Hochschule für
Wirtschaft und Recht Berlin
Berlin School of Economics and Law

Master of Arts (M.A.) - International Economics

The digitalization impact on the performance of the Russian banking sector. Trends and cyber threads

Master Thesis

Berlin School of Economics and Law

Summer Semester 2020

Supervisors: Prof. Dr. Martina Metzger

Lecturer Dennis Uckel

Word Count: 31828

Submission Date: 2nd November 2020

Name: Anastasiia Samsonova (s_samsonova18@stud.hwr-berlin.de)

Student ID: 77211728792

Name: Polina Voronina (s_voronina18@stud.hwr-berlin.de)

Student ID: 77211730405

Table of contents

List of figures and tables

FIGURES

TABLES

List of abbreviations

AIPS – Automated incident proceeding system

AM – Asset Management

AS – automated system

ATM – Automated teller machine

BLUE – best linear unbiased estimator

BRICS – Brazil, Russia, India, China and South Africa

BS – Bank Size

CEMEA – Central and Eastern Europe, the Middle East and Africa

CI – Confidence Intervals

CIS – Commonwealth of Independent States

CNP – Card not present

CR – Credit Risk

DIG – digitalization

DoS – Denial of Service

DR – Debt Ratio

DW – Durbin-Watson test

EAEU – Eurasian Economic Union

EBF – European Banking Federation

EO – Percentage of electronic orders in transfers in total

EP – Electronic payments for goods and services in thousands rubles

EY – Ernst&Young

Fintech – Financial technology

GCI – Global Cyber security Index

GDP – Gross Domestic Product

ICT – Information and Communications Technology

IDC – International Data Corporation

IDI – ICT Development Index

IEC – International Electrotechnical Commission

IMF – the International Monetary Fund

ISO – International Organization for Standardization

IT – InformationTechnology

ITU – International Telecommunication Unit

KRBR – the key rate of the Central Bank of Russia

MLR – Multiple Linear Regression

MR – average mobile banking rank

NDCO – Non-bank depositary organizations

OE – Operational Efficiency

OECD – the Organization for Economic Cooperation and Development

OWASP – Open Web Application Security Project

PCI DSS – Payment Card Industry Data Security Standard

PNCO – Payment non-bank credit institutions

POS – Point of Sale terminal

RNCO – Settlement non-bank credit institutions

ROA – Return on assets

ROE – Return on equity

SMS – Short Message Service

SQL – Structured query language

TA – Total assets

TER – amount of terminals

U. K. – the United Kingdom

U. S. – the United States of America

UNCTAD – the United Nations Conference on Trade and Development

XSS – Cross-site scripting

Intro

In 2010 World Bank stated that the level of competitiveness in Russian banking sector is relatively low compared to other economies such as Brazilian, for example, and the number of banks is extremely big (World Bank 2010, p. 18). The development of banking sector has led Russia to the emergence of innovative banking technologies. Many things have changed since that time: the number of banks has greatly decreased, and the remaining banks have a trend towards the reduction of physical offices and the transition to the online space (Central Bank of Russia 2020b). Despite the economic and financial instability, limited access of country's banks to external funding sources, high volatility of exchange rates and tight monetary policy of the Central Bank of Russia, the banking sector indicates a dynamic growth in banking competition (Central Bank of Russia 2017, p. 1). This makes it necessary for banks to maintain a profitable level of competitiveness. Such a level is achieved through the introduction of innovative banking products and technologies that require attention of the banking business to the security. The digitalization of the banking sector is gaining momentum. In 10-15 years from now banks may change beyond recognition.

Banks and financial sector in general have enough financial recourses, motivation and people who are able to implement the most modern technologies into their services. But does this give any return in terms of profitability? 'Banking digitalization' is the digitalization of various processes in banks in order to make them simpler, cheaper, more convenient and available to the greater amount of people (Boston Consulting Group 2020). In Russia and in the world in general there are articles which are dedicated to this topic. However, many of them touch only one side of the digitalization of financial sector. They either discuss the development, profitability, and benefits of digitalization (Dolgushina 2016, Kosheev, Tsvetkov 2018, Didenko 2016), or concentrate on cyber risks and security (Bouveret 2018). Our **motivation** was to look at this process from both sides at the same time on the example of Russian banking sector. Hence the object of our research is Russian banking sector, and the **subjects** are the positive and negative sides of its digitalization and their impact.

It is very important that in Russia the most of banking transactions nowadays are carried out in electronic form. Because of this, the risk of some kind of failure in customer service decreases significantly. Indeed, it is often the human factor that leads to some mistakes, shortcomings, and, accordingly, to problems. Presumably this leads to an increase in income. On the other hand, after the transition to digital space, cyber

risks increase significantly. Data transmitted through channels can be stolen, misused, and altered. Considering the scale of data that banks exchange every day, and how fast this amount of data grows, we can see how fragile the balance is. Banking sector traditionally was one of the most conservative, and it was not in vain: the cost of a mistake here ranges from just a couple of minutes delay in a transaction to the loss of huge amounts of money. Both of them have an incredibly strong effect on the reputation of the bank itself. Therefore, every step towards digitalization must be thought out to the smallest detail and protected to the maximum. This fact is crucial for the economic understanding of the real implications of digitalization. As digitalization of the Russian banking sector started not long time ago but already has penetrated to almost all banking processes, the topic of its impact on banks' performance and analyses of its threats is extremely **relevant**.

In this thesis, we are going to answer three **research questions** and state three **hypotheses**. The first research question is: what effect does digitalization have on the performance of the Russian banking sector? Our first hypothesis states that digitalization changes the way banking services are provided, promotes the creation of new distribution channels, increases banking sector profitability in general. According to Deloitte (2020, p. 2), cyber risks are one of the main barriers for the development of the digital banking services. In our thesis we want to check if this also true for the Russian banking sector. The second research question is: what kind of effects do cyber crimes have on digitalization growth trend? The second hypothesis says that the cyber crimes do not have a significant effect on the digitalization growth trend. Since the protection of the entire banking sector from cyber threats is not subject of private banks, we decided to look at how the main regulator of the banking sector, the Central Bank of Russia, is dealing with this with the support of the government. The third research question is: what are the main methods and objectives of cyber attacks in the Russian banking sector and what are the regulator's measures of protection? The hypothesis related to it states that the main method of cyber attacks in the banking sector are social engineering and the uses of malware, the main objectives are the people. The most effective cyber security methods which the regulator uses to protect banks are: improving the detection of fraudulent transactions by developing the information exchange system. To assess the validity of our hypotheses, we will use such **research methods** as literature review, regression model building, statistics and annual reports analyzing.

In our research, we would like to look at the formation of the digitization process in the Russian banking sector and its impact on the profitability of the banking sector. Since digitalization is inextricably linked to increased cyber risks, we want to dedicate a separate chapter to them. With the help of up-to-date statistics, we want to show the scale of cyber threats to the banking sector, the types of common threats, as well as the ways to deal with them that are used in Russia.

We **proceed** as follows: In the second chapter, we will examine the existing literature on the topics of banking digitalization, focusing on its drivers, possible effects and metrics which will help us further in the regression model building. We will discuss the risks of this process and talk about indexes which measure the development of IT and Security in the world which will help us later to demonstrate the place of Russia in the digital world in the next chapters. In chapter three we will talk about the structure of the Russian banking system and provide the brief history of it, as well as the analysis of the statistics of the current state and trends. We will talk more precisely about the positive and negative sides of digitalization. In the fourth chapter we will build the regression model, explain the factors and data selection, check out the adequacy of the model and analyze the results. By providing a practical example, we aim to show the dependency between the banking performance and digitalization. In the fifth chapter, we will discuss the other side of digitalization: cyber security and cyber risks. First we will look at the actual situation of cyber attacks on the Russian banking sector, their volume, amount, methods, motives and aims. Next, we will analyze the cyber security situation in Russia. We will look at its infrastructure, regulation base and actual measures taken by the regulator against cyber crimes. The last chapter concludes and summarizes our findings.

During conducting our research, we face several **limitations**. First and the main one is the lack of data. The Central Bank of Russia reports do not contain any indicators related to digitalization or its costs, hence we have to create our own proxies for measuring the digitalization impact. Some of the indices that we use are measured annually, hence they do not carry much information about the development and limit the data. It also decreases the accuracy of the regression results. Another limitation is the difference in concepts in statistical sources. The theoretical doctrines of Russian and European sources differ, and this makes it difficult to compare their indicators and draw conclusions. Since the theory and classification of cyber security is more developed in European sources, and we need data from Russian sources, it will be difficult to compare theory and practice.

Chapter 2. The digitalization process of the financial sectors in the world (Samsonova, Voronina)

In the modern world, it is hard to imagine life without digital technologies (the Internet, gadgets (electronic devices) and related services), and the faster they develop, the faster the surrounding reality changes.

In an era of rapid changes, a business cannot operate according to the old models - it must change, otherwise there is a great risk of being left behind competitors, or even stagnating altogether. Therefore, sooner or later, companies have to accept new rules of the game and experience the digitalization process. Banks are under serious pressure - the technological development brings to the market many new players capable of performing the functions of banks, hence digitalization turns into an endless race to be ahead. Banks and international organizations understand this, this is the reason why the topic of technologies is touched upon in almost all reports and public speeches.

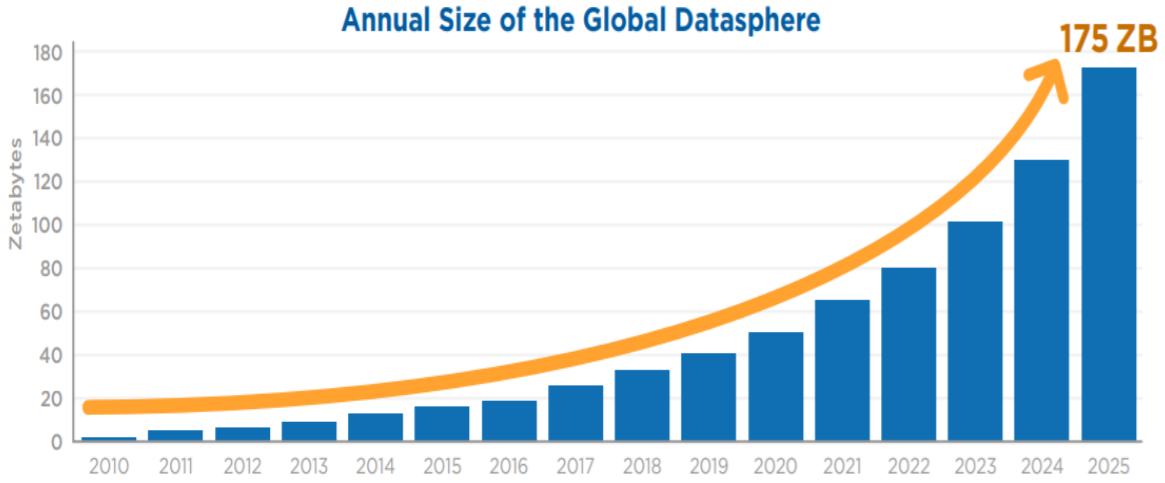
In this chapter, we would like to focus on reviewing the most interesting points of view on the topic of digitalization. We will discuss the digitalization process of economies in general, giving an overview of the main forces which promote it, then we will analyze benefits and after that we will proceed to risks of this process focusing on cyber risk as one of the most dangerous. In the end of the chapter we will discuss metrics which can help us to build models.

We would like to start with the base for digitalization – the amount of data. IDC's Global DataSphere is *'the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, it measures the amount of data created and consumed in the world each year'* (IDC 2020, p. 2). According to one of the last researches of them, '*More than 59 zettabytes (ZB = 10^{21} byte) of data will be created, captured, copied, and consumed in the world this year (2020). The COVID-19 pandemic is contributing to this figure by causing an abrupt increase in the number of work from home employees and changing the mix of data being created to a richer set of data that includes video communication and a tangible increase in the consumption of downloaded and streamed video' (*IDC 2020, p. 3). Considering the fact, that in 2018 the total summation of all data in the world, whether it is created, captured, or replicated, was only 33 Zettabytes (ZB), we can follow the dynamics of data creation, which is displayed on the

graph (Figure 1). As we can see, the amount of data grows every year, which gives more opportunities for digitalization.

Figure 1:

Annual size of Global Datasphere, 2020



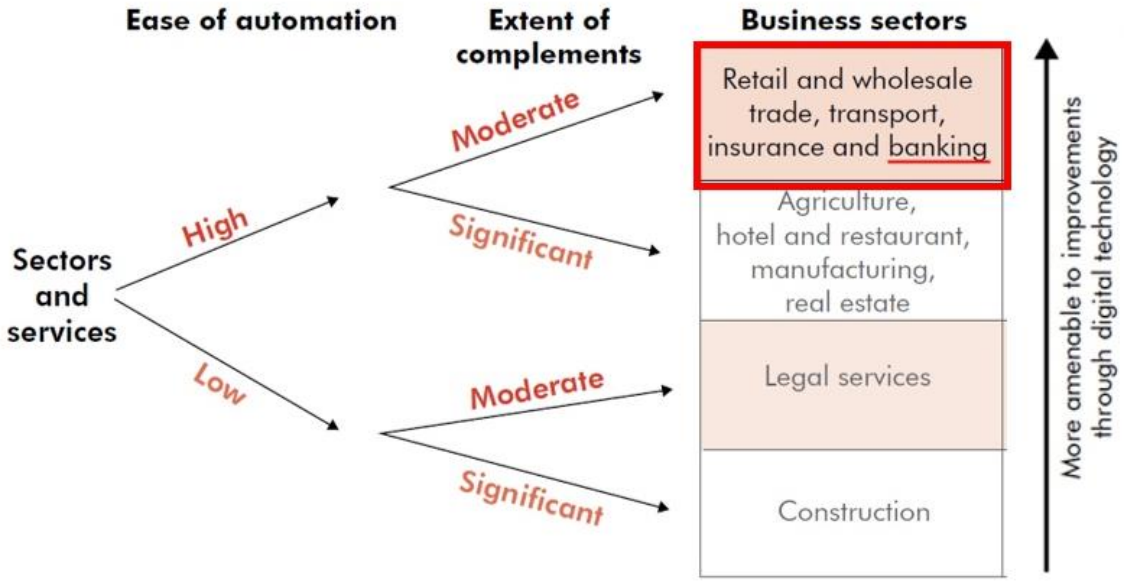
Source: IDC (2018).

'The amount of data created over the next three years will be more than the data created over the past 30 years, and the world will create more than three times the data over the next five years than it did in the previous five' (IDC 2020, p. 3). The idea of this sentence is that we are living in a very special period of time when technologies are growing especially rapid.

The active development of technology and the growth of data are leading to the digitalization of all spheres of public life. According to Gartner's IT Glossary (Gartner Glossary 2020) '*Digitization is the process of changing from analog to digital form*'. In the Figure 2 (World Bank 2016, p. 251) we can see, some sectors, occupations, and services are better amenable to technological transformation. If a sector mainly consists of routine processes, then such a sector is easier to automate. Vice versa, the more a profession requires skills such as judgment and intuition, the more difficult it will be to implement technology into it. As we can see, banking takes a high position here, as it is easy to automate and extend of complements is not that significant as in other sectors (for example, legal services). Moreover, banking sector accumulates a lot of assets, and the level of competitiveness is high. Banks and financial sector in general have enough financial and human recourse to implement the most modern technologies into their services. That is why we decided to choose the banking sector.

Figure 2:

Services and sectors which are more amenable to digital technology than others



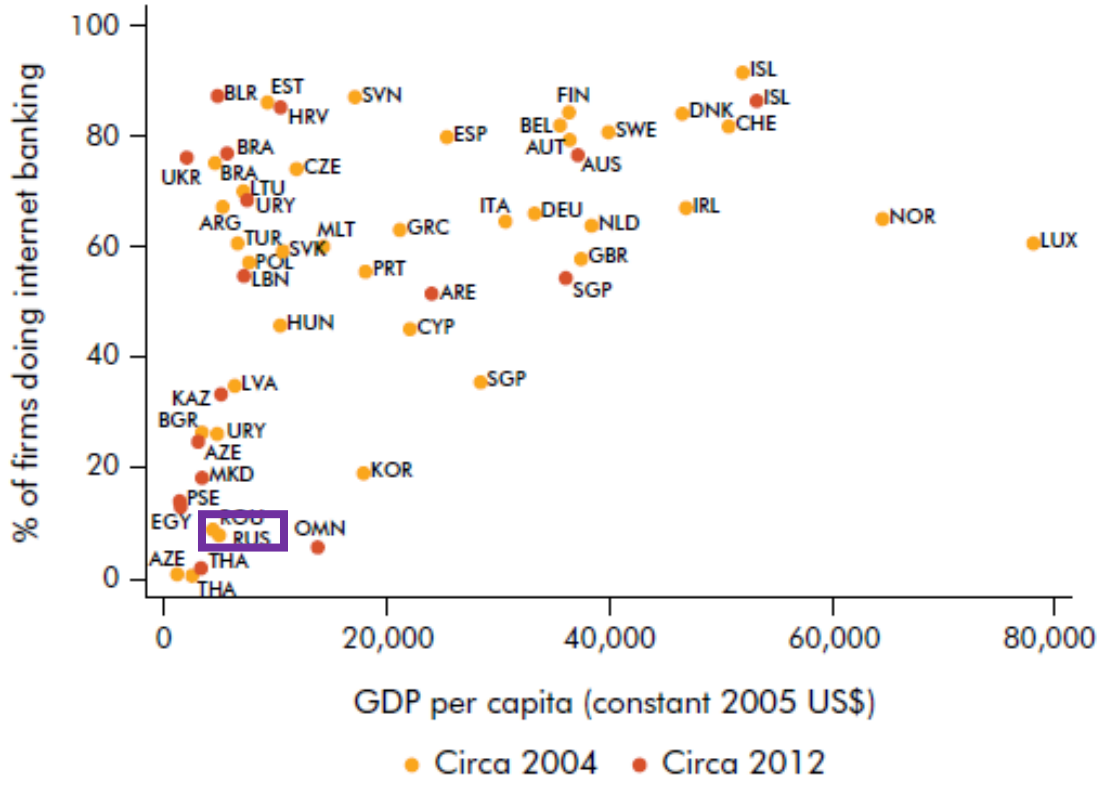
Source: World Bank (2016).

