ORIGINAL PAPER

DOI: 10.26794/2220-6469-2022-16-2-51-63
UDC 336.717.06(045)
JEL G21

Digital Banking: Modern Finance Paradigm Shifting

I.A. Zaripov
Plekhanov Russian University of Economics, Moscow, Russia

ABSTRACT

The article presents author's view on the current problems facing the banking system of the Russian Federation as part of the transition to digital banking services, especially aggravated due to the massive using of remote channels of interaction caused by the restrictions of the pandemic period. The author analyses the current problems of financial sector due to increased criminal cyber attacks and offers his recommendations to counter these crimes. There is evidence of the needs to revise the concepts and strategies of the development of banks in connection with digitalization, to improve approaches to information security. Finally, the author concluded that a key element in the process of digitalization of banking activities is information security, and the soundness of banking institutions can be ensured only by the joint efforts of the state, banks, and their customers.

Keywords: digitalization; financial sector; banking; digital finance; information security

For citation: **Zaripov I.A. Digital banking: Modern finance paradigm shifting. *The World of the New Economy*. 2022;16(2):51-63. DOI: 10.26794/2220-6469-2022-16-2-51-63**

INTRODUCTION

It is now a time digital banking (DB) — this is a trend, of whom speak banking institutions, representatives of IT-companies, experts and officials. Is digital banking really the future: i.e. will be able to digital banking displace from the market traditional banking structures, transfer them into a "niche" position? And what are the main threats that digitalization can bring to the banking sector?

The digital revolution contributed to the development of digital technologies in the financial sector, including banking — Digital banking. These trends, together with the urbanization of the economically active population, have led primarily to an acceleration of the pace of human life and a change in the psychology of the mass customer, which no longer sees traditional banks with their conservative branches, bursts, and often leisurely service as something acceptable to him personally. Fortunately, technology and service providers have emerged, which allow you to carry out all the basic operations required by banks' clients at a distance at a time that is convenient for the client, and not during the strictly allotted hours of banking branches and branches. Banks have started to take advantage of these new features by developing and offering mobile applications to their partners, contractors and customers, improved remote servicing systems and internet-banking. Having a smartphone or tablet and installing a mobile app on it, any customer can make a transfer, pay bills, check the balance, order a new plastic card or lock the old, even open an account and make a deposit. Therefore, the functionalities of bank branches as universal financial hubs, where clients could conduct all kinds of financial transactions, go into the past.

Banking industry is changing rapidly. Two years ago, more than half of the customers

were ready to switch banks if their local branch closes. Currently, the number of expressions of such sentiment has decreased to less than 1/5 of the total number of clients.[1]

Currently, the bank and banking network functional review — is one of the most important tasks of banking institutions. The owners and top management of banking institutions should move in the direction of modern trends, so the old view of bank branches and affiliates as places is unacceptable now, in which funds are moved between the bank and the client. Previously, the growth of the banking network, especially in the regions, spoke about the scale of the banking business, there were the concepts of "key region", "region of the bank's presence". Now the situation has changed.

CHANGING THE ROLE OF BANK BRANCHES

At present, there is no need for a physical presence of banking units in different regions of the country, can limited to a small representation of bank staff who would be functionally responsible for technical support and advice to clients. Banks are now abandoning such representation, moving customer support and interaction with clientele into virtual space, sometimes offering first bots or virtual assistants that can solve the most simple and standard problems. In the US, for example, banks have closed about a third of their branches nationwide in the last five years, that significantly (almost half) reduced transaction costs and had little impact on the number of clients engaged.[2] As for Russia, according to the author, the minimum costs of opening a branch of the bank will cost 15 million rub., and annual maintenance, with a minimum number of staff, will require about 10 million rub.

Therefore, banks, reducing branches and developing digital services, have the opportunity to reduce service fees, reduce loan rates, i.e. offer its clients more favourable terms and conditions. This is another advantage offered by digital technology.

Due to the reduced need for a wide banking network, bankers will have to decide what to do with the vacant space. It is premature to talk about complete dismantling of banking networks in the next 15–20 years — still a significant proportion of clients of pre-retirement and retirement age prefer to go to the bank and there by live communication with the bank officer to make a payment or receive cash.

In addition, in any society there are conservative sentiments, gradually being transformed into the category of "national tradition". So, in the USA, the UK, Malaysia and countries — former colonies of the United Kingdom, customers still pay by cheque, which in the banking system of other countries has never been.

