

DIGITAL TRANSFORMATION OF BANKING SERVICES IN RUSSIA

Etembekov R.K.

Financial University under the Government of RF, Moscow, e-mail: Hotline3773@gmail.com

In this article the author describes the process of digitalization of the banking services sector in Russia on the example of well-known Russian banks, problems and prospects for the development of digital banking in Russia at the present time, the author's point of view on the general process of digitalization of banks is given, a legal point of view on the process of digitalization is considered, the problem of cybercrime in modern Russia is assessed. At the moment, Russia is at the stage of active development of digital banking; the state is supporting banks on the path to achieving a digital future. Many leading Russian banks are setting up research laboratories to search for new technologies for implementation. However, cybercrime has an extremely negative effect on the development of banks. Banks fight this serious threat by introducing new technologies, improving security, using sniffers to track fraudsters, and using client notifications to alert them to all possible methods of stealing their personal information. The Russian Federation supports banks in this by creating various security protocols and programs, for example, a biometric identification system. In general, all opportunities are open for Russian banks to digitalize and improve the quality of their services.

Keywords: digitalization, banking services, banks, cybercrime, net gain

Digitalization is inextricably connected with the society of the 21st century. More and more spheres are influenced by rapid technological development. Economy is situated at the forefront of the changes. A significant part of economy – financial sector – is being fulfilled with new technologies and innovations in interaction with computers and machines. This article is going to analyze the process of digitalization flowing in Russia. The results of digital revolution on banking services are the implementation of Digital Finances, Internet of Things (IoT), mobile platforms and Artificial Intelligence (AI). Today it is an axiom, that in the nearest future the preferred influence on type and character of financial interactions will have digitalization. Even today we already consider banks as high-tech companies [1].

Purpose of the study. Observe the process of digitalization of banking services in Russia and highlight the main stages of digitalization in general.

Research material. Scientific articles, reports of banking associations of Russia, scientific research, open electronic sources

Results of the research

1. Digitalization in Russia on the example of banks

The process of digitalization in Russia started at the beginning of 21st century. In Russia there was opened the first digital bank in the world- Tinkoff Bank. It was unnecessary to finance creation of departments in different cities. The more rational thing was to build an integrated financial system, which can correspond to many accesses from different parts of the world. Today Tinkoff Bank is the biggest digital bank in the RF, at the end of Q1 2017 net profit was 3.4 million of rubles and with index RoS (Return of Sales) of 43% [2, p. 7].

One of the main players on the financial arena of Russia is Sberbank, that shows the biggest percent of innovations integrated. In 2015-2017 Sberbank introduced approximately 20 innovative projects based on digitalization, from controlling the bank accounts via platform Etherteum to digital workflow and different bonus programs [3, p. 2]. The expenses of Sberbank to innovative projects show a tendency of growth. In a quarterly report, the bank notes that it is actively using AI technologies, implementing AI processes with the help of almost a thousand of its data scientists. The effect of the implementation of AI initiatives at Sberbank in 2019 was estimated at 42 billion rubles [4, p. 78]. AI is integrated into the Sberbank platform at all levels. Eight platforms were put into commercial operation, including NLP, Speech Analytics, biometrics and others. According to calculations, Sberbank increased net gain by 73,31%. Table (1) represents net gain of 5 main banks in 2020 in comparison with 2016. Data in the table allows us to assume, that one of the main reasons of growing net gain is the implementation and introduction of new technologies into banking services. Sberbank steadily takes the leading position in the list, having a significant lead over other banks. Therefore, Sberbank is an object of interest [5].

In the Central Bank of the RF was opened a “Department of financial technologies, projects and organization of processes”. This department is analyzing new technologies and seeking for possible ways of implementation of these technologies into financial sector of the RF. There was created an association “Fintech”, where the biggest representatives of Banking sphere of Russia became participants – The Bank of Russia, VTB, Sberbank, Alpha-Bank and others [2, p. 6].

Table 1

Net Gain of the first five biggest banks in the RF

Position	Bank	October, 2020	September, 2016	Change, thousand of rub.	Change, %
1	Sberbank	559 412 190,00	322 787 679,00	236 624 511,00	73,31
2	Alpha-Bank	180 692 333,00	-8 823 989,00	189 516 322,00	
3	VTB	52 193 737,00	42 340 524,00	9 853 213,00	23,27
4	Bank "Otkritie"	40 338 773,00	6 824 406,00	33 514 367,00	491,1
5	Tinkoff Bank	25 363 014,00	5 075 258,00	20 287 756,00	399,74

2. Process of digitalization of banking services itself

Digital transformation of banking services is a part of digital economy. At first digital economy touched only banking services, but now it penetrated everywhere, starting from digitalization of documents and ending with robotization of manufacturing. Digitalization itself is a high investment-required process. Digital Banking- is not only an interface applications and multi-channel customer service, but also offering an exceeded and full client service via automated processes everywhere, where there is an Internet access.