Digital economy is defined by World Bank as '*an economy which functions primarily by means of digital technology, especially electronic transactions made using the internet*' (World Bank 2017, p. 2).

The need for digitalized Banking varies a lot among sectors and countries. As we can see in Figure 3 (World Bank 2016, p. 71), countries are distributed on the graph by two indicators: GDP per capita and the percent of firms doing internet banking. '*The share of firms that used the internet for banking in 2012, for example, was below 20 percent in several middle-income countries, but more than 80 percent in others*' (World Bank 2016, p. 70). Russia has a position in the lower left corner in the Figure 3, meaning that it has relatively low percentage of firms doing internet banking (10%) compared to countries like Brazil Czech Republic or Estonia. For example, in Belarus, which has almost the same amount of GDP per capita, this indicator is almost 90%. At the same time Russia has relatively low GDP per capita compared to Scandinavian countries or Luxemburg. However, this picture shows the situation in 2004 and in 2008. In the following chapters, we will try to analyze the current situation by plotting the current percentage of firms using digital banking and GDP, and then we will show the dynamics.

Figure 3:

Firms' use of online banking varies across countries at comparable incomes, 2003-06 and 2008-13



Source: UNCTAD (2013).

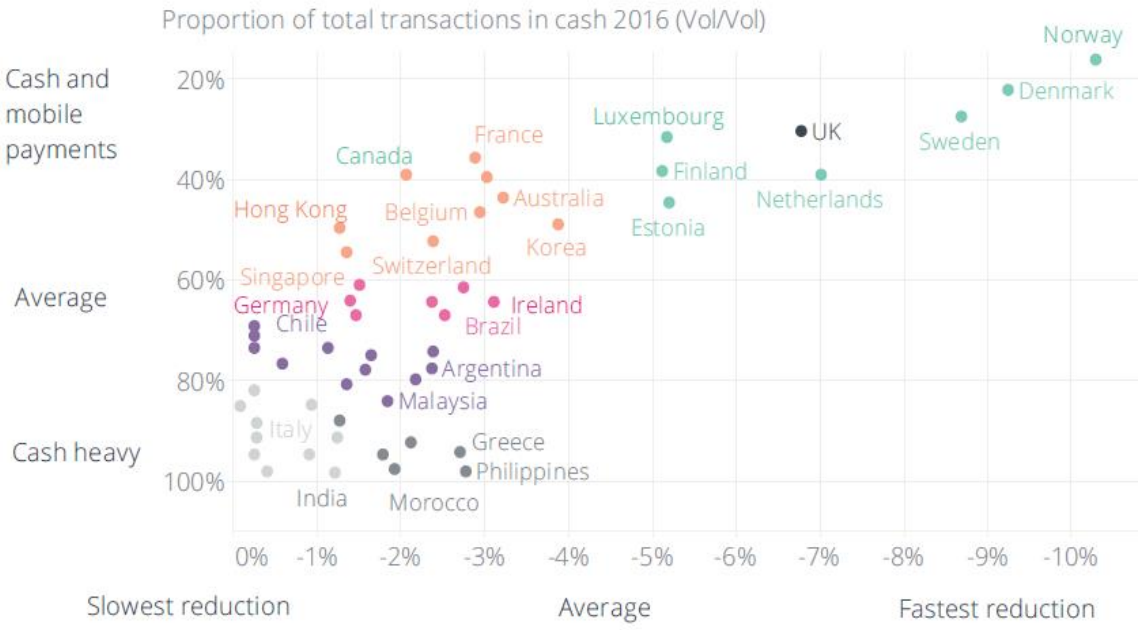
We have mentioned several times that the digitalization process is developing rapidly. What is the reason for such a rapid development? Talking about the drivers of digitalization, we should take a look at a review UK Financial system by **Bank of England (2019)**, where the forces influencing the modern economy are described.

The *first* force is that economy shifts to digital payments. It leads to change in business models. Banks are able to control all processes better, for example, to receive feedback from customers using a mobile application, to quickly realize the need or obsolescence of services with the help of that feedback, and to automate some processes if needed. For example, now the largest Russian banks, mobile operators and Internet holdings are actively building their ecosystems (Sber 2020). Among the banks that changed their business models, Tinkoff was one of the first. Having opened as the first bank without physical offices, it has become incredibly popular due to its convenient services. Then it launched Tinkoff Mobile, its own mobile operator, which could be profitable for the growing number of bank users. There are also opposite examples. MTS is a mobile operator which has opened its own bank, offering users deposits on

favorable terms. But the most striking example of a change in business model is Yandex, which started as a browser, but then created a service for delivery, money transfers, taxi, marketplace, ticket purchases and much more. Moreover, shift to digital payments contributes to the emergence of fintechs, start-ups and big technology companies. In today's world we can see the transition to electronic payments, which is shown in Figure 4. In the Scandinavian countries, which are in the upper right corner of the Figure, the transition is faster, and the share of non-cash transactions already exceeds cash, which has a share about 20% in all transactions. In European countries there is a trend that the volume of withdrawals from ATMs is permanently declining. On the graph it is shown that in the European countries the reduction of cash is average or above average. '*Based on current trends, this would imply a fall by a third over the next five years*' (Bank of England 2019, p. 27). Moreover, it should be noticed that shift to digital has a strong impact on cross-border payments, the amount and share of them increase.

Figure 4:

Countries shift from cash, amount of cash and transition speed, 2016



Source: Bank of England (2019).

The *second* force is '*enable innovation through modern financial infrastructure'* (Bank of England 2019, p. 11). The very possibility of creating alternative payments is pushing technological innovation forward. Since the financial sector is a complex area, a new product must meet security standards, be convenient, and be better than others. One more thing is a shift to clouds. *'Research suggests up to a quarter of the activities of largest global banks may already be on the public cloud or software hosted on the*

cloud. Looking forward, up to 40%–90% of banks' workloads globally could be hosted on public cloud or software as a service in a decade, according to McKinsey & Company' (Bank of England 2019, p. 11). The future is coming, and for being able to suit to the modern world's reality many banks are moving their data to the clouds.

The *third* force is data economy. '*Automated decision-making based on machine learning is one of the most important trends in technology today*' (Bank of England 2019, p. 11). Financial and banking operations are one of the most important processes in big data, and the ability to process them quickly and efficiently makes it possible to compete among banks and financial institutions. Why are banks that interested in algorithms for working with big data? There are three reasons: they work with different types of data at the same time, the speed of data processing is of great importance, and the amount of data generated daily is very large. Banks can use big data to combat fraud, assess customer solvency, manage personnel, calculate bonuses, identify the needs of potential and existing customers, and assess risks, plan marketing and sales. Some banks also analyze information and feedback about their work on social networks and user actions on the bank's website, analyze and predict queues at bank branches.

The *fourth* force is demographics. Each generation has its own needs, which are subsequently of great importance for changes in the financial system. People live longer, pension risks arise, hence the financial system and banks are forced to adapt to the new reality, expanding the range of investments.

The *fifth* is cyber risks. The banking system is an attractive target for cyber criminals. The Bank of England (2019) suggests banks to enhance data recovery, conduct cyber exercises, and provide data to build the cyber insurance market. To enhance data recovery, it would be useful to map the mechanisms for data recovery and in case of serious incident a firm should 'step-in'. Cyber exercises will enable cyber security services to better understand system weaknesses and work to improve them. Banks could work together to help developing the foundation for an effective cyber insurance market. Insurance will help banks cope with the growing risks of the digital economy by making up for the damage from cyber incidents.

The *last* force is embracing digital regulation. '*The Bank will want to embrace regtech and data science techniques to improve its productivity and effectiveness*' (Bank of England 2019, p. 15). Machine learning and datasets can help banks identify violations and calculate risks faster. Routine work is automated, which improves the entire process. '*Supervisors spend more time on relatively manual gathering and manipulation of information than they do on value-adding activities like analysis,*

interpretation and recommendations' (Bank of England 2019, p. 15). Therefore, automation will free up resources that can focus on analytical and research work. The provision of data and their processing can be fully automated, which will save huge amounts of money. Therefore, we can say that the banking system is very interested in automating the data processing and control process. '*Machine-readable rules could ensure better adherence and save the private sector a significant amount*' (Bank of England 2019, p. 15).

Realizing that the digitalization process has a very large impact on the present and the future, people want to translate it into measurable values to track and control the development process. Next, we would like to refer to indices and metrics.

Knowing the importance of digitalization, companies and countries also want to use new technologies. However, according to **Gottlieb and Willmott**, '*organizations involved in digitalization face multiple issues related mainly to the prioritization of investments and understanding the true value of digital'* (Gottlieb and Willmott 2014, p.4). These problems are quite relevant for the banking sector. It is relatively easy to calculate the benefits of automating the bank account creation process. At the same time, the benefits of automating the issuance of a loan or, for example, renovating an official website are not that obvious.

Both these issues lead to one problem – the problem of measuring digitalization and its impact on banks' profit. *'What you measure is what you get'* (Kaplan and Norton 1992, p.71). Many different organizations were and are trying to find appropriate metrics for digitalization process to show how it can affect the performance of banks.

An interesting research was conducted by **Marcin Kotarba** from the Warsaw University of Technology (Kotarba 2017). After analyzing many indexes and methods for measuring the digitalization process, he offers several indicators, which are specific for the banking sector. First of all, he talks about the banks' usage of online solutions. This includes: logins per day/month, number/volume of transactions per session, most frequently used functionalities, hardware and software analyzing and others (Kotarba 2017, p. 123). The author also offers to look at such indicators as: *'product sales, revenues, and profitability of digital clients, self-service ratio via digital solutions in sales, business activity generated via the mobile and app-world performance'* (downloads of applications, rankings/stars and feedback, application updates) (Kotarba 2017, p. 123).

However, to search for relationship between digitalization and banks profit, it is essential to understand what other factors define it.

In the study of the financial performance of Jordanian commercial banks A. **Ahmad** (Ahmad 2011, p. 10) used ROA (Return on assets) as a measure of banks' performance and the bank size, assets management and operational efficiency as independent variables which affecting ROA. He has found a negative correlation rate between ROA, bank size and operational efficiency, and positive correlation between ROA and assets management.

Khizer (2011) in the research 'Bank-Specific and Macroeconomic Indicators of Profitability - Empirical Evidence from the Commercial Banks of Pakistan', has found that profitability depends on operating efficiency, assets management ratios, and size, and this dependency is positive, while using ROA as an indicator of profitability. When we change ROA for ROE (Return on equity) the dependence changes. '*ROE is positively related with assets management and negative association is find with size and operating efficiency*' (Khizer 2011, p. 12).

Nataraja, Nagaraja and Ganesh (2018) measured the performance of banks in India using ROA and ROE as dependent variables and Bank size (BS), Credit Risk (CR), Operational efficiency (OE), Asset management (AM) and Debt Ratio (DR) and Log(Total assets(TA)) as independent variables.

- Bank size = Log(Total Assets)
- Credit Risk = Reserves for doubtful loans / Credit facilities
- Operational efficiency = Total operating expense / Net interest income
- Asset management (AM) = Operating income / Total assets
- Debt Ratio = Total debt / Total assets

They found out that there is a positive correlation between ROA and AM, as well as with Bank size. There is negative correlation between ROA and CR, OE and DR. '*Operational efficiency and asset management are positively correlated whereas credit risk and bank size are negatively correlated with ROE*' (Nataraja, Nagaraja, Ganesh 2018, p. 7). The conclusion of the research is that size of the bank, credit risk, operational efficiency asset management and debt ratio have an impact on bank income and performance in India.

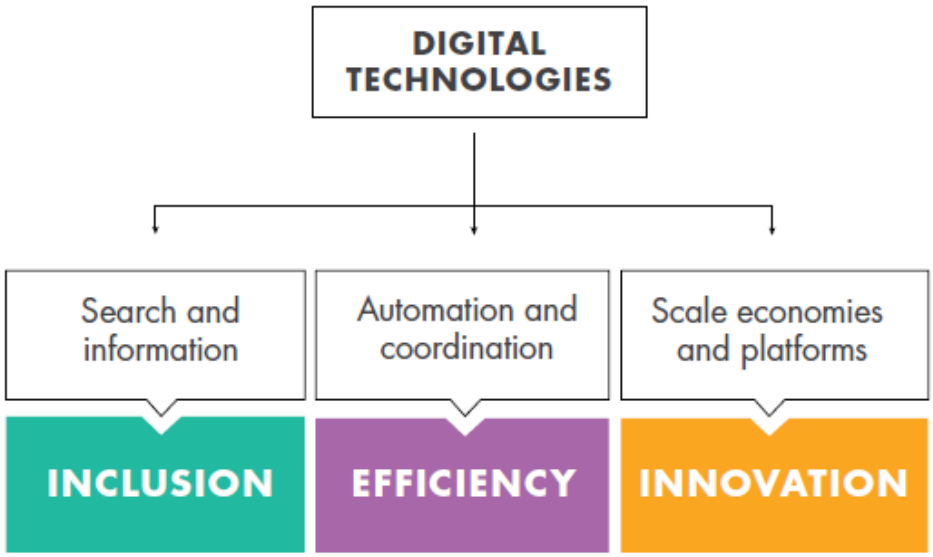
As we can see, there are tens of metrics already built to measure the profitability of banking sector, but at the same time, not so many indicators describing banks' digitalization.

The process of the banking sector digitalization has its pros and cons, which we would like to talk about.

According to World Bank (2016), benefits of digital finance can be described in three main trends which are shown in the Figure 5. We want to discuss each of them more detailed.

Figure 5:

The internet promotes development through three main mechanisms



Source: World Bank (2016).

The first trend is that digitalization promotes financial inclusion, especially for developing countries. For example, not all people in the world can get a bank account by going to the bank physically, but thanks to online banking now they only need a mobile phone to become participants of the banking system.

Moreover, digitalization promotes cost reduction, which also makes financial services available to wider audience and allows getting more control over spending, as people can see advanced statistics of their transactions. On another hand, digital finance lowers the information asymmetry (it is a situation when one party to transaction has more information than another). That is especially important in credit markets. Due to new technologies the lender can estimate the ability to repay the loan by a potential borrower, using digital footprints.

The second positive trend is that digital finance increase efficiency. Using new monitoring and statistics software, managers can supervise their workers and analyze the results of work more effectively. It also leads to lower costs and better division of labor. Another benefit of this trend is reducing frauds. '*Electronic payments create a clear digital record and can be traced, so the likelihood of funds not reaching the beneficiary or of duplicate payments or payments to "ghost" recipients who do not exist will be lower*' (World Bank 2016, p. 96). However, this benefit can also be considered

as a risk, as digital finance growth also promotes the growth of cyber crimes, which we will discuss further.

The third main trend is that digital finance spurs innovation. Financial sector was always interested in new technologies and automatization, as it is very transaction-intensive. The extreme case of efficiency is when transactions are made automatically, without human intervention, this leads to the fact that the costs fall to zero. This is the realm of the 'new economy', such as search or e-commerce platforms, digital payment systems, e-books, streaming music, and social media. The initial cost of creating a platform is quite high, but the additional costs of performing another transaction or adding another user are minimal. This translates into increased returns to scale and therefore fosters new business models and benefits online organizations.

As a result, new fintech companies, which were able to adopt innovations easier, offered services for lower price. This triggered a technology competition not only between traditional banks and fintech companies, but among banks themselves. However, this is only possible with adequate regulation. In some countries government closes the market to protect domestic banks from foreign competitors. In this case banks are no more interested that much in investing in digitalization as there is no danger of losing clients.

The digitalization process is multi-faceted and brings new opportunities to our lives. However, with new opportunities always come new risks. Below, we would like to talk about the difficulties faced by the companies during the transition to a new stage of technological development.