Of course, bank branches will continue to exist in the future, although in some countries (e.g. Switzerland) they will become analogous to elite clubs. It is possible, that will be prioritized functions of financial adviser or private-banking.[3] Branch Bank officers will provide advice on various economic issues, supporting clients throughout their life cycle.

Famous banking expert Dan Raymer also believes that the branches will not disappear. Within the concept of digitalization, banking branches from the main channel of interaction become only one of the means of communication, and in the future will move from the mainstream into a niche, specialized area, will complement other channels of

[1] Accenture. North America Consumer Banking, 2015. North American retail banking product report, 2015. URL: https://www.accenture.com/us-en/~/media/Accenture/Conversion-Assets/Microsites/Documents17/Accenture-2015-North-America-Consumer-Banking-Survey.pdf#zoom=50 (accessed on 12.12.2021).

[2] ABIATEC. URL: www.abiatec.by (accessed on 08.12.2021).

[3] Private-banking — a type of banking service focused on providing a complex of banking and financial services to a wealthy clientele, including a 24-hour personal manager (concierge service). Traditionally carried out in separate specially equipped banking branches.

digital banking business. But the offices will still perform some functions: opening and service of accounts (especially for new clients); counselling (especially on credit and new services) and supporting the bank brand [1].

It should be noted that at present the technology of opening accounts to clients and without their physical presence is improved. Modern software and technical solutions allow to comply with all requirements of the Russian legislation on client identification in the framework of countering the laundering of criminal proceeds and the financing of terrorism, as well as the protection of personal data. Therefore, over time, clients will not need to come to the office to open an account, and the credit card can be ordered through the Internet, and the bank, using its procedures, will check the client and make a decision. The client will receive the PIN-code through the call center and the card will be activated through any ATM of the given bank.

THE MAIN ISSUES IN THE TRANSITION TO DIGITAL BANKING

When reformatting the bank model, its management needs to find answers to the following questions in Digital Banking:

- How many branches does the bank need? Which departments will be built on a self-service system, and which will become consulting centers and sell simple and transactional products?
- How many people do you need in the head office, consulting centers, sales outlets? Maybe it is worth outsourcing some of the functions? What should I do with the employees who are already working? Is there a need to significantly reduce staff or perhaps retrain a number of qualified employees for a new banking profession?
- What are your customer preferences? Is it necessary to reorient the branches to more specialized [branches for Private Banking, Islamic (partner) banking, etc.]?
- What technologies should be used in each department, and how will they be correlated with certain customer groups?
- What other ways of interaction with customers and counterparties should be used by the bank, and how to integrate various technologies, techniques and products into the bank's unified digital systems?

The competitiveness of the bank not only to other financial institutions depends on the correct answer to these questions, but also to various digital companies, gradually but increasingly entering the territory of the banking system.

So, the first property of digital banking — active use of Internet and other digital technologies leading to reformatting of branches, branches of traditional banks — sufficiently significant, but not the main trend of digitalization.

CHANGING THE BANKING PARADIGM

The main thing in the modern processes of transition to digital banking — change of bank behavior when there is a general transformation of the banking paradigm itself. Digital banking means that the bank itself comes to the areas where there are customers. In addition, the digital bank concept assumes that the bank will develop in new areas,— it is in these areas that a financial institution creates special opportunities for different groups of clients. It often offers not only hybrid, transactional products, but also a clear and customer-friendly technology interface with the technical solutions required for this particular category.

Before the era of new technologies, the financial institution declared: "Here I am, here's my product line, here are my customer criteria and conditions,— will be glad to see you as our customers, if you come". Today, in the era of development of virtual systems, the financial institute states that it can determine the location of the client, approximately understood the area of its needs and is ready at any time to provide a range of services for comfortable use.

Within the framework of the new concept of digital services, banking structures, being a kind of virtual intermediaries, are ready to offer all necessary services to the client, not limited to financial operations. At the same time, the bank can create channels of interaction with clients in information services and social networks, in e-business and the Internet of things, in applications to mobile devices, using any virtual space system in which the client may require banking services.

And although it is the technologies of Digital Banking that are the means that gave rise to this new concept in banking, the main thing is that the approach itself has changed.

Digital banking aims to cover all areas of human activity,— financial institutions are active in mobile and social networks, but in other channels the banks are still at the experimental stage. Intensive working at the level of R&D,[4] searching solutions that we believe will be successful.