As all banking services are performed online, banks need to protect their data from malfunctions in the system stability and cyber-attacks. The whole work must be arranged with high precision. There must be used new systems to help banks integrate technological advantages. For example, BPM-systems (business process management) that coordinate the overall system of a facility with using means of automatization and integration of IT-technologies, that are necessary in making decisions. Another significant and important part of digitalization of banking services is Intellectual System of Control (ISC). The purpose of such systems is to optimize the work of managers, to minimize the level of human work at all levels and to transfer many processes in an automatic mode, which is seen on the example of Sberbank [2, p. 10]. Furthermore, banks need to analyze and protect data. One of the modern systems of protection of banking services performed online is Unified biometric system (UBS) – digital platform, created by “Rostelecom” company on the initiative of Ministry of connection and mass communication of the RF and the Central Bank of the RF, of identification by voice and face [6]. The implementation of distant identification in the financial sphere is regulated by Federal Law № 482-FZ on December 31, 2017, that makes changes into Federal Law № 149-FZ “On Information, Informational technologies and protection of information”. As part of the development of the Unified Biometric System, “Rostelecom”

has implemented a platform for detecting attacks on biometric presentation – BIS Platform [6]. The company announced this on November 27, 2020. A multi-level information security system allows to repel an attack at the moment, when receiving a banking service or purchasing goods and services, the user confirms his identity – records a video and says a sequence of numbers. The solution developed by BI Solutions, a Russian developer of solutions in the field of information security and biometric technologies, allows the simultaneous use of technologies from different developers. Banks also need to establish a special IT department, involved in coding and protecting data of customers. The success of banks is also estimated with their ability to protect personal data of customers.

To create a system of protection of personal data, banks operate with Federal Law “On personal Data”. Since the data is stored in automated bank system, that has different levels of protection, there are special standards of personal data protection established by the Central Bank of RF. In Russia today there are several standards that regulate such relations. These standards prescribe the construction of several subsystems. These subsystems are: 1) Systems of authentication, access and control of personal data; 2) the registration of personnel’s actions related to personal data of customers and avoidance of illegal actions; 3) provision and maintenance of unified informational library of personal data; 4) internetwork security, that excluding access to personal data for those users that have no permission for it. In terms of decentralized systems, it is necessary to install cryptographical elements for encryption and protection of transmitted data [7].

Another very important point is that banks should aim at increasing the quality of interaction with customers and attempts to improve this interaction to new levels. Today customers are satisfied with a very quick service and convenient options. This ideology is not based on assumptions and myths. To increase productivity and Index NPS (Net Promoter Score), banks need to increase the quality of services pro-

vided and reduce processing time [8, p. 3-4]. In general, in Russia Banks, being involved in process of digitalization, pass several steps, represented on Fig. 1.

3. Cybercrimes and banking in the 21st century

At the beginning of 1990 the whole world faced cybercrime. A high proportion of informational technologies in all the spheres of the world, including financial sphere, in the 21st century gave a strong stimulus for development of cybercrime [9].

Cybercrime society uses a wide range of tools: from spam and targeted messages to hacking software and hardware. Mass character acquired theft of money, personal data of customers, evidence that include trade secrets, malfunctions in mobile devices and applications, hacker attacks via harmful software and trojans, DdoS- attacks, blackmail of owners of personal data and credentials stolen. According to Positive Technologies, the line between cybercrime and other types of illegal activity has been increasingly blurred in recent years. A significant part of the incidents is not directly related to the theft of money, but only to the theft of confidential information, when hacking computer systems is a preparatory stage for conducting fraudulent schemes and operations that cause financial, economic and even political damage.