Aside from the emergence of new services and the transition to a new lifestyle and vision of business, the explosive growth of data leads to digital threats. The larger the amount of data that is contained on the servers and in the clouds, the more likely it is that someone might try to hack, steal, change or destroy it. Antoine Bouveret in the IMF Working paper 'Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment' (2018) taking GCI index as a base, develops the topic of cyber attacks further. He begins with confirming two ideas by two graphs: 1) that cyber risks are the most dangerous among all risks to broader economy (Figure 6) and 2) that financial sector suffers the most from cyber attacks (Figure 7).

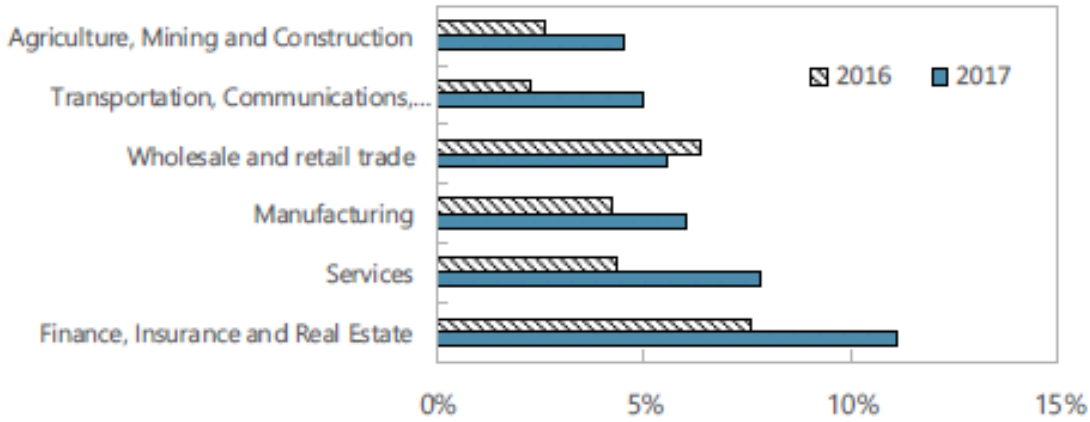
Figure 6:

Risks to financial stability in the U.S., 2016-2017

Source: Bouveret (2018).

Figure 7:

Reporting of cyber risk in the U.S., 2016-2017



Source: Bouveret (2018).

'*Cyber risk shares characteristics with both property and liability risk, as well as catastrophic and operational risk*' (Eling, Wirfs 2016, p. 6), and it distinguishes it from other risks covered by insurance, it is more complex. Cyber risks can affect both the target of attacks and the counterparty of the target of attacks.

'*Cyber attacks can impact firms through the three main aspects of information security: confidentiality, integrity and availability'* (Bouveret 2018, p. 5). The first issue arises when the confidential data is disclosed to third parties. Integrity issue is connected with misusing of the systems, such as fraud. Availability issues relate to business disruptions. *'Cyber attacks have different direct impacts on targets'* (Bouveret 2018, p. 5). Data breaches need a lot of time to eliminate the consequences, because of

two things: 1) it has a large impact on reputation and 2) sometimes it leads to litigation. Fraud is a direct monetary loss. Business disruptions interfere with the work of banks, which leads to losses. However, the most important and difficult-to-recover consequence is the loss of banks' reputation due to cyber attacks.

Knowing the importance of digitalization risks for the world and for the banking sector in particular, IMF Deputy Managing Director **Tao Zhang** focuses on these risks in his speech about the challenges and opportunities of digitalizing money and finance.

In the beginning of the speech Tao Zhang (2018) stresses that macroeconomic implications of digitalization may change the way low-income countries develop. The latest IMF World Economic Outlook contains a study that new technologies will reduce the need for labor-intensive industries, and labor recourses will be able to move to the service sector, which is extremely important information for developing countries.

The *first part* of the speech is devoted to implications for finance. Artificial intelligence, big data, biometrics, and distributed ledger technologies such as blockchains will definitely affect finance in terms of fintech. According to Zhang's definition, '*fintech is the collection of technologies whose applications may affect financial services*' (2018, p.1). Fintech makes financial services faster, cheaper, more convenient and user-friendlier. Hence, it helps finance grow faster, especially in developing countries, which is relevant for our research, because we are focusing on Russia which is now considered an emerging market. However, Tao Zhang says that this shift towards the digital economy brings us risk, which is inevitable. '*Financial stability could be affected—through disruptions to existing service providers and business models. Unregulated sectors could create additional operational risks related to cyber crime and outsourcing*' (Zhang 2018, p.2). Agreeing with the author on the danger of cyber crime, in our research we will focus on cyber security risks and show their impact on the Russian financial sector. *'New technologies may upset the balance between transparency and privacy*', says Zhang (2018, p.2). In the following chapters, we will try to highlight what actions banks are taking to overcome this problem.

In the *following part* of the speech he talks about the possible regulatory responses in the digital era. The most important step is to find a balance between free development and regulatory restrictions. He stresses two main points: 1) governance needs to be strengthened and 2) new policies should support open networks and simplify the licensing to foster competition. Zhang says, that '*Fintech is difficult to regulate because it cuts across the responsibilities of different national agencies, and operate on a global scale*' (Zhang 2018, p.3). Nevertheless, regulation and protection

are necessary. As a brief conclusion the author uses an idea that the most important thing nowadays is to strengthen protection in the world of technology, but not negatively influence competition by measures of protection. In our research we will show the process of developing legal bases for regulation of technologies in Russia.

Next, we would like to talk about the concentration risk, a situation where the overwhelming share of banking assets is concentrated in the hands of several large players. This risk is related both to the specifics of the banking sector, which we will discuss in Chapter 3, and to cyber threats. High concentration leads to the fact that large banks are the desired target for attacks.

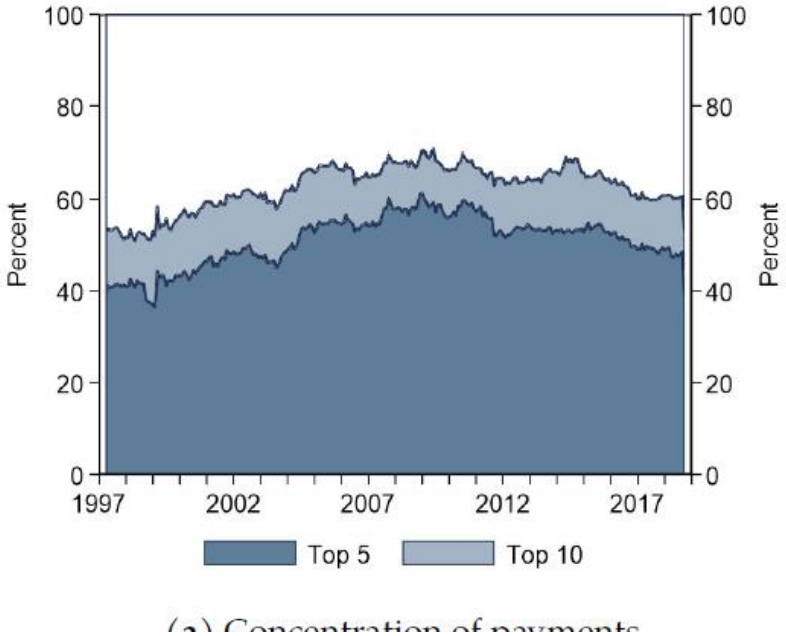
Talking more detailed about the risks of digitalization, we would like to review the report 'Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis' **by Federal Reserve Bank of New York**. '*The U.S. payments network has a core-periphery structure*' (Soramäki, Bech, Arnold, Glass, Beyeler 2007, p. 6). '*Consistent with this, payments are highly concentrated among a small set of institutions. The top five most active banks in the payment system account for close to 50 percent of total payments and the top ten for over 60 percent* (Figure 6a). *Activity is concentrated not only in terms of payments value but also in terms of network connections, with the most active banks' connections outnumbering the average banks' by several orders of magnitude* (Figure 6b)' (Federal Reserve Bank of New York 2020, p. 10). The bank associates a high cyber threat with the fact that the concentration of assets in the top U.S. banks is very high. This case is interesting for our research because as we will show in the following chapters, concentration of assets in top Russian banks is even higher compared to total assets.

Figure 8:

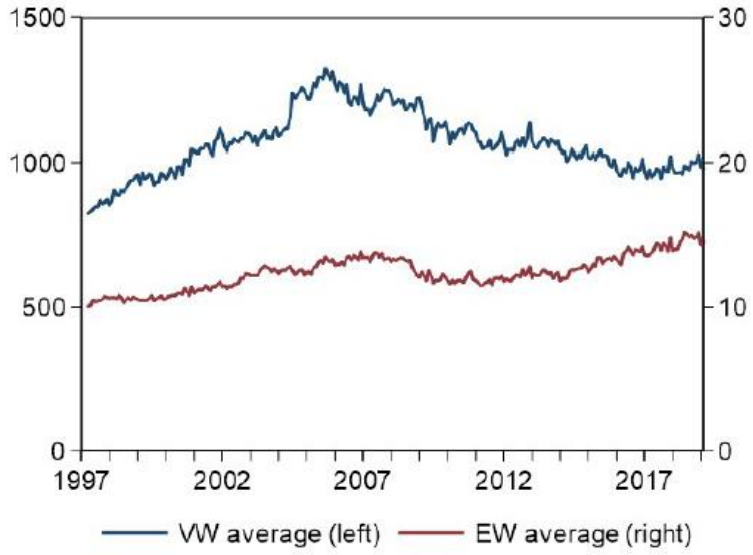
Concentration and network dependencies in the U.S. banking sector (1997-2019)

8a panel demonstrates the share of payments sent by top-5 and top-10 banks.

8b panel shows value-weighted and equal-weighted averages across participants.



(a) Concentration of payments



(b) Network dependencies

Source: Federal Reserve Bank of New York (2020).

As we can see the risks of cyber attacks are crucial for financial institutions, as they are dependent on highly interconnected networks. Consequently, in the case of a high concentration of the banking sector, as in the U.S. or Russia, when one large bank suffers from attacks, the losses of the banking sector are much greater than in the case of a low concentration. Moreover, the appeal of the major banks to cyber criminals is much higher as well.

We have mentioned the term ‘cyber attacks’ many times but what kind of attacks are meant? Now we would like to discuss the most popular and effective methods of cyber attacks in financial sector.

There are huge numbers of classifications of cyber attacks’ types, but they are all very specific. In the context of our work, we would like to divide cyber attacks in two groups and name the most important of each group.

All banking sector cyber attacks can be divided into two types:

- attacks based on the vulnerability of machines, equipment and software;
- attacks based on the vulnerability of the human factor.

The **first type** includes:

1) Denial of Service (DoS) ‘*is the act of performing an attack which prevents the system from providing services to legitimate users’* (Chen 2007). In case of success the next step can be the acquisition of control over the system (if in an abnormal situation the software gives out any critical information - for example, a version, a part of the program code, etc.). But more often its final aim is the economic pressure. In case of banks, a simple temporary loss of paying service will lead to loss of customers, reputation damage and losses from equipment downtime.

2) SQL injection is one of the most widespread methods of hacking banking websites and programs working with databases, based on injecting arbitrary SQL code into a query. *‘An SQL injection attack consists of insertion or “injection” of a SQL query via the input data from the client to the application’* (OWASP 2020). The purpose of this attack is to extract or modify sensitive data from a database, for example, personal information about bank customers, for their subsequent sale on the black market or direct use for financial gain.

3) Attacks using Malware. Malware is a malicious program or code that can cause damage to a computer system. *‘Malware breaches a network through vulnerability, usually, when a user clicks on a dangerous link or email attachment that then installs risky software’* (Cisco 2020). Once inside the system, malware can do the following:

- *‘Blocks access to key components of the network (ransomware);*
- *Installs malware or additional harmful software;*
- *Covertly obtains information by transmitting data from the hard drive (spyware);*
- *Disrupts certain components and renders the system inoperable’* (Cisco 2020).

It seeks to penetrate the system, inflict damage, partially take over control of some processes, or completely disable computers, computer systems, networks, tablet and

mobile devices. In case of banks it can lead to industrial espionage and sensitive data stealing.

4) Brute forcing - one of the popular methods for cracking passwords on servers and in various programs. The main goal of this attack is to gain access to a closed resource, for example, a personal account on the bank's website. The cracker tries to gain access by brute-forcing passwords according to the criteria set by the hacker: by the dictionary of the most popular passwords, by length, by combinations of numbers, and others. One of the protection methods of this attack can be imposing specific requirements to passwords: length, special symbols, upper and lower case letters etc.

5) Cross-site scripting (XSS) attack - is *'a type of attack on web systems that injects malicious code into a page issued by a web system (which will be executed on the user's computer when the user opens this page). An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script'*. (OWASP 2020) If such script will be injected into bank's website, it can steal the credentials nor only of users, but also of the employees of the bank and system administrators.

The intensity and the scale of damage of machine-based attacks make companies and software vendors more concerned about the security of their applications and networks.

However, it is also important, that the understanding of cyber risks have changed. If before most of online consumers were sure that the level of IT security totally depends on how the companies protect their networks, now we all know that is also defined by our behavior.

The **second group** of cyber attacks is based on a human factor vulnerability and called social engineering.

According to J. A. Ross, *'in the context of information security, social engineering is the psychological manipulation of people into performing actions or divulging confidential information'* (2020).

Social engineering includes three main vectors:

1) Phishing is an Internet fraud attack. Its purpose is to gain access to confidential user data - logins and passwords. *'This is achieved by sending bulk emails on behalf of popular brands, as well as private messages within various services'* (Tadviser 2020). For example, it can be done on behalf of banks or within social networks. *'The letter often contains a direct link to a website that looks indistinguishable from the real one, or to a site with a redirect'* (Tadviser 2020). After that the scammers try to induce the

users to enter their username and password on the fake page, which allows the fraudsters to gain access to bank accounts and other personal data.

2) Vishing (or telephone phishing) is other method of fraud using social engineering. Attackers use telephone communication and play a certain role (bank employee, customer, etc.). Under various pretexts they deceive confidential information from the payment card holder or encourage certain actions with his or her card account / payment card. For example, the victim receives a request (most often through a phishing email) to contact the bank and confirm or update some information. Further, the pre-recorded voice imitates the work of an answering machine and asks the user to name a code word or enter a password or pin code. As a result, the hacker obtains the victim's personal data.

3) One more type of social engineering is called smishing. This attack has the same scheme as phishing and vishing with the only difference that it is carried out via SMS. The victim receives SMS from a bank or any other organization that looks reliable. For example, a message with a reminding to pay a penalty for late payments on a loan. The SMS will contain a link to the site through which you can make a payment. When the user enters his card details, funds are debited and transferred to the hacker's account. Funds can also be debited for the provision of services via SMS. The message can also include an MMS file: picture or audio. After downloading the file, the victim receives a virus on his smartphone. When the smartphone is restarted, the virus reads the victim's mobile bank login and password and suppresses SMS notifications from it. As a result, the victim will not receive a message about debiting money from his or her card.

Understanding the types of attacks and their main threats and targets will help us better understand the impact and scale of cyber attacks in the Russian banking sector. In our thesis we would like to focus more on social engineering and on phishing in particular, as this group is responsible for the biggest part of cyber crimes in Russian banking sector.

As a result of understanding the cyber risks, in recent years online users have changed their behavior to be more secure in many ways. For example, the attitude to personal data sharing has changed a lot. We are less likely to share our personal information on websites or send it to people in the internet we do not know well. No doubt, it is a positive trend in terms of safety. However, it also brings us a problem of collecting data for measuring risks and the current state of IT security.

As it is mentioned in OECD report 'Measuring the digital economy: a new perspective' (2014), statistical *'data on online security and privacy are typically drawn from three major sources: user surveys, activity reports and the Internet'* (OECD 2014, p. 65). Surveys can be helpful in getting actual information for very specific questions. However, the respondents can give false answers because of lack of knowledge, or just because they want so. The biggest advantage of activity repots is their periodicity. It allows building large datasets and time series. However, difference in reporting standards over the world brings a lot of difficulties. The internet is a rich source of actual data which is replenished and updated every second, but it is also the reason of its chaotic nature. It is very hard to structure and manage terabytes of information, especially if it is collected from various sources.

'Besides the issues specific to each data source, there is a more fundamental challenge to the measurement of security and privacy, whether online or offline. Because of the illegal nature of privacy and security violations, not all incidents are identified or reported' (OECD 2014, p. 68).

