybersecurity as a component of the national security of the state. *Journal of Security and Sustainability Issues*. 2020;9(3):775–784. DOI: 10.9770/JSSI.2020.9.3(4)
19. Cybersecurity capacity maturity model for nations (CMM). Revised edition. Oxford: Global Cyber Security Capacity Center; 2020. DOI: 10.2139/ssrn.3657116
20. Sutherland E. Cybersecurity: Governance of a new technology. In: Proc. PSA18 Political Studies Association Int. conf. (Cardiff, 26–28 March 2018). London: Political Studies Association; 2018. DOI: 10.2139/ssrn.3148970
21. Camillo M. Cybersecurity: Risks and management of risks for global banks and financial institutions. *Journal of Risk Management in Financial Institutions*. 2017;10(2):196–200. URL: https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/jrmfi-mark-camillo-article-mar-2017.pdf
22. Wang F.F. Legislative developments in cybersecurity in the EU. *Amicus Curiae*. 2020;1(2):233–259. DOI: 10.14296/ac.v1i2.5131
23. Bakker T.G., Streff K. Accuracy of self disclosed cybersecurity risks of large U.S. banks. *The Journal of Applied Business and Economics*. 2016;18(3):39–51. URL: http://www.na-businesspress.com/JABE/BakkerTG_Web18_3_.pdf
24. De Fréminville M. Cybersecurity and decision makers: Data security and digital trust. Hoboken. NJ: John Wiley & Sons, Inc.; 2020. 224 p.
25. Semeko G.V. Information security in the financial sector: Cybercrime and countermeasures strategy. *Sotsial'nye novatsii i sotsial'nye nauki = Social Novelties and Social Sciences*. 2020;(1):77–96. DOI: 10.31249/snsn/2020.01.06 (In Russ.)
26. Nesterova D.A. Information security risks of commercial banks in the new economic and technological reality. *Innovatsii i investitsii = Innovation & Investment*. 2020;(5):144–151. (In Russ.).
27. Shkodinsky S.V., Dudin M.N., Usmanov D.I. Analysis and assessment of cyberthreats to the national financial system of Russia in the digital economy. *Finansovyi zhurnal = Financial Journal*. 2021;13(3):38–53. DOI: 10.31107/2075–1990–2021–3–38–53 (In Russ.)

ABOUT THE AUTHORS

Mikhail N. Dudin — Dr. Sci. (Econ.), Prof., Deputy Director for Science, Market Economy Institute, Russian Academy of Sciences, Moscow, Russia
http://orcid.org/0000-0001-6317-2916
Corresponding author
dudinmn@mail.ru

Sergey V. Shkodinsky — Dr. Sci. (Econ.), Prof., Head of the Laboratory of Industrial Policy and Economic Security, Market Economy Institute, Russian Academy of Sciences, Moscow, Russia; Chief Researcher at the Center for Sectoral Economics, Financial Research Institute, Moscow, Russia
http://orcid.org/0000-0002-5853-3585
sh-serg@bk.ru

Conflicts of Interest Statement: The authors have no conflicts of interest to declare.

The article was submitted on 13.02.2022; revised on 28.02.2022 and accepted for publication on 27.03.2022.
The authors read and approved the final version of the manuscript.