Speaking about financial sphere, the main aim of attacks is still financial benefit (about

62%), but a percentage of data theft is increasing. This happens due to the fact, that operations aimed at obtaining data, in most cases also contain financial connotations: stolen data are subsequently used to steal money. The main attacked system remains the processing of bank cards. Hackers try to get to the interface of the processing control system, regardless of its type, or to the database server in order to secretly increase balances and limits of previously prepared and the cards in the possession of their accomplices. Then on these cards all are removed available funds through ATMs. Theft of information from financial institutions has already become a multifunctional criminal business. Passwords and logins from various credentials, bank card details occupy about 80% of all information sold on the shadow Internet networks. The tendency of growth of attacks, aimed to obtain personal data, will continue. The criminals will continue to attack weak points in informational defense in order to theft personal data. In the zone of increased risks are also financial facilities, including banks. Methods of hackers do not remain unchanged. To hack and bypass protection methods hackers use novel harmful programs or modifications of traditional viruses. They more often use complicated and multi-stage tools, including many different processes, to successfully perform an operation. Common delivery method malware remains phishing mailings [10, p. 52].

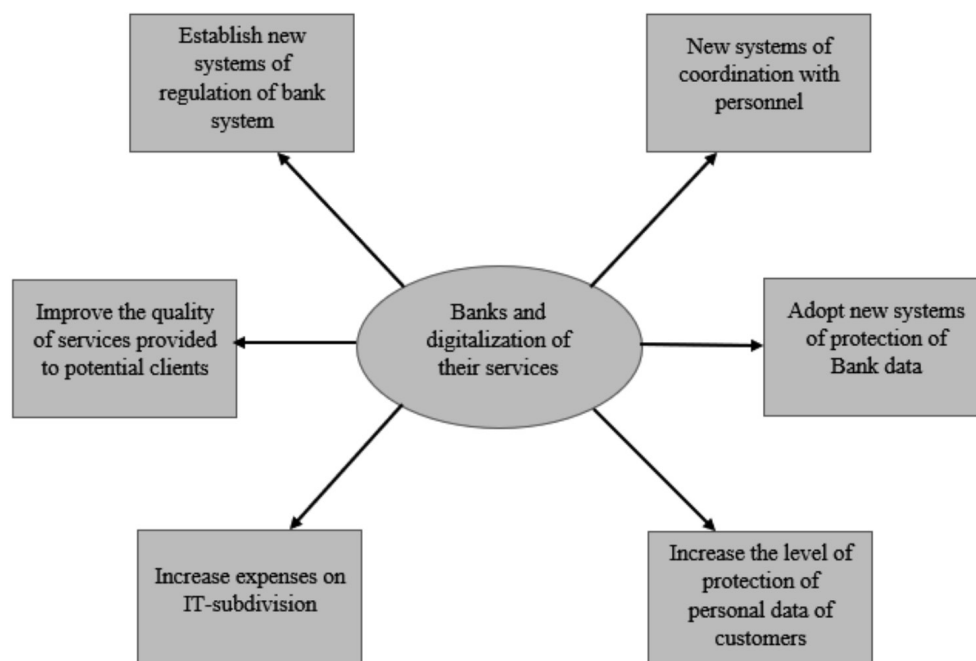


Fig. 1. Steps in digitalization of banks in the RF

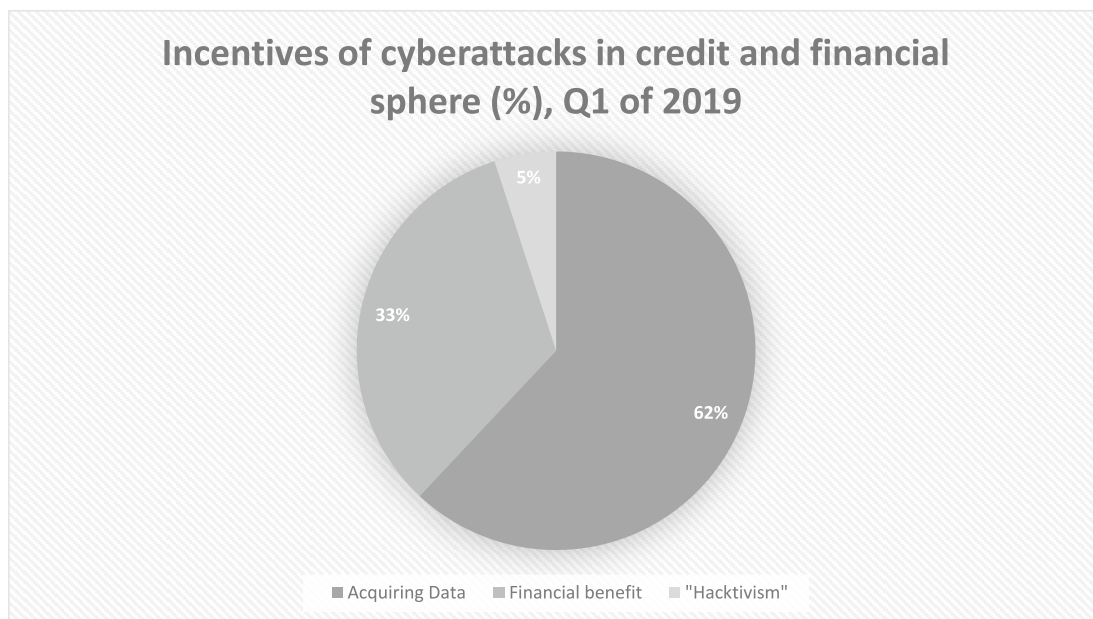




Fig. 2. Incentives of cyberattacks in credit and financial sphere in the RF

Table 2

Problems of digitalization in the RF

 State	<ul style="list-style-type: none"> · In case of massive automatization new approaches for education will be necessary · New kinds of facilities and relations will demand new type of regulation and control · All people will be involved to digital economy partly with assistance from the state. There also required a digitalization of state and municipal services
 Companies	<ul style="list-style-type: none"> · There must be presented an ideology of permanent innovations. · Success of digitalization is connected with cooperation with educational and research centers, as well as high-tech companies

Monitoring results of BIZONE show that 27-30% employees of Russian companies open emails with malicious attachments allegedly from contractors and colleagues. But e-mail is far from the only way for viruses to spread. For example, users are actively downloading files from torrent trackers, which means the risk infection increases many times. There is a noticeable increase in infections ransomware. This type of cybercriminal activity is increasingly used in combination with phishing. In the future perspective social engineering and harmful software will be the main weapon in the hands of hackers. Banks will have to face a serious power, and they will have to struggle with it via introducing new technologies, improving the defense, using sniffer programs to track scammers. Another effective method

is customer notifications. This method is used today. Banks will notify users about possible and new ways of scammers to theft information from direct interaction with them.

4. Perspectives and problems of Digitalization in the RF

Digitalization sets many problems to both Russian Companies, including banks, and state itself. Some of them are represented in Table 2 [11, p. 4].

From one side massive automatization require availability of people, that aware, how to operate with machines and computers. That is why education is becoming more and more demanded nowadays. State must revisit process of education fundamentally to fit the requirements of today's paradigm. Furthermore, new kinds of relations and entities will demand a