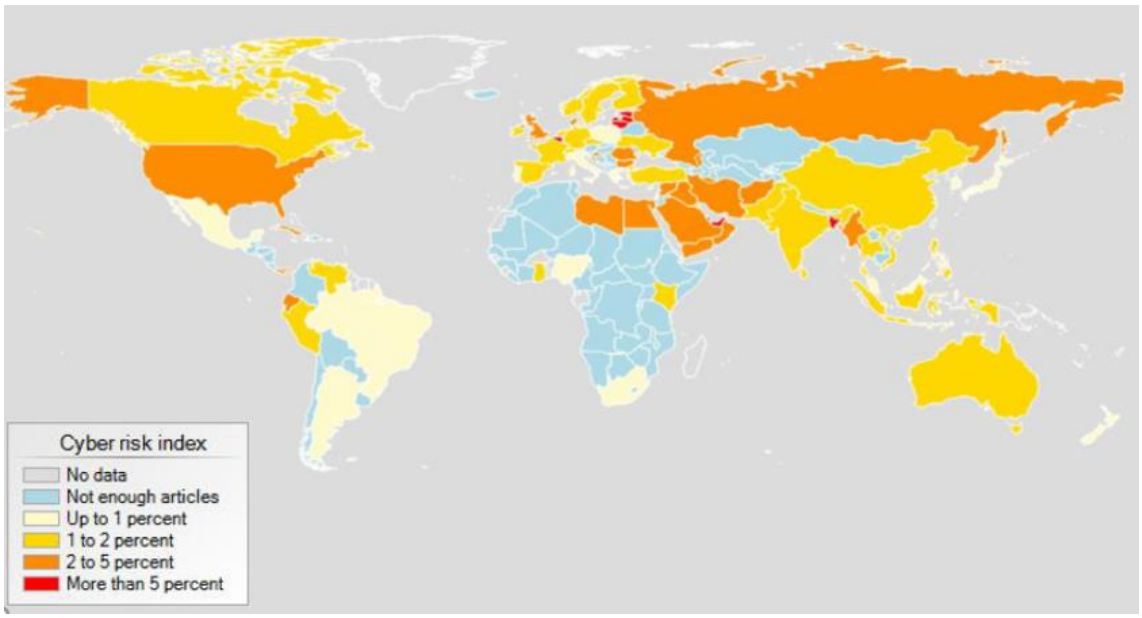
As we have found out, cyber risks increase with the course of digitalization, and they, in turn, are dangerous for bank income and reputation. Therefore, much attention is paid to the issue of measuring the level of cyber security.

With a very limited available data it is challenging to build datasets and, hence, metrics and indexes in area of cyber risks and cyber security; however, some organizations accept this challenge.

Antoine Bouveret, the scientist from IMF succeeded in building international cyber risk statistic for the banking sector. He built an index using the number of articles referring to the risk in financial sector by country and divided it on the number of publications referring to cyber risk (Figure 9). He took the number of articles and reports including words "cyber attack", "hack", "cyber risk", "cyber security", "banks" and "risk" and divided them by the number of articles with the words "banks" and "risk" by country. But this index has several disadvantages. For example, some countries can have poorly developed financial sector and the index for such countries will be higher. Moreover, it is sometimes hard to draw a line between pure financial publication and a publication about cyber risks in financial sector, as the second one is becoming more and more popular every year. Nowadays most of bank reports include a part about cyber security. The fact, that he used only publications in English also can be a factor of less accurate results.

Figure 9:

Measure of cyber risk for banks



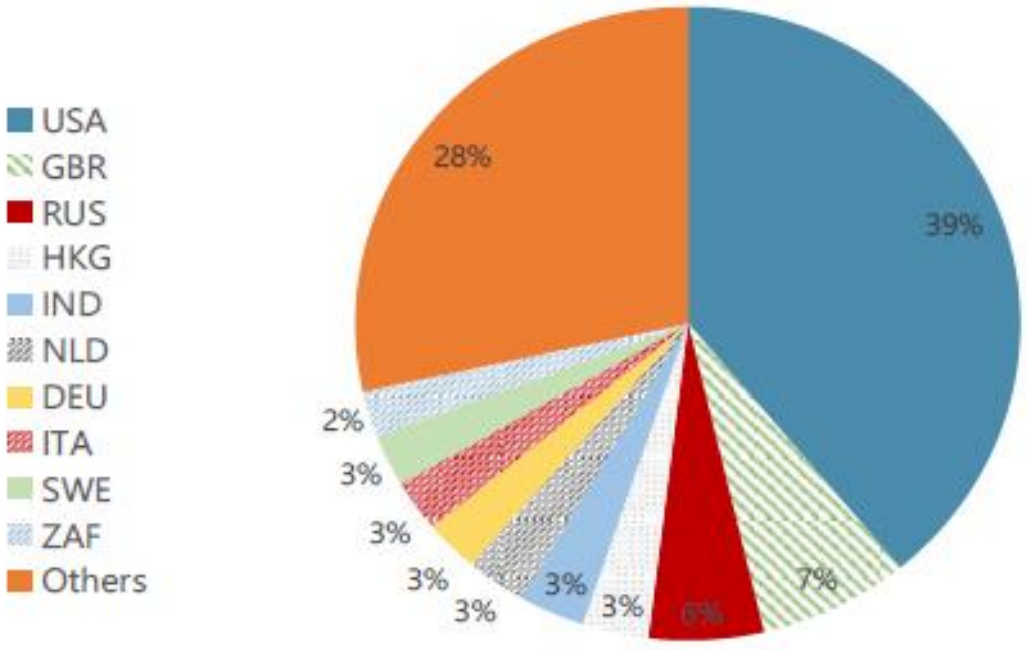
Source: Bouveret (2018).

In other words, this index cannot deliver the perfect picture of the cyber risk situation in financial sector. Nevertheless, it gives us a general idea of trends in banks' cyber security. As we can see on the map, the index is high in such countries as the U.S., Bangladesh, Baltic countries and others. These countries are known to suffer from cyber attacks. Russia is also in dangerous orange area. This shows us, that Russian financial sector is relatively vulnerable.

According to Bouveret, *'advanced economies are the main targets of cyber attacks but emerging markets and developing economies are also exposed to cyber risk (Figure 0), based on data from ORX News. Advanced economies account for 80 percent of successful attacks, mainly in the U.S. (39 percent) and U.K. (7 percent) as shown in Figure 10. Among emerging markets, the BRICS account for most of the attacks (17 percent), mainly in Russia (6 percent), China (4 percent) and India (3 percent). Overall, financial institutions in more than 50 countries have been victims of cyber attacks over the last few years according to reports in the public media'* (2018, p. 8).

Figure 10:

Cyber-attacks on Financial Institutions (% of total)



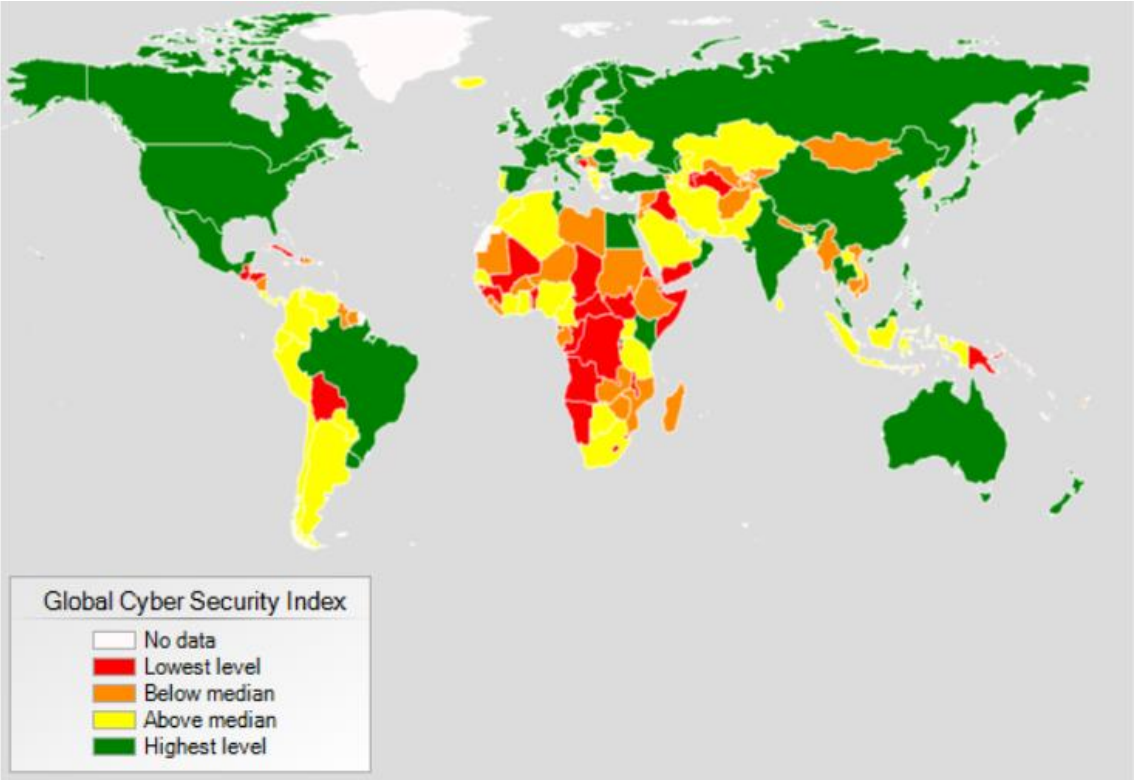
Source: Bouveret (2018).

In addition to cyber threat indexes, there are also indexes that aim to measure cyber security. Next, we will look at several indices compiled by the ITU.

The International Telecommunication Unit (ITU) – is an agency of the United Nations which provides a global cyber security index for the whole world. Their index is based on a range of different factors, including legal, technical etc. Figure 11 shows the cross-country heterogeneity regarding cyber security. As we can see, *'advanced economies and emerging markets have a higher value of the index, while middle income and low-income countries tend to have lower values'* (ITU 2018, p. 8). According to this map, Russia has the highest level of security. It means that despite the fact that the Russian banking sector, as with the banking sectors of other countries, is the target for many cyber attacks, as we discussed earlier, the level of cyber security in Russia is very high, therefore, adequate to the existing threat.

Figure 11:

Global Cyber security Index (GCI)



Source: Bouveret (2018).

'*The Global Cyber security Index (GCI) is a composite index combining 25 indicators into one benchmark to monitor and compare the level of the cyber security commitment of countries with regard to the five pillars of the Global Cyber security Agenda (GCA)*' (ITU 2018, p. 7). The aim of the index is to help countries identify areas for improvement by measuring the type, level and evolution of cyber security and to motivate them to improve their cyber security rating which will be helpful for the level of cyber security worldwide. The index focuses on *'five pillars: legal, technical, organizational, capacity building and cooperation'* (ITU 2018, p. 7), more detailed they are demonstrated on the Figure 12.

Figure 12:

Five pillars of Global Security Index

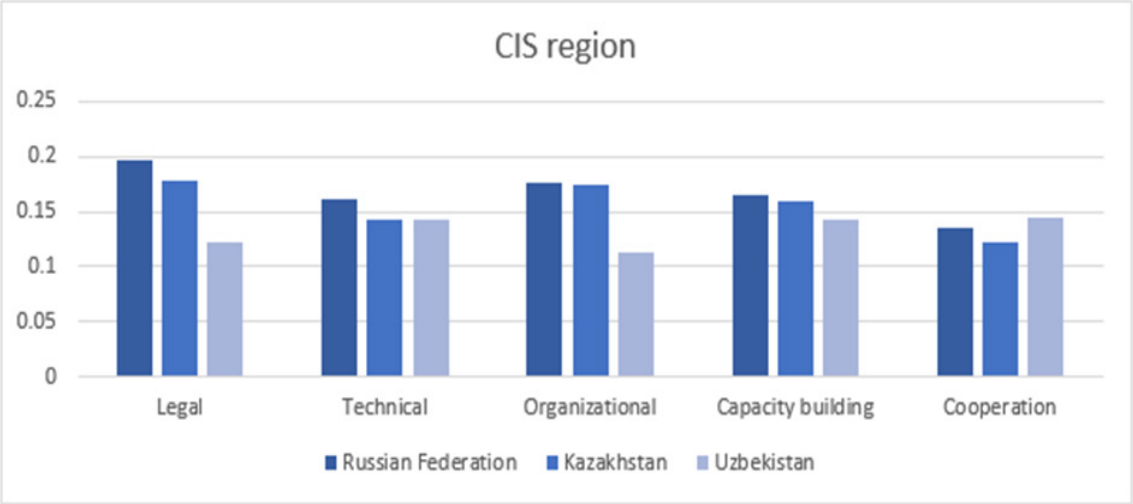
Source: ITU (2018).

The key findings of the index include two types of ranking for all countries in the world: global and regional. In a global rating Russia takes 26th place with an index score of 0.836 (ITU 2018, p. 29). And it scores 1st in a CIS (Commonwealth of Independent States) region, which includes: Russia, Kazakhstan and Uzbekistan (it is shown in the Figure 13). *'The Russian Federation scores the highest in almost all the*

pillars except in the cooperation pillar where Uzbekistan has the best score. Kazakhstan scores well, with a close second place in all pillars but cooperation' (ITU 2018, p. 29). Russia has strengthened the control, regulation and counteraction of fraud using electronic payment systems. The financial system has been improved in order to increase confidence when using online payment services. We will discuss it more detailed in following chapters.

Figure 13:

Top three scores in the CIS region according to the five pillars of GCI



Source: ITU (2018).

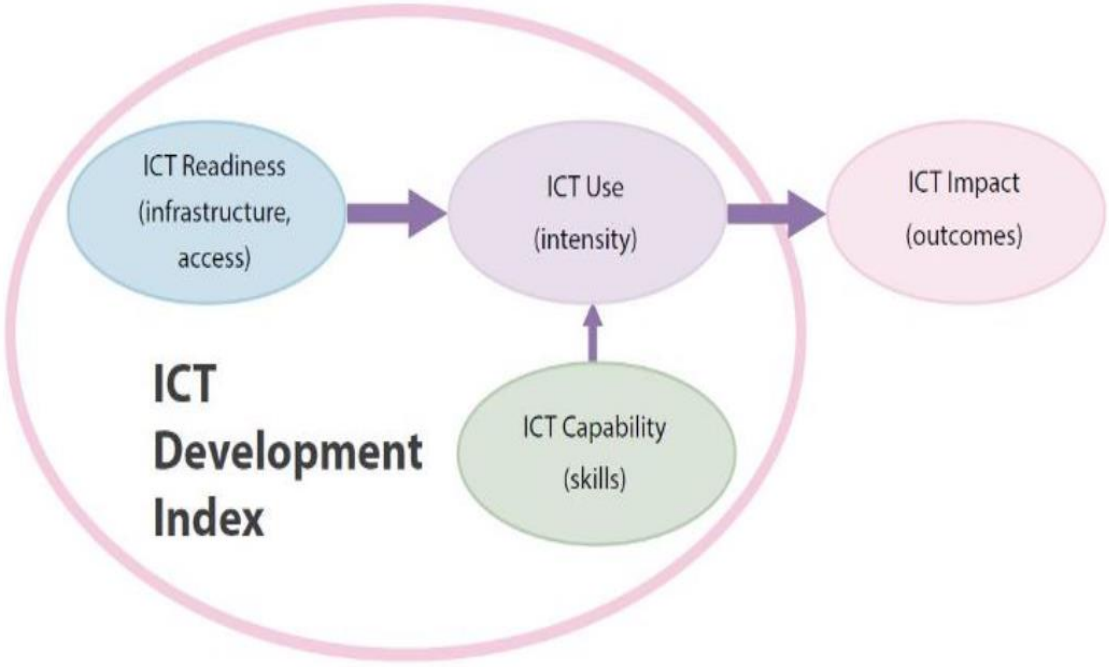
The other index, ICT Development Index (IDI), which was also created by ITU, is a composite index which has 11 indicators into one benchmark measure. It is used to measure:

- *'the level and evolution over time of ICT developments within countries and the experience of those countries relative to others;*
- *progress in ICT development in both developed and developing countries;*
- *the digital divide, i.e. differences between countries in terms of their levels of ICT development; and*
- *the development potential of ICTs and the extent to which countries can make use of them to enhance growth and development in the context of available capabilities and skills'* (ITU 2018, p. 24).

The index is also used for analyzing trends in the digital area. *'Recognizing that ICTs can be development enablers is central to the IDI's conceptual framework'* (ITU 2018, p. 25). The ICT development process in the country is described by the model shown in Figure 14.

Figure 14:

Three stages in the evolution towards an information society



Source: ITU (2018).

The first stage demonstrates the readiness of ICT at the infrastructural level. The second stage shows intensity – the level of use in the society. The third stage is the outcomes of efficient and effective use of ICT.

Table 1 demonstrates the 11 indicators which are included in the IDI. They are divided into 3 groups: ICT access, ICT use and ICT skills. The index will be used by us in the Chapter 4 for building a regression model.

Table 1: Indicators included in the IDI
ICT access
Fixed-telephone subscriptions per 100 inhabitants
Mobile-cellular telephone subscriptions per 100 inhabitants
International Internet bandwidth per Internet user
Percentage of households with a computer
Percentage of households with Internet access
ICT use
Percentage of individuals using the Internet
Fixed-broadband Internet subscriptions per 100 inhabitants
Active mobile-broadband subscriptions per 100 inhabitants

ICT skills
Mean years of schooling
Secondary gross enrolment ratio
Tertiary gross enrolment ratio

Source: ITU (2018).