There are certain opportunities for banks in a new direction called the "Internet of things", where the financial institution needs to find options for embedding in the chain of interaction of customer devices.

DIGITAL BANKING — NEW IN RETAIL OPERATIONS

Digital bank — is a comprehensive business strategy that includes all information channels. We believe it is possible to note that the situation with the transition to digital technologies is changing so rapidly, that banking institutions that have not started the transition process, according to the new concept, will fall so far behind, will not be able to compete with those banking structures that are already being transformed from traditional banks to an ecosystem that provides a set of all virtual services, of which the actual banking operations will be only a small part.

Digital bank — this is the next stage in the evolution of retail banking operations, including mobile payments, online loan systems (including peer-to-peer) and deposits, mobile banking, MPOS,[5] personal financial management (PFM).

Of course, banks need to actively develop and Internet marketing, which will expand the reach of clients, already segregating them into groups based on their needs.

Increased competition in the banking sector, which actively uses digital technologies, has led to special customer demands, especially in terms of speed and convenience of banking operations. Modern customers of a new type — Homo informaticus, people of the generation Z (Next Generation) — there are increased needs and serious opportunities to search for your ideal virtual bank, as these customers want to receive exclusive banking services, selected specifically for them, at any time and it is necessary for them. And this need is quite understandable, as the lifestyle of clients is connected with the Internet environment and virtual space.

It is no longer enough for traditional banks that want to succeed in the transition to a new digital banking platform simply to have an official Internet site and some kind of bank application for mobile systems Android and iOS. Such systems, responsible for consumer loyalty and supporting the sales mechanism, firstly, there are all without exception medium-sized and large financial structures, and secondly, do not give enough significant increase in the customer base, because they are not unique products. Therefore, in today's conditions of increasing competition, both in the banking business and online space, banks need to develop a new unique concept of building information infrastructure and competently present it to the market.

Currently, most credit institutions manage classically formatted multi-level processes

[4] R&D — Research&Development — the direction responsible for analyzing and determining the ways of development of the business structure.

[5] MPOS — mobile points of sale — compact device, which is connected to a smartphone or tablet computer trading terminal.

with special supervision. But these processes in the modern environment allow to retain some of the conservative customers, rather than attract new ones with special needs in digital technology. However, even if traditional banks offer only a few digital services (for example, a mobile bank or Internet service using remote access through a personal account), this is no longer enough, as it is not possible to fully construct an integrated digital banking model for a financial institution.

Most experts believe that it is counterproductive to build digital infrastructure without an integrated approach. It is quite difficult for new players to integrate into the existing digital space, and even more — to form their unique digital infrastructure, sufficiently flexible and effectively developing in accordance with the demands and requirements of a new type of customers.

The pioneers of digital banking were global banking empires that started investing in digital strategy earlier than other banks, as well as next-generation banks that immediately built their business strategy as digital banks. It was they who rightly took the top places of the leading digital banks in the ratings of the largest consulting companies.[6]

The leaders of the digital banking market have already managed to ensure that the interaction of the bank and the client is carried out without the participation of bank employees. Other financial institutions have to double and triple their efforts to catch up with their competitors in this area.

In addition, non-bank companies are entering traditional banking services markets (Google, Apple), developing suppliers of new generation financial products: Moven, Knab, Fidor Bank — in the world Marlket; Instabank, Modulbank, Roketbank — in Russian Federation.[7]

RECOMMENDATIONS OF BANKS TO DEVELOPMENT DIGITAL BANKING

In our opinion, the optimal strategy of the bank should be aimed at such customer service, in which all transactions are conducted quickly and conveniently, and requests are processed in real time,— 24/7.

To achieve this, you should synchronize all service channels, clearly focus product offerings on a specific customer, use end-to-end information processing and constantly communicate with customers online.

At the same time, given the rapidly changing situation in the world of digital technologies, it is necessary to provide flexibility in both IT-systems (allows you to quickly make changes, adjust and change services, channels of interaction, banking instruments and products), as well as in the bank's job descriptions and management mechanisms, to respond quickly to a changing environment without delaying decision-making.

To build a comprehensive digital banking system, you should create a standard and uninterrupted customer service mechanism in any comfortable channel. Often the client is equally convenient to get service as through distance technologies (through a dedicated segment on the bank's website or through a mobile application), and in-person format (through a manager in a branch or through an ATM in a shopping mall). At the same time, all channels of interaction with clients should be integrated with each other, as well as the interaction with the API[8] and with core banking system.