completely new methods of regulation. In case of banking services, as all of them are being digitalized today, Russian government should continue to develop normative acts, that concern the activity of banks in the sphere of digital economy. But the state itself must keep up with the times. Transformation of the most state services into digital world will push people to interact with the new digital world, including both the digital economy and digital banking [11, p. 51-53].

From the other side companies, as well as banks, must accept the ideology of permanent innovations. The world today is very dynamic and quick, new technologies appear every time. The subjects of economy must adopt these technologies very fast and even try to develop its own exclusive developments in order to remain competitive. As it was said before, education is very important. Banks can sign contracts with educational centers and retaining centers to teach their employees with new skills and abilities.

For Russia itself involvement of digital economy and digital banking is very perspective. According to the data of global institute McKinsey, expected economical effect of involvement of digital economy in the RF to 2025 will be 4.2-9 billion of rubles or 20-35% of expected growth of the whole GDP [2, p. 3]. [11, p. 4]. In terms of market volume and structure, as well as institutional and regulatory environment Russian fintech sector is at an early stage of development. Open development in perspective legislation can give fintech companies every chance to become from innovative laboratories to aggressive competitors to classic banks and even press their positions in the market. Only in 2016 the number of companies on Russian market of fintech services increased by 1/3. The small number of such companies can be explained that on the Russian venture market there are few huge private investors or the fact that they prefer to invest abroad, and state investors are reluctant to invest in risky startups in the early stages of development of the project. An important perspective is the development of mobile offline payments. In China e-wallets in the form of applications for smartphones, for example, Alipay, WeChat Pay and Caifutong have become the daily lives of consumers. Despite the fact, that the use of QR codes to pay for purchases did not take root in Russia, new technological solutions (such as NFC technology, used providers of mobile payment systems – Apple Pay, Google Pay, etc.) has potential for distribution among Russian consumers. Institutional

infrastructure of Russian sector is on the first stage of development. There are already sectoral incubators and accelerators of involvement of technologies, for example Future Fintech, and huge banks have created their own laboratories (“Alpha-Laboratory”, “Sberbank Technologies” and etc.) [11, p. 96-97]. Successful examples of coordination of banks and fintech companies arise. For example, in mortgage lending, Tinkoff Bank acts as an interface for attracting customers and interacting with them, while partner banks are directly involved in mortgage financing [11, p. 97]. If the regulatory and infrastructure environment will begin to transform at an accelerated pace, the role of fintech companies may become more meaningful. Removing obstacles to development financial technologies (including the opening of banking APIs and the ability to identification of clients without their personal presence) will lead to market redistribution in favor of new players. In this scenario, traditional banks have a risk of becoming an industry infrastructure – similar with reinsurance companies in the insurance market. In its turn high-tech innovative companies close to customers and transactions, such as payment systems (Visa, Mastercard), providers mobile payment systems (Apple Pay, Google Pay), financial aggregators services will become the masters of client preferences.