The digitalization process is complex and controversial; it removes some of the society problems and simplifies life, but adds new vulnerabilities which should be overcome. At the same time, if it is measured and well-monitored, this process will certainly be of great benefit, especially in banking sector with its great resources and willingness to improve. All of the above theoretical material and metrics help us to analyze the current position of Russia in the digital world and the influence of various factors on its development. But before proceeding with the measurements, it is necessary to briefly characterize the banking system of Russia, since this has a large role in the subsequent interpretation of the results.

3. Banking sector in Russia: structure and the digitalization path (Samsonova, Voronina)

In this chapter we would like to give a brief overview of the banking sector in Russia, take a look at the participants, their shares and functions. Then we will move to the development history and current state of the remote banking services in Russia which can be considered as channels of banking digitalization. After that we will talk about the upcoming changes and evolution of Russian banking sector and the ways they can be implemented. And then we will analyze the barriers of banking digitalization.

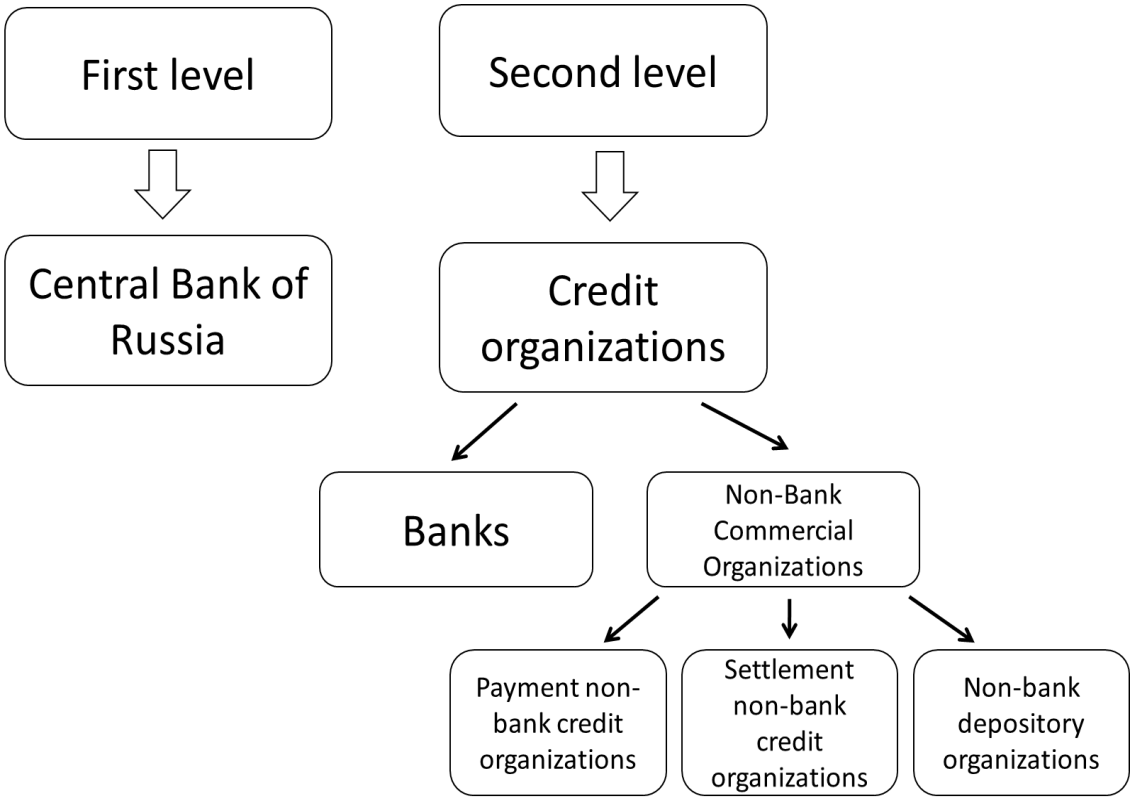
3.1. Intro into the structure of the Russian banking sector

The digitalization process of the economy is highly dependent on which country we are considering. Humanity is seeking to reduce the gap in the standard of living at the individual level and economic development at the state level. Nevertheless, the initial condition and type of economy, the level of education of the population, attitude to digitalization, the availability of gadgets and the development of the Internet - all these factors vary greatly in different parts of the world.

According to the Federal Law ‘On banks and banking activities’, the banking system of the Russian Federation has two levels: the first includes the Central Bank of Russia, the second - credit organizations (1990, Article 2), which is shown on the Figure 15. We would like to talk about the role of each participant.

Figure 15:

Two levels of Russian Banking System



Source: Financial University under the Government of the Russian Federation (2017).

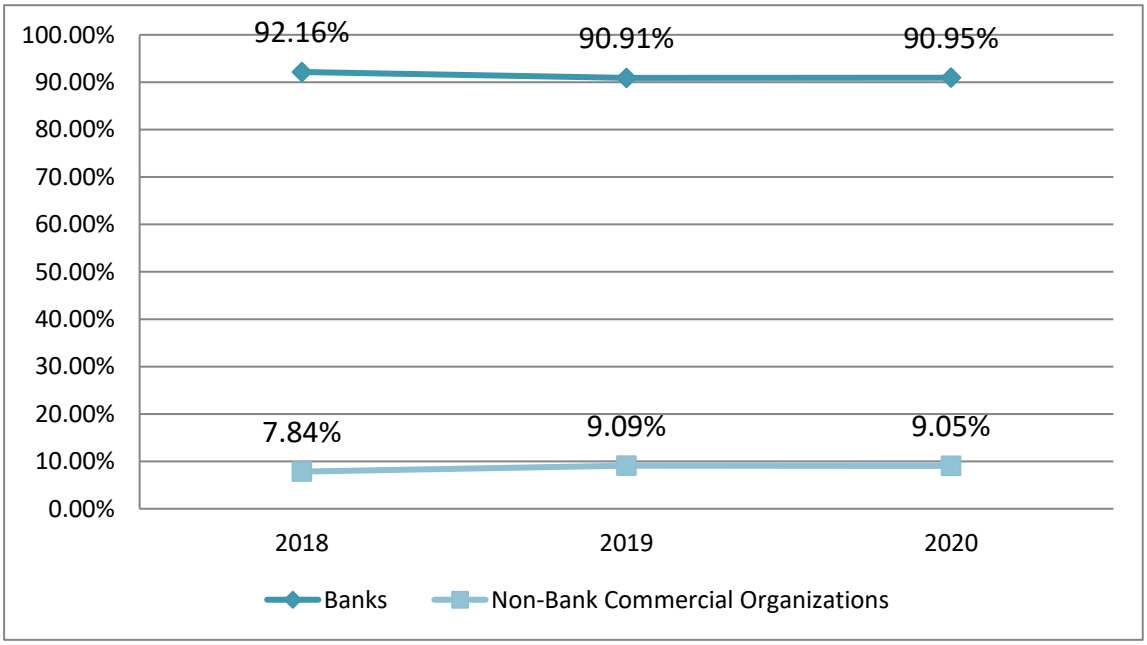
In accordance with Article 3 of the Federal Law 'On the Central Bank of the Russian Federation (Central Bank of Russia)', the objectives of the Central Bank of Russia are*: 'protection and stabilization of the ruble; development and strengthening of the banking system of the Russian Federation; ensuring stability and development of the national payment system; development of the financial market of the Russian Federation; ensuring the stability of the financial market of the Russian Federation'* (2002, article 3). The key element of the legal status of the Central Bank of Russia is the principle of independence, which is shown in the fact that the Central Bank of Russia acts as a special public-legal institution with the exclusive right to issue money and organize money circulation. It is not a public authority, but its powers relate to the functions of public authorities, since their implementation is associated with measures of government control. The Central Bank of Russia performs its functions independently of government authorities as it is written in the Constitution of the Russian Federation, as well as in the Federal Law 'On the Central Bank of the Russian Federation'. For example, there is a legislative ban on the Central Bank's direct credit to the Government. At the same time, The Central Bank of Russia has the right to issue regulations that are mandatory for federal government authorities, all legal entities and

individuals. It does not have the legislative power, but participates in the legislative process. The Central Bank of Russia is accountable to the Parliament. The Parliament appoints the Chairman of the Central Bank of Russia (a candidate is proposed by the President) and members of the Board of Directors (candidates are proposed by the Chairman of the Central Bank of Russia). Unfortunately, such a system in reality limits the independence of the Central Bank of Russia as it becomes dependent on decisions of the Parliament and the President. Among the functions of the Central Bank, touched upon in our study, we can stress three of them: '*1) it decides on the state registration of credit institutions, 2) it establishes the rules for conducting banking operations, 3) it supervises the activities of credit institutions and banking groups'* (Federal Law 'On the Central Bank of the Russian Federation (Bank of Russia)' 2002, article 4). Bank of Russia has a power to withdraw banks' licenses.

Now we would like to talk about the second level of Russian banking system - **Credit Organizations**: Banks and Non-bank commercial organizations. First of all, for the better understanding of the structure of the Russian banking sector it will be useful to look at the information on the share (in terms of assets) of banks and non-bank credit institutions in the period 2018-2020, which is shown in Figure 16.

Figure 16:

Share of Banks vs Non-Bank commercial organizations in Russian banking sector



Source: made by authors, based on data from Central Bank of Russia (2020b).

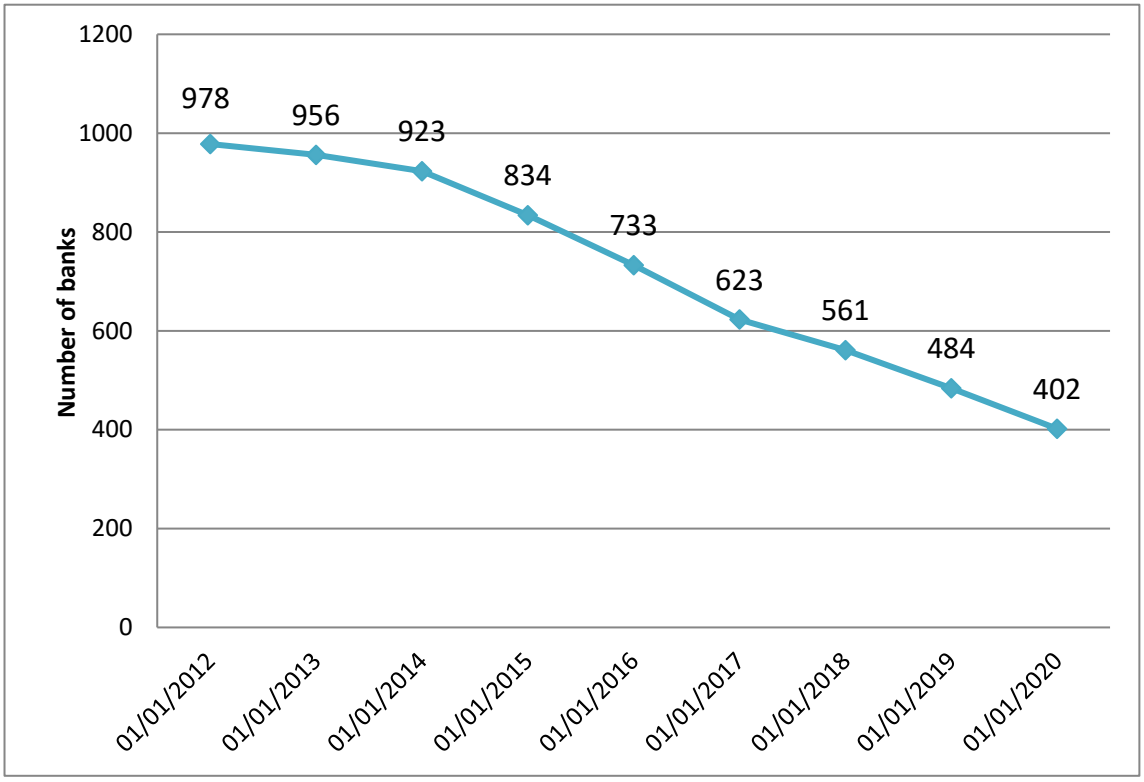
According to the Federal Law 'On banks and banking activities' (1990), **Banks** in Russia have the exclusive right to carry out all the following banking operations: *'to attract deposits from individuals and legal entities, to place funds on its own behalf and*

at its own expense, to open and maintain bank accounts of individuals and legal entities' (Federal Law 'On banks and banking activities' 1990). As noted above, the Central Bank of Russia *'controls the activities of credit institutions, issues and revokes their licenses and credit institutions, works with other legal entities and individuals'* (Federal Law 'On banks and banking activities' 1990). There are no banks in Russia that can be called completely state-owned, since the government does not fully own them. However, the government has a controlling stake in the largest banks. For example, Sberbank is half-state, the Central Bank of Russia owns 50% plus one more share, that is, a controlling stake, all other shares of the organization belong to private investors, and none of them holds more than 1% of Sberbank's securities. The same situation is with VTB Bank and Gazprombank.
After all, althow many big russian banks a rulled by the governemnt on paper the still can be called privat banks.

In June 2020 there were 389 banks in Russia (Central bank of Russia 2020b). Figure 17 shows the dynamics of the reduction in the number of banks in Russia for 2012-2020. As we can see, the number of banks has almost halved. What is the reason for this? The revocation of the license by the regulator due to poor financial condition and violations of legal requirements were the main reason for the bank's termination. The number of valid licenses was also reduced due to bank mergers, as well as voluntary refusals of credit institutions to continue their activities. Analysts associate such a significant reduction in the number of operating banks with the 'Financial Sector Recovery Process', which was started by the Chairman of the Central Bank Elvira Nabiullina, who took office in the 2014 year.

Figure 17:

Number of banks in Russia, 2012-2020



Source: made by authors, based on data from Central Bank of Russia (2020b).

Moreover, the ongoing process has greatly undermined confidence in non-state players. Corporate clients, like citizens with deposits of more than 1.4 million rubles (the maximum amount of money on the deposit, which is guaranteed to be insured by the bank), prefer to open current accounts and keep funds in systemically important banks - the largest credit banks of the country, the stability of the financial condition of which affects the banking system as a whole. This trend can be traced in the Figure 18, which shows the share of the first 200 banks (sorted by the amount of assets) in the banking sector. This share has grown significantly, and in June 2020 it reached the point of 99.4%.

What does such a global reduction in the number of credit institutions mean for the population? There may be positive and negative aspects to this situation.

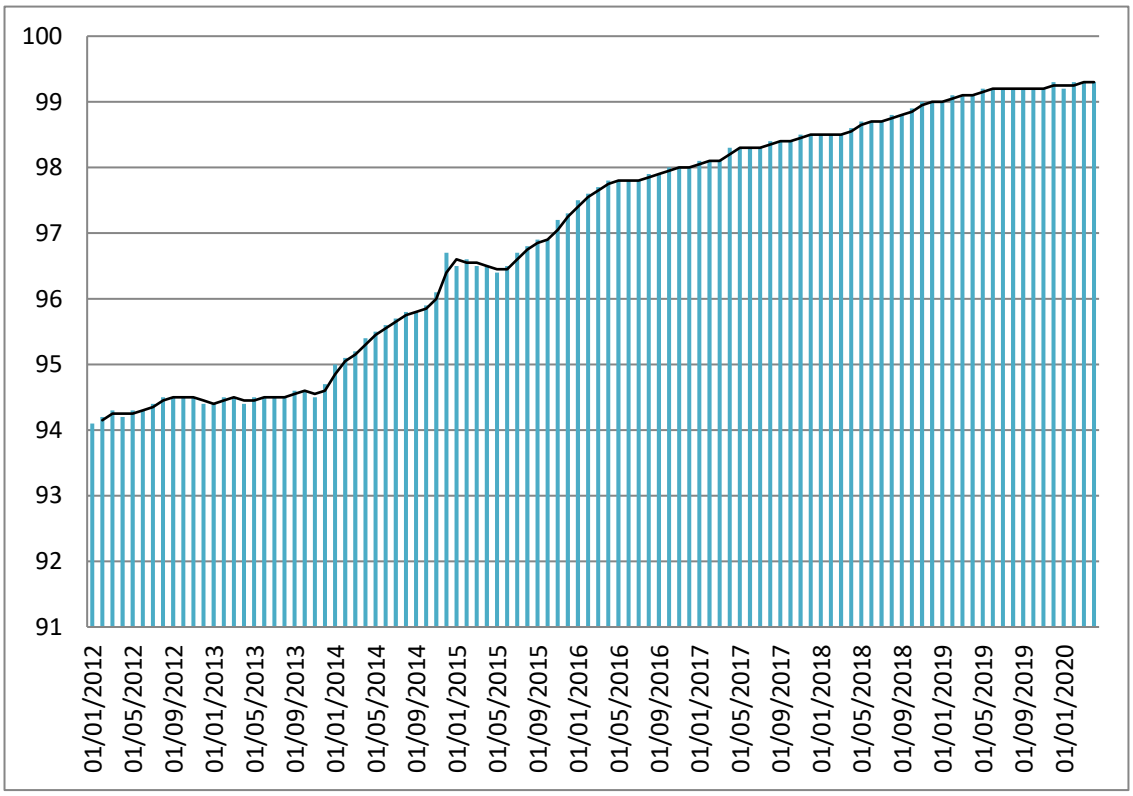
The positive effect: relative reliability of the remaining banks, but only in case if the state in some way guarantees the full fulfillment of their obligations and the stability of their activities, because at any time any of the banks that retained a license can lose it.