Within the Digital-platform special attention should be paid to the coherence of actions, and the possibility for clients to

[6] Internet banking rank. Deloitte, Markswebb Rank & Report, 2016. URL: https://markswebb.ru/report/internet-banking-rank-2016/ (accessed on 16.12.2021).

[7] Diasoft, BIAN: Digital banking as a strategic direction of development of the modern bank. Site of the journal "Banking technologies". URL: http://bosfera.ru/bo/ekspertiza-bian-i-diasoft-digital-banking-kak-strategicheskoe-napravlenie-razvitiya-sovremennogo (accessed on 15.12.2021).

[8] API — Application Programming Interface, programmable interface for applications — software shell, responsible for interoperability of different applications in a common information system.

manage the virtual services provided by banks is provided. For a modern bank customer, it will be important to be able to customize the channels of realization of banking services with other virtual systems: social networks, search systems, etc. Banks can provide such opportunities if they use an open interface that allows them to integrate their service channels into the information systems used by the client.

Bank information system should be flexible, easy to change and customize, quickly change the structure, remove or add software components developed by various manufacturers, upgrade and modify them. Relevant for the development of modern Digital-platforms is the concept "Open API", i.e. an open programmable interface that manages various applications in a common information system. It is the use of such a concept by banks that will allow banking structures to interact quickly and comfortably with customers, to collect and process information about their needs, offering additional services needed precisely for a certain category of customers.

MODERN MAIN TRENDS IN DEVELOPMENT OF DIGITAL BANKING

Digital banking is now becoming a topic of research in various professional communities, as it is at the junction of finance, IT technologies, sales, both retail and corporate. Head of Digital Banking Department of company Global Digital Banking Nabendu Misra highlighted the following current trends in the most sought-after channel of interaction of the tandem "bank-client" — banking applications [2].

Mobile payments, instant pay

The idea that the phone can be used as a payment card originated long ago, almost along with the creation of a smartphone. However, implementation has only recently begun. Special chips began to integrate into a number of Android smartphones in 2013. A gadget with a similar chip could be used as a payment card. Smartphone and tablet operating systems have improved in Android 4.4, — in 2014, technology was proposed to replace the owner of the settlement card (HCE — host card emulation). Almost all applications based on this OS and later versions will allow for contactless calculations. Apple, starting with iPhone 6, equips smartphones with a special chip. The new Apple Pay method, which allows for contactless payments using fingerprints as an identifier, made it easier for banks to design their iPhone apps.

Software that will allow users to pay for purchases contactlessly, tied debit and credit cards, is now in the assets of many companies. It is predicted a massive replacement of plastic payment instruments with virtual (as it is already practiced PayPal). Visa Company also offers online services within the program "Visa Digital Solutions". There is a similar system in Mastercard.

Contactless payment function is in demand with payers, and banks should be included in this direction, otherwise their place will be taken by non-bank companies.

At present, processes of digitalization of banking services of domestic credit and financial institutions are carried out within the framework of additional sanctions of the USA and EU countries, imposed by them in response to the start of the Russian special military operation in Ukraine in February 2022 year. Sanctions and pressure from leading Western states forced to withdraw from the Russian market or stop serving Russian customers by the world's largest IT-companies, as well as payment service corporations. Cessation of service to Russians by companies Apple, PayPal, Western Union, Visa, Mastercard, American Express, disconnection of some Russian banks from the international SWIFT system forced Russian public and private companies to find alternative payment systems, which will

allow Russian customers to make payments inside Russia and serve abroad. Inside Russia, it is recommended to replace ApplePay with SberPay and use interbank QPS (quick payment system). One of the alternatives to Visa, Mastercard can be a joint project to issue an international plastic card of the National Russian payment system "Mir" and the Chinese payment system UnionPay, supported by most Russian banks. Note that the Chinese national payment system is very widespread in the world: 180 states accept its bank card. To date, more than 3 billion UnionPay plastic cards have been issued.[9] Other options are also being considered, taking into account the existing circumstances, in particular the project for the creation of an international payment system, an alternative to the SWIFT system. Given that all the countries of the Middle East, China, India, South Africa, the Eurasian Economic Community countries, as well as a number of Latin American countries support Russia, the success of the creation and operation of such a system seems quite feasible.