Conclusion

Even today we can see all the benefits and drawbacks of digitalization of banking services. A lot of operations are executed online, without direct presence at the bank. We can safely transfer money to any person in the world, contact with the bank’s support services in convenient mobile applications, pay with our phones without credit cards, use our biometrics to perform all the operations connected with finances and many other things. Digitalization is going to change our life completely. Despite of the fact, that due to digitalization we gained a new weak point represented by our personal data, stored in the banking servers, it became easier for us to perform all the functions necessary today. Banks are concerned about the protection of personal data of their clients and the quality of protection is being improved day by day. The Russian Federation is fully trying to force the current trends towards digitalization, which can be seen from the regulations adopted by the Central Bank and the government of the Russian Federation. Banks itself establish laboratories, aimed at creating new technologies, organize festivals, where people can present their start-ups in the digitalized banking.

In general, the enhanced process of digitalization in Russia only begins, and there are many perspectives and barriers, which we will have to overcome.

References

1. Khubulova V., Seregina Ya. Khachatryan M., Digital Transformation of the financial sector of the economy // Expert Council Bulletin. 2019. № 3 (18). P. 48-51.
2. Miroshnichenko M.A., Trelevskaya C.-A.I., Mamykina E.V. Studying the process of "Digitalization" of the banking sector within the framework of the ecosystem of the digital economy in Russia // Scientific journal KubSAU. 2017. № 133 (09). P. 1-14. Doi:10.21515/1990-4665-133-034.
3. Svetlana Yu. Pertseva Digital Transformation of the financial sector // Innovations in management. 2018. P. 48-52.
4. Annual report. 2019. Sberbank [Electronic resource]. // URL: <https://www.sberbank.com/common/img/uploaded/files/pdf/yrep/sberbank-ar19-rus.pdf>.
5. Banks rate on Netgain // URL: https://www.banki.ru/banks/ratings/?PROPERTY_ID=30.
6. Unified Biometrical System, BIS Platform [Electronic resource]. // URL: [https://www.tadviser.ru/index.php/Продукт:Единая_биометрическая_система_\(ЕБС\)#.2A_.D0.92.D0.BD.D0.B5.D0.B4.D1.80.D0.B5.D0.BD.D0.B8.D0.B5_BIS_Platform](https://www.tadviser.ru/index.php/Продукт:Единая_биометрическая_система_(ЕБС)#.2A_.D0.92.D0.BD.D0.B5.D0.B4.D1.80.D0.B5.D0.BD.D0.B8.D0.B5_BIS_Platform).
7. Protection of personal data in banks [Electronic resource]. // URL: <https://searchinform.ru/resheniya/biznes-zadachi/zaschita-personalnykh-dannykh/realizaciya-zashchity-personalnyh-dannyh/perechen-personalnyh-dannyh-podlezhashchih-zashchite/zaschita-personalnykh-dannykh-v-bankakh>.
8. Votintseva L., Andreevna M., Kovalenin I., Votintsev R. Digital transformation of Russian banking institutions: assessments and prospects // IOP Conference Series: Materials Science and Engineering. 2019. № 497. P. 1-6.
9. Dementeva M.A., Likhacheva V.V., Kozyrev T.G. Cybercrimes in the banking sector of the Russian Federation: ways of identifying and combating // Economic Relations Journal. 2019. Vol.9. no. 2. P. 1010-1019.
10. Association of Russian Banks "Russian banking system today. Interaction of real and financial sectors in conditions of digitalization of economy". September 2019 [Electronic resource]. URL: https://asros.ru/upload/iblock/c30/20397_informatsionnoanaliticheskoeobozreniesentyabr2019.pdf.
11. Alexander Aptekman, Vadim Kalabin, Vitaly Klintsov, Elena Kuznetsova, Vladimir Kulagin, Igor Yasenovets Digital Russia: New Reality. 2017. // McKinsey report.