The negative side: a decrease in competition in the banking market. In this regard, the conditions and cost of banking services for clients may undergo negative changes,

since the largest banks don't need to compete with small credit institutions, the terms of service and tariffs which they still have to take into account at least a little when building client policy.

Figure 18:

Bank concentration, first 200 banks' share (in total), %, 2012-2020

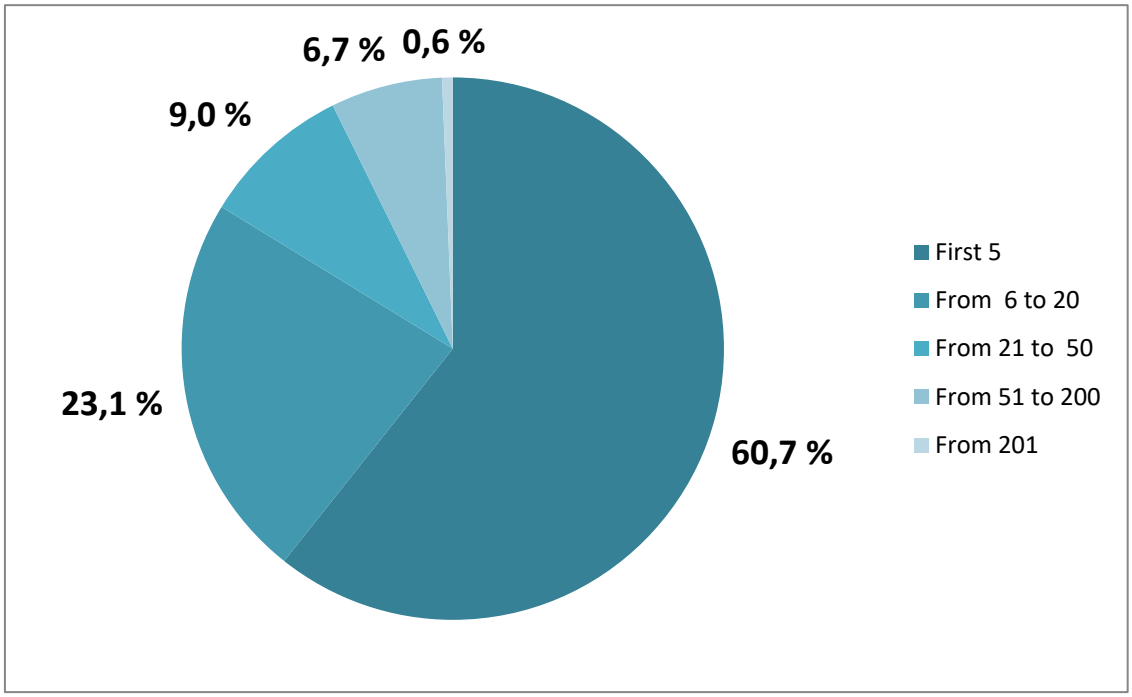


Source: made by authors, based on data from Central Bank of Russia (2020b).

One more negative consequence is an increase of concentration of banking assets. Figure 19 shows that the first 20 banks in Russia owe almost 85% of all assets of the banking sector. In the previous chapter we discussed a similar feature of the existence of giant banks in the American banking system, and we would like to notice once again that this feature increases the vulnerability of the banking sector to cyber attacks.

Figure 19:

Current bank concentration in Russia, June 2020



Source: made by authors, based on data from Central Bank of Russia (2020b).

The second type of credit institutions is **non-bank credit organizations**. A non-bank credit organization is an organization that has the right to carry out certain banking operations. Legal requirements for non-bank credit organizations are lower than for banks, which is associated with a lower degree of risk on transactions.

There are three main types: settlement non-bank credit institutions (RNCO, all of the abbreviations for the non-bank credit organizations further are Russian abbreviations written in Latin to acquaint the reader with how they are called in Russia), payment non-bank credit institutions (PNCO), and non-bank depositary organizations (NDCO).

Settlement non-bank credit institutions (RNCO) carry out the following types of activities: they open and maintain accounts of individuals and legal entities, make settlements, buy and sell foreign currency in non-cash form, and operate in the securities market. NBCO has no right to attract deposits and issue loans; it provides a system of settlements and transfers.

Payment non-bank credit institutions (PNCO) have the right to make money transfers without opening bank accounts and other related banking operations. Compared to the settlement payment non-bank credit institution, a narrower range of operations is allowed. It should provide a risk-free transfer system within the framework of the organization of instant, electronic, mobile payments.

Non-bank depositary organizations (NDCO) can attract funds for deposits, issue bank guarantees, buy and sell currency in non-cash form. In other words, NDCO is not entitled to carry out settlement operations, but it can carry out certain credit and deposit operations.

Non-bank credit institutions, like banks, are regulated by the Central Bank. The total share of non-bank credit institutions in 2020 does not exceed 9% (Figure 14). The number of these organizations remained almost unchanged since 2018 (44 in 2018, 40 in 2020), but the share in the banking sector is steadily increasing due to the reduction in the number of banks.

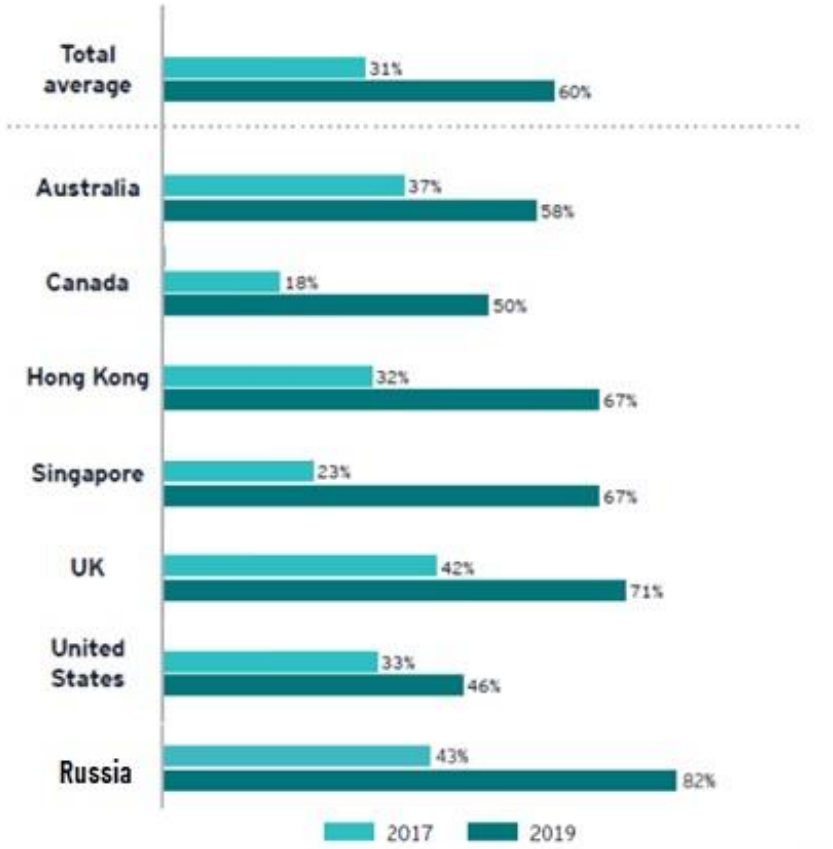
The type of Russian banking system has significantly influenced the development of digitalization, which we will discuss in the next subchapter.

3.2. Development history and current state: from traditional bank to digital laboratory

Banking digitalization is a complex task that cannot be simply ‘started’ or ‘implemented’. It requires a serious preparation of the material base, such as the provision of the population and business with technical means, as well as the willingness to accept changes in providing and getting services on both sides, staff training, etc.

The main factor which allows banks to step into digitalization is the fact that the population has technical means to access the Internet and want to use Internet services. The Figure 20 demonstrates the level of fintech adoption in seven markets including Russia. We can see that the percentage in Russia in 2018 is 82%, which is well above average (60%); moreover, it is the highest value of the graph.

Figure 20:
Comparison of fintech adoption in seven markets in 2017 and 2019

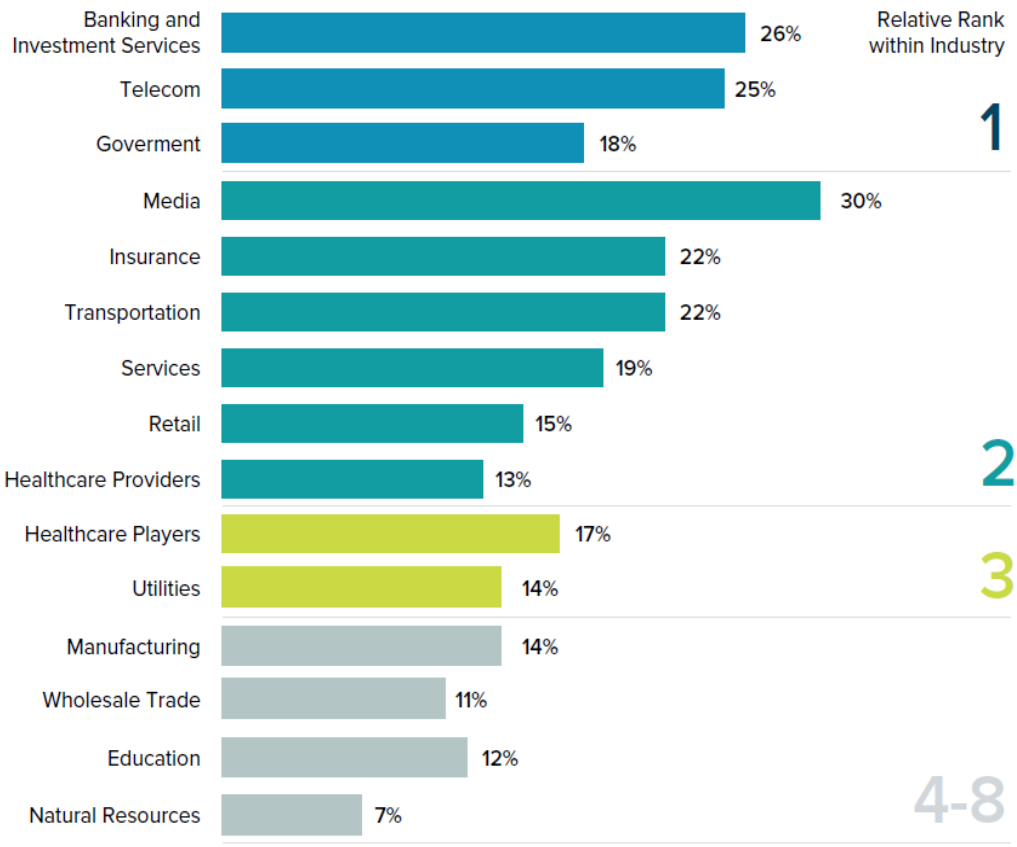


Source: EY (2019).

The percentage of the Russian population who could be interested in Internet services and technologies in general can also be demonstrated by the graph of Internet penetration. We see an increasing trend in the share of users, the percentage in 2018 exceeded 80%, which is a significant indicator. Internet users, as a rule, have a positive attitude towards digitalization and the transition of services to the Internet, which could also become a factor of the rapid development of banking digitalization in Russia.

Moreover, the majority of Russians consider the banking sector a priority for digital transformation, which can be seen in Figure 21. As we can see, according to the World Bank (2018), the category which includes Banking services, Telecom and Government services rank first in terms of the average Business Priority Ranking of Digital Transformation, which suggests that this industry is the most promising for technological change. Moreover, within the sector, the banking sector is in the lead. This once again confirms that the digitalization of the banking sector is a priority for the population and the state.

Figure 21:
Business Priority Ranking of Digital Transformation by Industry, % of respondents



Source: World Bank (2018).

Digitalization is rapidly transforming countries, continents and regions. The use of innovations is changing the way we live and do business. Technologies, and especially technologies in banks, have always had a lot of impact and reflected the trends of the newest tech-trends, since the financial sector was always attractive because of accumulated resources. We want to take a look at how technologies have developed in the world and in Russia in particular, what services arose at certain stages. For the purposes of our research it will be enough to consider the evolution of remote banking service channels since the beginning of the 21st century.

Since the beginning of the 21st century, information technology for remote banking has been rapidly improving. At the present stage, we can distinguish the following types of remote banking channels, depending on the type of technology: telephone banking, terminal banking, mobile banking, Internet banking (Dolgushina, 2016).

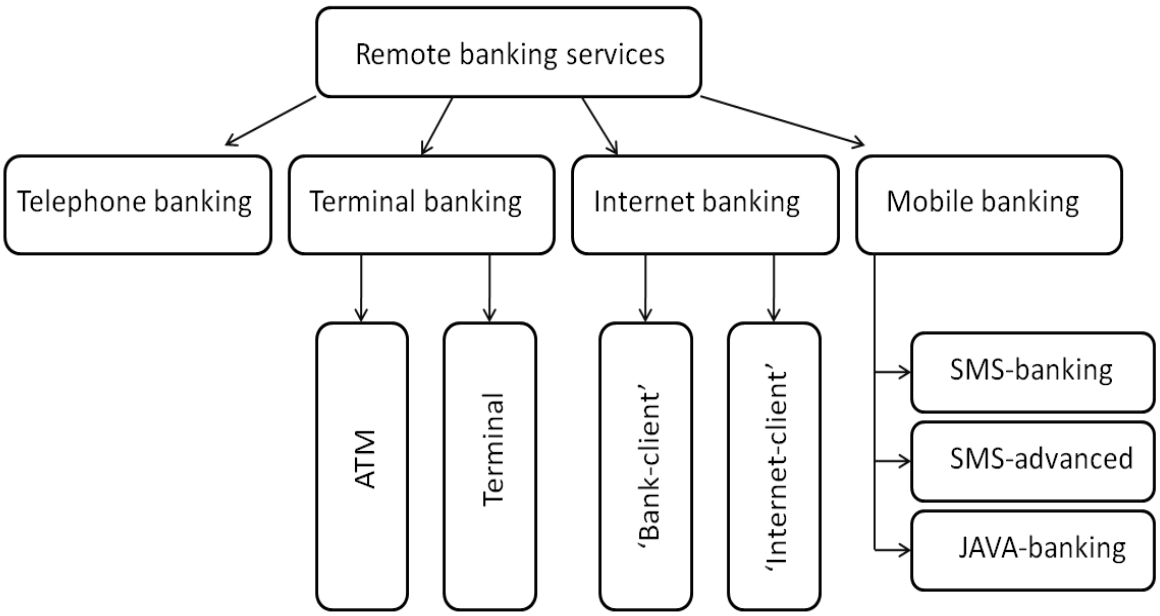
To begin with, we would like to provide definitions of remote banking channels, which are provided in Dolgushina (2016):

- *Telephone banking* is a system for providing remote banking services through a telephone connection.
- *Terminal banking* is a system for implementing remote banking services BS through self-service terminals, the types of devices for which are both ATMs (Automated teller machines), terminals (Point of Sale (POS) terminal or credit card terminal – *'a device which interfaces with payment cards to make electronic funds transfers'* (European Payment Council 2019, p. 2), and automated bank kiosks (which provide banking services for remote areas).
- *Internet banking* is a modern low-cost service for providing information and financial services to the bank customers online.
- *Mobile banking* is a system for remote banking services via a mobile phone.

All types of remote banking services, which we have now defined, will be described below and also shown in Figure 22.

We would like to describe the evolution of remote banking channels separately in the order of their historical origin in the world and in Russia. At the same time, having studied the literature we have found, that the key points in the development of remote banking are similar in Russia and globally. Since a 'tech-discovery' is made, it quickly spreads around the world, especially into the tech-friendly countries to which Russia belongs. Therefore, in describing the evolution of banking development, we often use global dates not only Russian ones.

Figure 22:
Remote banking services structure



Source: made by authors, based on data from Dolgushina (2016).

The first channel for remote banking was historically **telephone banking**. The widespread use of electronic computers has significantly improved the technological aspect of remote banking. In the 1990s, the first bank-client systems were introduced in Russia. Bank-client systems are the systems which allow depositors to control their accounts by connecting to a bank. Since its inception, telephone banking has gone from a telephone connection by an operator through telephone communication systems using huge devices to an automated connection with a client via IP telephony using cloud platforms. Now the telephone banking system is used by the older generation to check account balances, information about connected services, and other simple actions that do not require operator participation.