Introduction of the principles of computer games in the banking business

This trend is the application of the principles of computer games to various information channels of interaction between the bank and the client, and is the introduction of options such as obtaining points or granting special status for a deposit of a certain level. The main task, which is solved by the bank,— motivation for regular opening of the application, site, group in social networks. Experts believe that, unlike other digital initiatives, these efforts are ineffective, as it is difficult to assign additional points to the customer, however, being financially low-cost, this option of attracting and retaining customers has the right to exist and will be demanded by part of the customer base.

[9] UnionPay. Official website. URL: https://www.unionpayintl.com/ru/ (accessed on 18.04.2022).

Multitasking in one digital banking product

Digital Banking is now becoming a competitive advantage, and financial institutions are working to produce customized digital products to attract customers, but within a single banking application. Thus, one of the most demanded services against the background of the growth of labour migration is the system of remittances. Traditional industry leaders were companies with history: Western Union and Moneygram. However, everything has changed, and now most of the market is occupied by online transfers companies Xendpay, Transfer Wise and Xoom at the expense of the convenience of their services and advantageous tariffs. The financial institution can not only provide in its proprietary application additional functions for mobile devices, such as money transfers, utility payments, currency exchange, but also carry out various advertising companies and market research.

Special products can be offered to customers for money transfers in the territory of individual countries (transfers to CIS countries will be in demand for Russia), replenishment of electronic wallets, transactions with financial instruments, etc.

Multichannel banking — synchronized customer service in offices and in the digital environment

Financial institution, being able to track through its application the search activity of the client, can quickly prepare an individual proposal designed for a specific client or a narrow group of clients. In this case, the proposal can be announced through any communication channel. After face-to-face customer consultation in the branch, the bank staff can prepare the appropriate product and distribute it by calling through call-centers or via push notifications in applications.

Banks need correct and up-to-date information about their existing and potential customers, therefore, they should use the maximum amount of useful information

from social media profiles and analyze what banking products can be offered to them.

Customer location and customer activities

Location of any person, and especially a customer whose phone bank knows, can be tracked through triangulation (search and display of the phone by base stations via GPS or BLE systems[10]). Such information is in demand by companies that can prepare marketing reports, targeting service customers and advertisers to a specific target audience, this allows for a more targeted approach to potential clients, already knowing their basic needs and location. Interesting data on the history of visits to different sites, search queries, movements, as well as any demographic data, such as marital status, family composition, child availability and age, social status. This information, not being personal data under Russian legislation and therefore in the public domain, is actively used by banking structures in marketing activities [3].

So, access to virtual channels for the collection and analysis of any information enhances the capabilities of banking structures, because in this way banks will be able to better understand the needs of their customers, more accurately build different customer profiles, which will give them a competitive advantage and provide commercial success.

But there is another aspect that is important to consider when engaging in digital banking — information security.

INFORMATION SECURITY OF FINANCIAL INSTITUTIONS — KEY ELEMENT OF DIGITAL BANKING

Transition to the concept of Digital Banking implies a special role of Digital and Internet technologies, which carries significant information and commercial risks. The threat of cybercrime is also a major concern.

Cybercrime is recognized as the most serious in terms of material and moral damage, targeting individual banking structures and the financial sector of the country as a whole. Crimes are directed to accounts and information systems of credit and financial institutions, intruders try to steal financial resources from correspondent accounts, including in the system of the Bank of Russia.

At all stages of implementation of digital banking operations — from the development of new software methods and technical solutions to the implementation of banking products to their clients — management of credit institutions should be aware of the risks, especially possible vulnerabilities of information security systems. Some banks think about investment in information security systems only at the initial stages of development of new systems. However, we believe that this approach is not realistic. And our opinion is supported by real-life situations, when criminals find vulnerabilities in information banking systems and commit multimillion-dollar thefts already in the first weeks after the project launch. Only then, convinced of the insecurity and inadequacy of their defenses, do commercial banks have to turn to developers, which with their successful experience in establishing reliable security systems, can provide banks with comprehensive and continuous information protection.

In an era of rapid development of information technologies, which allow business entities to expand the range of their operations, to reach more clients and therefore profit more, information security issues become key. It is by how much attention banks pay to the construction and improvement of information protection systems; it is possible to judge the maturity of business. The seriousness of the approach to early identification of potential threats and timely response to these threats to banking

[10] BLE (*bluetooth low energy*) — Bluetooth with low power consumption, which is based, inter alia, on the Apple iBeacon technology. This is a way to locate the user with an accuracy of 10 meters, while sparing the battery of the device.

information systems is determined by the stage at which the information security service is involved in all banking processes. Note that at present modern large financial structures already have the ability to successfully solve the problems of information protection, using their full-time specialists.

At the same time, it should be noted that in the field of information security there are two important categories: threat (potential risk of cyber-attack) and attack (direct attack on the information system for the purpose of stealing confidential information and/or money). In the event that potential threats are not considered, unprotected information systems will be attacked, resulting in serious, and sometimes catastrophic financial losses. In this case, it is often the client who bears most of the loss, because he is the least protected, although connected with banks through remote systems of service. Therefore, it is advisable for banks to start with the protection of the client, providing him with a reliable information security system.

The situation with cybercrimes against banks and their clients remains tense, both in Russia and around the world. Association of Russian Regional Banks reported that in the Q4 of 2015, cybercriminals kidnapped from banks — members of the Association — amount exceeding 1.5 billion rubles [4]. In 2016, at least 8 major cyber-attacks on information systems of banking structures were recorded in Russia. Only timely joint actions of employees of information protection of commercial banks and regulator allowed to reduce the real damage from 5 billion rubles to 300 billion rubles.[11] But cyberattacks are also possible on the protected systems of the Central Bank of the Russian Federation. In July 2018 cybercriminals with the help of virus malware managed to gain access to the automated workplace of the Bank of Russia client without authorization and steal 58 million rubles from a correspondent account, by assigning them to plastic cards of clients in 22 largest Russian banks. Within several hours, most of the funds were cashed [5]. Massive transition of banks to online customer service in 2020–2022, caused by the spread of the coronavirus pandemic, significantly worsened the situation in the field of virtual crimes against banking structures. According to expert assessment of specialists of Sber, the losses of the banking system of Russia from cyberattacks amount to about 600 billion rubles per year.[12]

Cybercriminals continue to improve their knowledge and skills, gradually gaining specialization in narrow areas. Thus, the specialists, who are ready to scan the organizational and technological components of the information system of banks and discover all potential vulnerabilities, have become particularly in demand lately. Based on the data obtained, cybercriminals are ready to provide their recommendations on the optimal hacking of banking systems and concealment of criminal activities. Such "expert" recommendations have already become the subject of active sales, including, at the level of States, not to mention criminal associations [6].

The number of crimes of theft of money from bank accounts increased intermittently using social engineering and neuro-linguistic programming, when criminals, having received part of the personal data of the bank's customer by telephone communication, are force him to report card data, gain access to the client's account or office and remotely steal money from bank accounts. However, given the overall scale of thefts, which reached hundreds of billions of rubles in a year, the banks are joining efforts to create systems to counteract such crimes (including active operational and preventive activities involving law enforcement agencies), create

[11] ARinteg. Current solutions for information security. 2016. Proceedings of the X International Conference. "Bank cards: practice and transformation", 14–15.04.2016 r. Moscow; 2016.

[12] Sberbank. Official website. URL: https://www.sberbank.com/common/img/uploaded/files/info/ir_presentation _march_2019_rus.pdf (accessed on 18.01.2022).

special units and create detailed instructions for customers [7].

Despite the active work of banking structures together with the Bank of Russia in the field of counteracting virtual crime, the situation in the field of information bank security remains not only dangerous, but is approaching a critical level. Currently, cybercriminals, united in organized groups, direct their efforts to attacks of the banking system, especially — the information system of the Bank of Russia. Not only client accounts but also correspondent bank accounts are threatened. This is a systemic threat!

An additional threat is posed by former employees of banks who had access to internal confidential information, relating to information security mechanisms and procedures, retention and withdrawal of funds. Such specialists become more in connection with the planned work of the Central Bank of the Russian Federation to improve the banking system, as a result, many banks lose their licenses, and, accordingly, the employees of these banks — work. It is obvious that, knowing information about the internal banking IT-infrastructure, intruders become owners of virtually unlimited opportunities: here and central ABS — Automatic bank system (storing all client account data), and automated workstation of Bank of Russia customer — AWS of a BoR (enable the transfer of financial resources from one account to another), and SWIFT system interface (for interaction with foreign banks).

One of the most vulnerable places remains AWS of a BoR, because the software for all AWS of a BoR is the same, and work with it is strictly regulated by the Bank of Russia. This attracts cybercriminals, as they study systems, choose the bank with the least security, select the methodology of hacking, attack this bank, access the funds in the correspondent account and transfer them to several other banks. Then, perhaps, the intruders "split" the funds on smaller amounts, distribute them into card accounts of retail customers and cash out. This is one of the possible schemes of cyber-attack of criminals from the moment of hacking the information system to getting the money at their disposal. In the framework of countering cybercrime against banks, the Central Bank of the Russian Federation has developed a system of measures for secure work with the AWS of a BoR system [8].