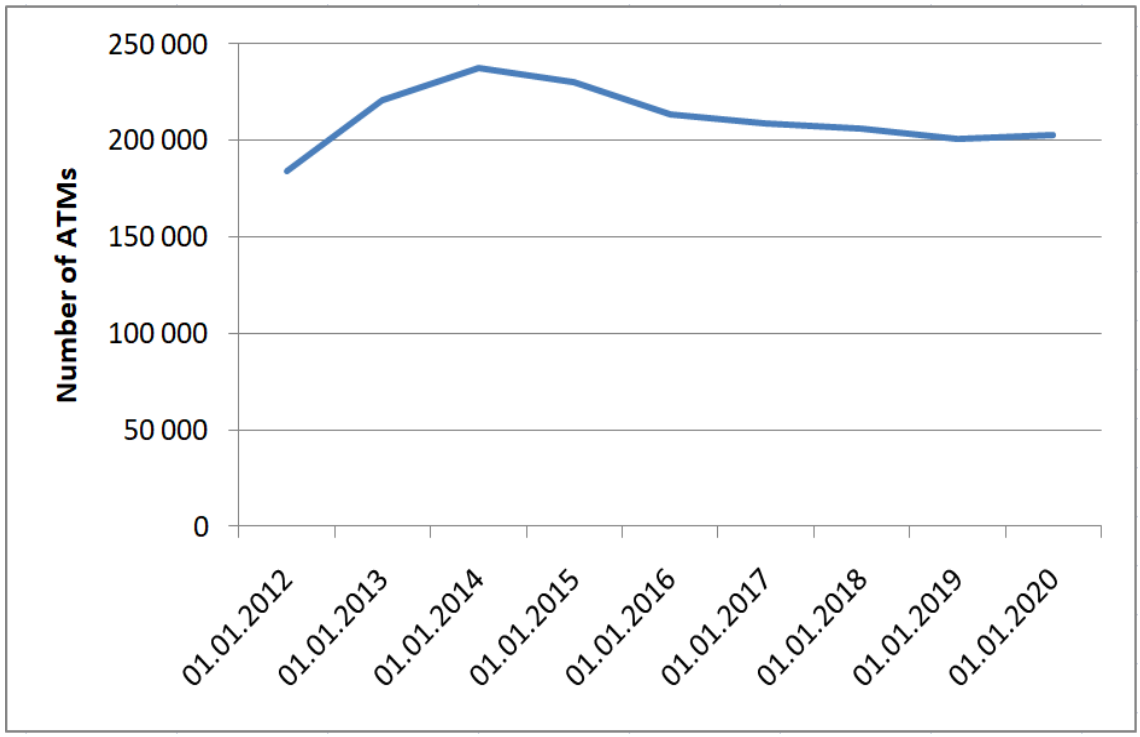
Terminal banking is historically the second remote banking channel. Terminal banking exists in two forms: ATMs and terminals.

Since the installation of the first ATM in 1967, its capabilities have been constantly improved. The first ATM which was created was cash-out only. A cash-in ATM with the function of accepting cash appeared in the late 1990s. The first ATM appeared in Russia in 1994. In the early 2000's the first ATMs with the cash-recycling function appeared - a function that allows a person to receive cash deposited by another customer into an ATM. At the beginning of the XXI century, ATMs around the world,

including in Russia, began to be supplemented with biometric and virtual computer technologies. Thus, terminal banking has evolved from large technical complexes without communication with the bank to compact devices with built-in biometric and virtual technologies. But the ATM system is still evolving and the new technologies quickly spread around the world.

Talking about numbers, Figure 23 demonstrates that the number of ATMs in Russia grew rapidly, and then reached its peak in 2014-2015. After that point it began to slightly decline and currently it is in a state of stagnation. We will see the reasons for this decline later when we look at the evolution of other digital banking channels.

Figure 23:
Number of ATMs in Russia, dynamics, 2012-2020



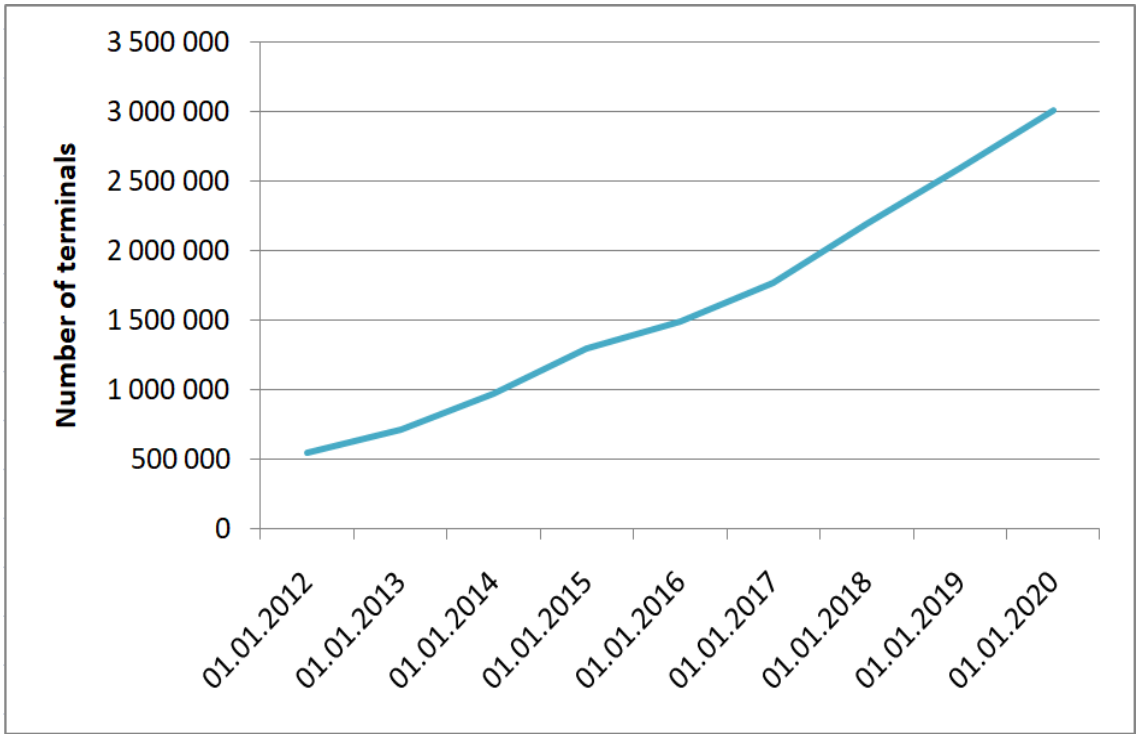
Source: made by authors, based on data from Central Bank of Russia (2020b).

POS (Point Of Sale) terminal is electronic software and hardware device for accepting payment cards (European Payment Council 2019). POS terminals have gone through a difficult development path from their prototype in the form of a mechanical cash register to mobile POS terminals. The defining event in the history of POS development is the emergence of cloud technologies. Cloud POS systems are independent of platform and operating system constraints, and are compatible with a wide range of POS machines and sometimes tablets. Thus, cloud technologies

contributed to the integration of POS systems into mobile devices. Terminal banking has become more mobile, interactive and virtual.

Figure 24 shows that the number of terminals in Russia continues to grow rapidly; in 2020 this amount is 6 times bigger compared to 2012, which is the fastest and most significant growth among all remote banking channels.

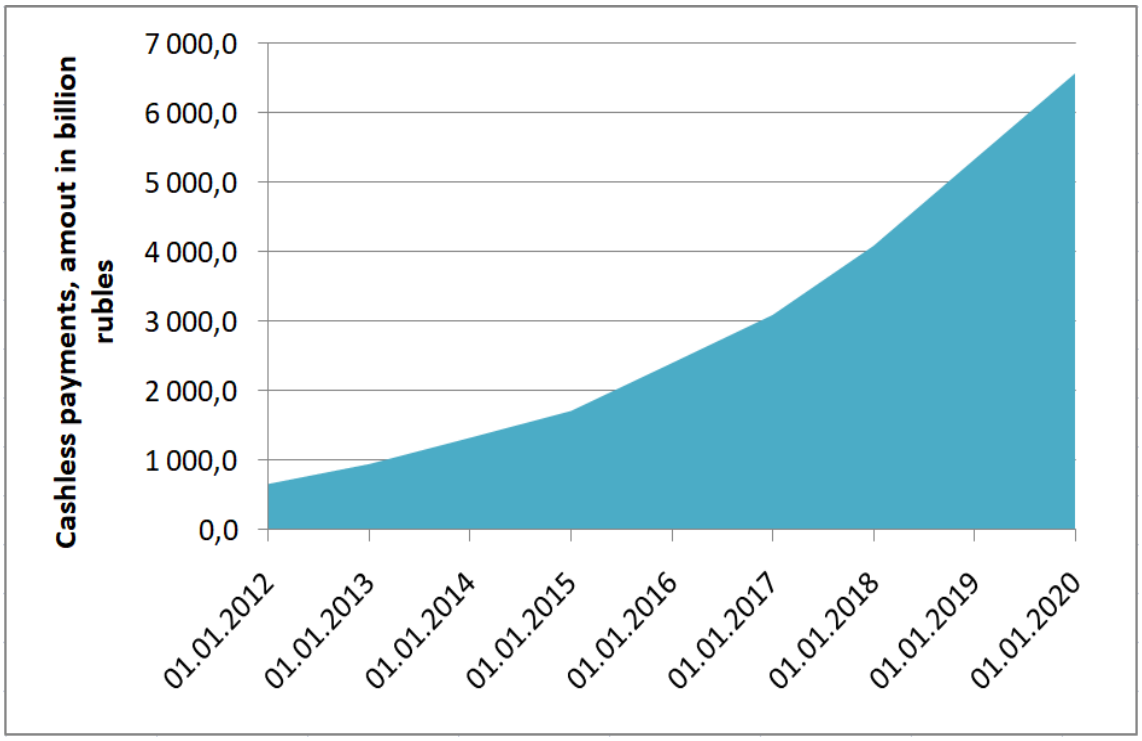
Figure 24:
Number of POS terminals in Russia, dynamics, 2012-2020



Source: made by authors, based on data from Central Bank of Russia (2020b)

Comparing the development of ATMs and terminals, we can note that the curve of terminals is more vertical since 2014-2015, and the increase is more significant than in previous years, while the dynamics of ATMs is the opposite. This happened due to the fact that since 2014-2015 there has been a sharp decline in interest in ATMs and physical branches of banks in Russia with the following transition to online. This led to a decrease in the volume of cash withdrawals and, consequently, to an increase in electronic payments, as shown in Figure 25. From 2012 to 2020 the amount of cashless payments for goods and services increased more than 7 times. We have omitted the dynamics of GDP, inflation and other macroeconomic indicators in order to show only the general growth trend, which, of course, would have persisted if all of the above factors were taken into account.

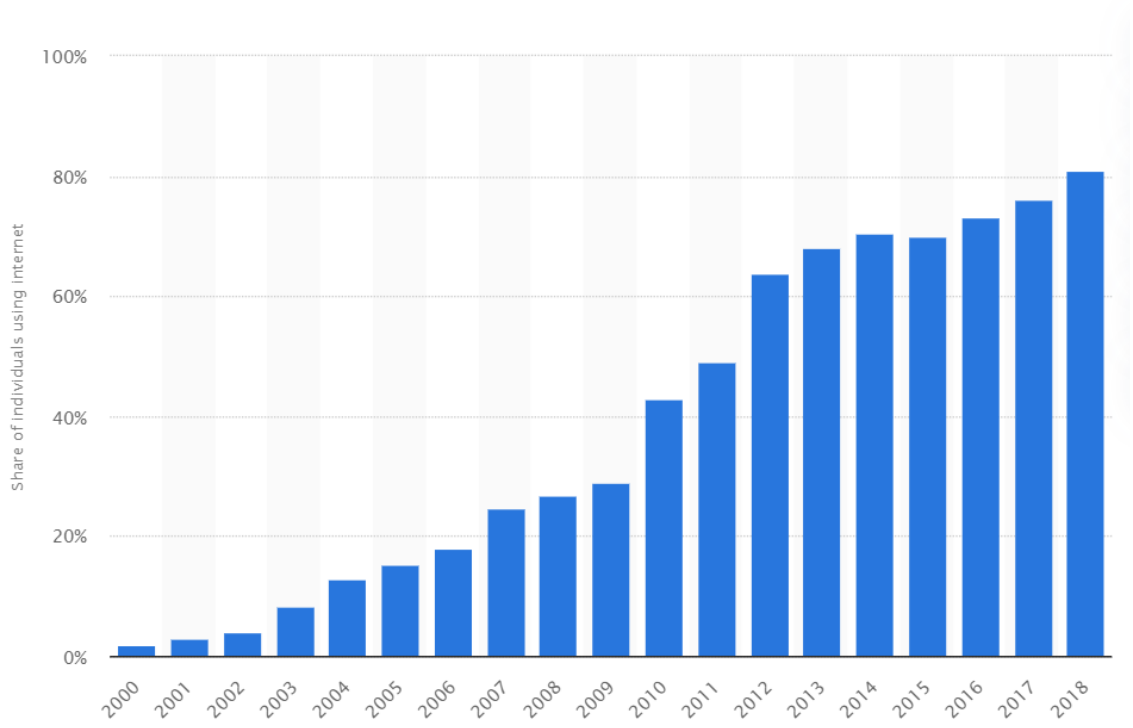
Figure 25:
Dynamics of cashless payments in Russia, amount in billion rubles, 2012-2020



Source: made by authors, based on data from Central Bank of Russia (2020b).

The third channel of remote banking services is **Internet banking**. The advent of the World Wide Web in the early 1990s allowed banks to create the first Internet banking systems using a wireless connection to a bank server; it was a 'bank-client' system, the definition of which is provided above. In 1994, Internet banking was integrated into Microsoft software, after which 100,000 depositors connected online account service. In Russia 'Internet banking' appeared in the late 1990s, it was based on the systems 'Internet – client', at the beginning it developed very slowly. *'By 2006, the number of remote clients at the flagship of Russian Internet banking at that time, Alfa-Bank, was only 100 thousand people, and the leader of the Russian banking system, Sberbank, did not have a remote service system for individuals at all'* (Dolgushina 2016, p. 36). The growing number of Internet users in Russia (Figure 26) and the widespread adoption of more portable devices such as laptops, netbooks and ultrabooks, have allowed Internet banking to grow rapidly.

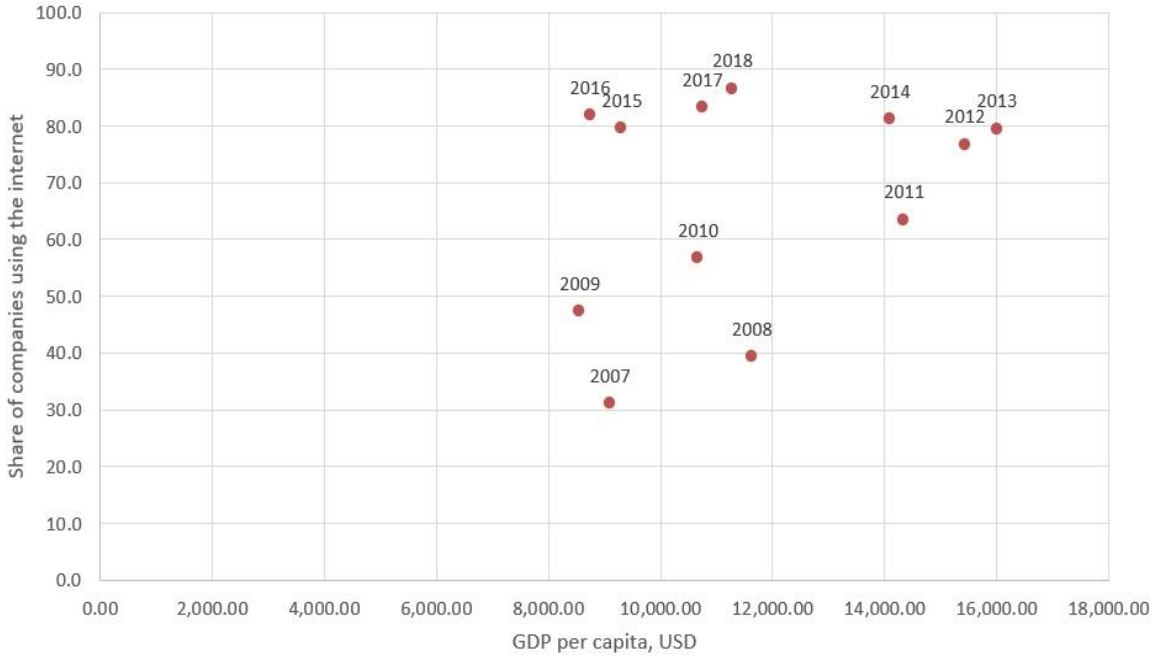
Figure 26:
Internet penetration rate in Russia, 2000-2018, %



Source: Statista (2020).

On the abscissa, Figure 27 shows Russian GDP for a certain year, on the ordinate - the share of companies that have access to and use the Internet. According to the Figure, we can see that in 10 years period the share of business using Internet has almost tripled. And in 2018 the position of the point on the map (Figure 3 from the Chapter 2) would look differently. It means that the amount of banks-internet users which are part of the business sector has increased. This prepared the platform for digitalization even more solidly.