In general, banks can be advised to take three main practical steps to protect this weak link. First, allocate AWS of a BoR in a separate network segment and minimize access to it at the network level. Second, the host of their corporate domain (this is extremely important because domain security is very difficult to maintain). Third, the maximum limit of what happens inside the operating system in the host AWS of a BoR: only authorized software and only pre-authorized processes.

We believe that tightening of control by the regulator, as well as wide informing of IT-specialists of banks about the possibilities of counteraction, engaging law enforcement agencies and bank clients, including retail, and cybercrime prevention can reduce the number and intensity of cybercrime attacks against financial institutions. However, researching the current situation in the field of information security in the Russian banking sector, it is possible to assume that common efforts may in the near future lead to an improvement in the protection of AWS of a Bo R.

But cybercriminals will have many opportunities to realize their intentions in other systems. There are still many vulnerabilities in the SWIFT international interbank transfer system. In addition, the intruders, having access to the automatic banking system (ABS), can falsify payment data, then send it to AWS of a Bo R. In the absence of additional protection systems, special shields between these systems, and given that AWS of a BoR works automatically, the system threat may again arise.

In addition, it should be borne in mind that domestic and international

information channels are interconnected and interdependent, so vulnerability, for example, in one remittance and payment system, a bank's information system may be adversely affected, or unauthorized access to one bank's ATM may lead to illegal debits from clients' accounts in another bank. The variety of available arsenal of virtual attacks reduces the expediency of countering them at the last stage.

The situation with cyber-attacks in late February 2022 became particularly escalated. Then all automatic systems of Russian state structures, ABS of Russian banks and sites of systemically significant companies were cyber-attacked within the framework of cyberwar deployed against Russia (hybrid war) on the part of highly professional and well-organized hacker groups commissioned by the USA and a number of EU countries in response to the 24 February 2022 Russia's special military operation in Ukraine. International hackers with the task of causing any damage to the information systems of Russian financial and non-financial structures, often direct their efforts to destabilize it is the Russian banking sector, realizing the systemic importance of the banking system for the overall economic situation in Russia.

It is now that the risk of cyber-threats is multiplied in the most difficult conditions, the risks and costs of any failure to build a system to counter cybercrime are increasing. Therefore, in these circumstances, it is so important to address the problem of developing and improving comprehensive measures to counter virtual cybercrime — from physical access control to computer and banking equipment to virtual security systems. The general opinion of the experts is that it is not possible to construct a completely safe system that excludes any unauthorized action [9]. But the challenge is to create such protection, which is technically difficult for criminals to overcome, expensive, long, and, therefore, this makes no practical sense to them.

CONCLUSION

Digital banking, both in the world and in Russia, is at the beginning of development, banks in this business do not have enough experience, first of all, they should start by changing the mentality, in the beginning — at the management, then — at the staff. Financial institutions should at this stage act quickly enough, but thoughtfully, try to take the best of the already active participants in the digital space. It is recommended that legislative constraints be taken into account when introducing new technologies. When attracting customers and tracking their needs we believe it is important to find a "golden middle" between obtrusiveness and perseverance.

The restructuring of the banking system, which envisages the transition to Digital Banking, assumes that the banking service will become more convenient, comfortable, accessible and safe for the client.

Financial institutions as they enter the digitalization process of their business should get closer to the client. Their main functions will change: from creditor and debt collector, banks will transform into financial advisor and assistant [10]. Such metamorphoses will increase the competitiveness of the banking sector, as well as attract new customers, including from the new generation of Homo informaticus.

At the same time, we believe that without the construction of a reliable and multi-circuit information security system, the bank will not be able to protect its financial resources and the funds of clients from cybercrime in the digital space. In addition, countering criminal cyberattacks should take place within the framework of effective cooperation between government authorities, financial institutions and their customers of various categories, including retail. It is the coordination of joint and joint efforts of all these actors, based on the principles of equal access to sensitive information, provide protection and contribute to the development of the domestic

financial sector, including regional segments, which will strengthen the ability to make secure and fast digital transactions.

Digital technologies have not only brought comfort to the clients of financial institutions, but have also changed the way of life of most of them, their needs and mentalities. On this basis, banks are transforming from traditional financial institutions into structures that create new digital business systems to provide services that are only formally linked to the holding's banking core. The example of the largest Russian bank, which left only a part of the previous name — "Sber" and who removed the word "bank", is very significant and determines the leading direction in which all banking institutions, including regional ones, will be transformed. As development progresses, new challenges and vulnerabilities will emerge, but it is — a natural evolution that will determine the development of the Russian financial sector in the coming decades.

While this publication was being prepared, there were events that fundamentally tested the strength of the entire economic structure of the Russian Federation, in particular the core of the economy — the financial sector. But, despite the systematic imposition of unprecedented economic, financial, and political sanctions by the US, the EU, and other countries, as well as the massive withdrawal of a number of significant and leading Western companies from the Russian market, the domestic banking sector has overcome, having suffered relatively small losses, showing the existence of serious immunity to unfriendly actions of external forces, mechanisms to reduce and neutralize external shocks, flexibility in making quick decisions, and demonstrating coordination of joint efforts with State oversight bodies. According to the forecasts of well-known experts, the Russian financial system will be forced to exist under the conditions of Western sanctions for a long time [11]. Therefore, it is necessary to use this false period for the development of their own digital technologies (independent of western payment and settlement systems), strengthening of the national currency, promotion of the digital ruble, training and advanced training of specialists in digital banking technologies and information security. Such a set of measures will allow the progressive development of digital banking services in Russia, ensuring the independence and reliability of the domestic banking system, despite external restrictions and sanctions.

REFERENCES

1. Reymer D. Personal website. URL: http://denreymer.com/digital-banking-branch (accessed on 10.12.2021). (In Russ.).
2. Nabendu M. Global digital banking. Linkedin. URL: https://www.linkedin.com/pulse/future-digital-banking-2015–2016-nabendu-misra (accessed on 06.12.2021).
3. Kolezneva A. V. Application of biometric-based identification technologies in banking systems. *PRO-Ekonomika = PRO-Economics*. 2018;(3):6. (In Russ.).
4. Aitov T. Presentation at the panel discussion "Mobile security and IT infrastructure of security management". In: Infoforum 2016 materials (Moscow, February 4–5, 2016). Moscow; 2016:12–16. (In Russ.).
5. Kondrashin M. Cyber attacks on banks: Trends, vulnerabilities and the role of the regulator. Website of the PLUS Magazine. July 27, 2018. URL: https://plusworld.ru/professionals/kiberataki-na-banki-trendy-uyazvimosti-i-rol-regulyatora/ (accessed on 15.02.2022). (In Russ.).
6. Petrova E. V., Kuznetsova T. E. Digitalization in the banking industry: Digital transformation of the environment and business processes. *Finansovyi zhurnal = Financial Journal*. 2020;12(3):91–101. (In Russ.). DOI: 10.31107/2075–1990–2020–3–91–101

7. Pashkovskaya I.V. Trends in the development of digital banking. *Aktual'nye problemy i perspektivy razvitiya ekonomiki: rossiiskii i zarubezhnyi opyt.* 2019;(3):46–52. (In Russ.).
8. Yakubenko V.V. Financial technology used to provide banking efficiency. *Teoriya i praktika obshchestvennogo razvitiya = Theory and Practice of Social Development.* 2019;(1):72–76. (In Russ.). URL: 10.24158/tipor.2019.1.13
9. Vasilyev I.I. Principles of organization of credit institutions in the digital technological environment. *Russian Economic Bulletin*. 2019;2(5):218–221. (In Russ.).
10. Bataev A.V. Evaluation of the world market of cloud technologies in the financial sphere. *Vektor ekonomiki.* 2019;(6):91. (In Russ.).
11. Achapovskaya M. Digitalization of the economy as a driver of innovative development. *Bankauski vesnik = Bank Bulletin Journal.* 2019;(3):52–58. (In Russ.).

ABOUT THE AUTHOR

Ilyas A. Zaripov — Cand. Sci. (Econ.), Assistant Professor, Plekhanov Russian University for Economics, Moscow, Russia
iliyas888@yandex.ru
https://orcid.org/0000-0002-0261-6592

Conflicts of Interest Statement: The author has no conflicts of interest to declare.

The article was received on 20.01.2022; revised on 10.02.2022 and accepted for publication on 12.03.2022.
The author read and approved the final version of the manuscript.