Figure 27:
The relation between russian GDP per capita (in USD) and share (%) of companies having access to and use the Internet in Russia



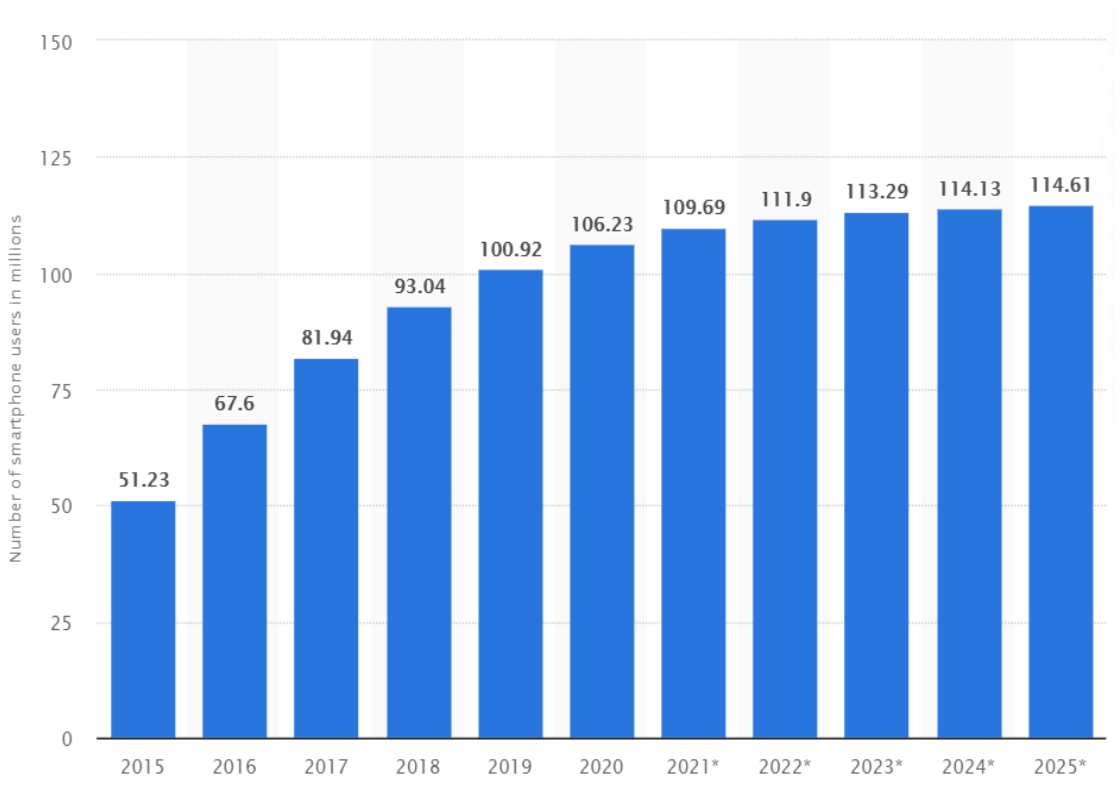
Source: made by authors, based on data from Central Bank of Russia (2020b) and World Bank (2020).

The history of the emergence of **mobile banking** starts in the end of the XX century. The earliest remote mobile banking services were carried out using SMS messages. The foundation of mobile banking is associated with the emergence of smart phones that support WAP (Wireless Application Protocol) technology. Further, cyber frauds led to a new type of mobile banking – SMS-Advanced banking, which was based on the use of a special card that allowed generating an encryption key again while performing authentication. An important technological step towards the creation of mobile banking was the separation and specialization of the Java language into the Standard Edition, which was intended for ordinary computers, the Enterprise Edition, used on servers, and the Micro Edition, which is used in mobile devices. Since 2004, mobile banking and the mobile payments industry has matured, and large-scale projects have begun to be implemented. From 2007 the use of banking services around the world and in Russia has been moving from personal computers to smart phones. In 2009-2010 the first java applications for Iphones appeared after which Java banking began to grow even more significantly. Thus, mobile banking technologies in Russia have evolved from simple SMS confirmation of payment to smart phone-based applications with full-featured banking. Since 2013, Russian banks have begun to move away from

conventional Java applications and favor more convenient and user-friendly technologies. Since mobile banking is a relatively new player, its stage of active growth continues.

On the Figure 28 we can see how the number of smartphone users (in millions) in Russia has grown significantly in the period from 2015 to 2020. And according to the Statista (2020) forecast, it will continue to grow until 2025. Considering the total population of Russia, which in 2018 was 144.5 million people, and has a tendency to decline, it can be said that by 2025 almost the entire population of Russia will become smartphone users. It makes mobile banking very important for Russians.

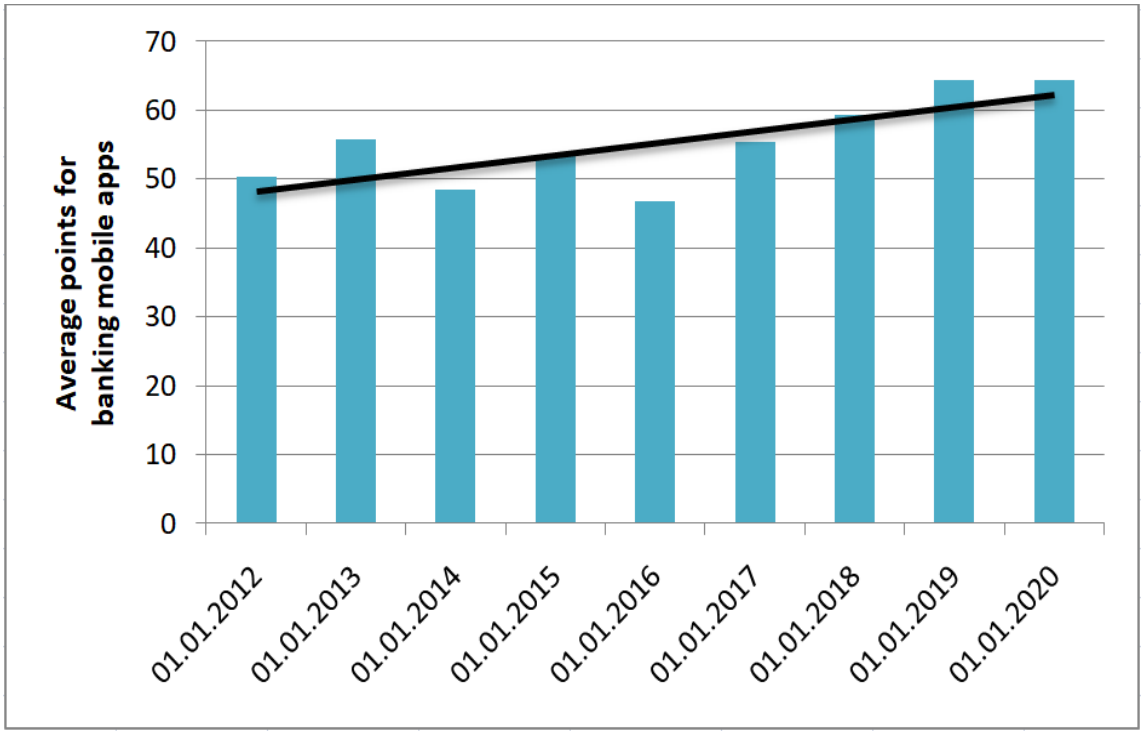
Figure 28:
Number of smartphone users in Russia from 2015 to 2025 (in millions)



Source: Statista (2020).

In the Figure 29 we can see the average points gained by mobile applications of the largest 30 banks in Russia for the period 2012-2020. The trend (a black line) is growing, as more and more attention is paid to mobile applications by companies, that is the reason why the average rating grows.

Figure 29:
Mobile banking rank, average points of russian molile bank apps rated by Markswebb consult in 2012-2020



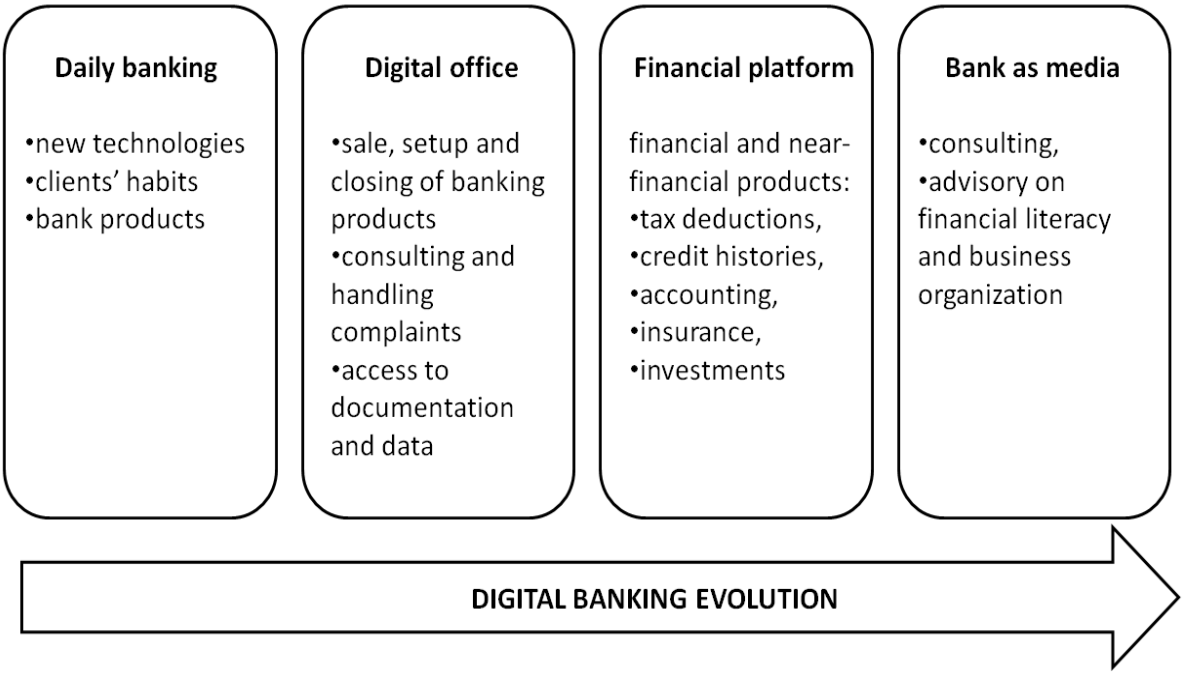
Source: made by authors, based on data from Markswebb reports (2020).

Summing up the digitalization of banking service channels, we can draw the following conclusion. Telephone banking has practically ceased its development - it has remained the prerogative of the elder generation and it is used to check accounts and perform the simplest transactions. The number of ATMs is declining, giving way to cashless payment terminals at points of sale. Many Russians make purchases online or paying by cards. The growing number of Internet users is giving a very strong impetus to Internet banking, which in turn is growing more slowly than mobile banking. Banks are now focused on improving their mobile applications and online service.

What is digital banking striving for in Russia? Now we will take a look at the Figure 30, in which the Markswebb agency depicted the path along which the Russian Banking system wants to go in the coming years of rapid development. We will explain each step more detailed.

The development of digital banking is taking place in several paradigms that are layered on top of each other, that is why each of them is interconnected with the previous one.

Figure 30:
Digital banking evolution: steps and their description



Source: made by authors, based on data from Markswebb report (2020).

Daily banking – all the tasks and needs associated with obtaining information on a product, as well as making payments and transfer money with it. This banking type focuses on meeting the basic needs of the client, hence daily banking is an integral part of any Internet bank. Daily banking mostly works with 1) new technologies, 2) clients' habits, 3) bank products. All areas of development of bank customer service are very closely related to technology, innovation, digitalization. This is because the process of interaction between the bank and its customers is changing. If earlier the bank used to say: "Here are my services, my offices, my Internet bank, come and use it", now the bank itself moves to the place where it is more convenient for the client to use the services. Penetrates into all spheres of human digital life, placing its services in those channels where it is demanded by users: in a mobile phone, social networks, portable devices. And this cannot be regarded as a rejection of offline sites, but only an expansion of interaction.

The next step is **Digital office**. Some user tasks are historically associated with visiting a branch: closing and opening an account, obtaining inquiries, resolving claims, etc. Digital office concept assumes that all of these tasks may be transferred to digital channels, as the result the client stops any kind of physical interaction with the offline branch. Economically, it saves a lot of money on customer service and additionally stimulates the transition of all processes to digital channels.

Financial platform appears when a bank transforms into a marketplace: bank helps clients quickly and conveniently to solve basic financial issues such as getting tax deduction or making an investment decision.

The last stage of digital transformation for banks is **Bank as media.** Here bank acts as an advisor, expert, consultant who helps clients to solve various consumer problems and problems, offering him useful products and services.

The main features of each step are presented on Figure 30.

Now the Russian market is at the intersection of two concepts - daily banking and digital office. Daily banking in Russia is already at a very high level, there will be no breakthrough here: the main development focus for banks in the next few years will be the digital office paradigm. Nevertheless, at any stage of digital banking development, daily tasks do not disappear; they correspond to new technologies and user habits which are formed under the influence of Yandex, Facebook and Google.

So what is digital office? The better we understand the concept itself, the better we can imagine the Russian banking sector in the nearest future.

First of all, it has four main features:

1) Availability: the client should be able to connect to the service at any time, quickly and remotely. For existing customers - a simple entrance, for new ones - a digital service as the first point of interaction with the bank.
2) Product Management: Any products should be possible to customize, manage, and reject. Offline services in digital channels are as important as online ones.
3) Legitimacy: the client should always have an access to his data in the bank, the banking conditions and the confirmation of the actions which are taken.
4) Communication: the client should be able to use a digital services to solve all issues related to the products and services of the bank, to receive advice and to conduct claims.

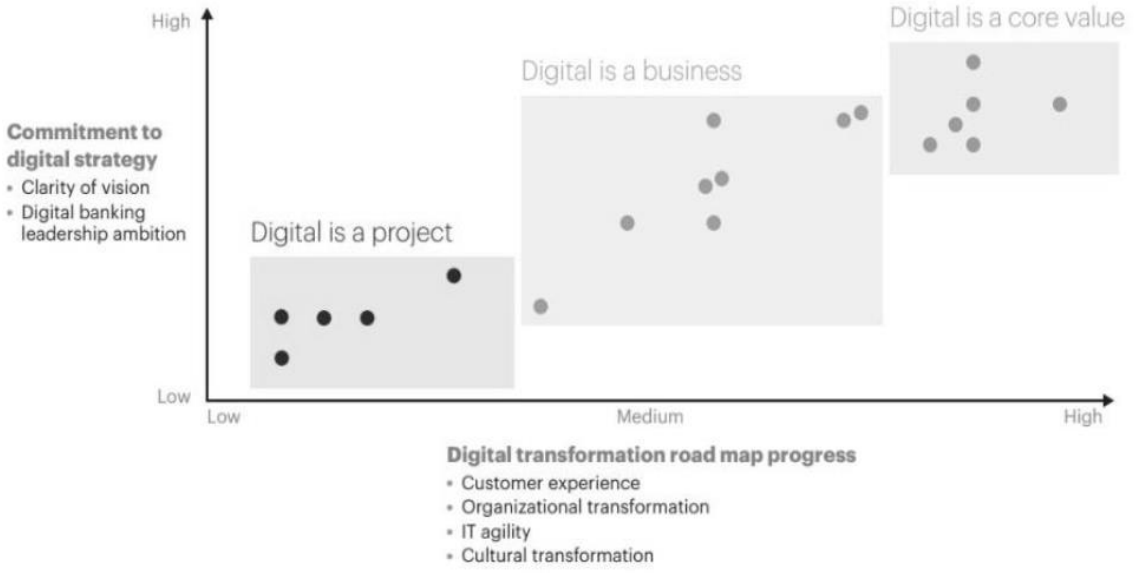
The availability, management of products and their sale in Russian digital services are well developed, but there are some problems with legitimacy and communication: the development of these components of a digital office requires the cost of restructuring processes within the bank but does not bring direct income. It mainly affects customer loyalty which is underestimated by some banks.

We have looked at where banks want to go. Now we want to talk about the ways they want to achieve this.

In terms of the development of the financial sector, *'digital transformation is seen as improving the applied methods of doing business, which creates a new working environment'* (Markswebb 2020, p. 10). Because of the processes of banks digitalization, personnel will be required that are capable of solving professional tasks based on the application of the achievements of digital technologies. *'In the formation of digital operating models, it will inevitably require not only the improvement of staff skills, but also the creation of new positions, such as the director of digital technology or the director of innovation development, which can be hired as new staff, and be selected from the existing employees of the bank'* (Markswebb 2020, p. 10).

There are three approaches to understanding the digital transformation of the banking sector, which are shown in the Figure 31. The abscissa is an indicator of digital transformation progress, which can be low, medium or high. As it is mentioned on the Figure, it depends on clarity of vision and digital banking leadership ambition. Ordinate - commitment to digital strategy, recognition of its paramount importance, which can also be high or low. Four things have an impact on this index: customer experience, organizational transformation, IT agility and cultural transformation.

Figure 31:
Three ways a bank can start digitalization process



Source: Kosheev, Tsvetkov (2018).

The first approach *Digital is a project* is the introduction of digital technologies through separate projects, which does not contribute to further full-size digital transformation. In it, digital transformation is being introduced gradually, based on

long-term planning and implementation of pilot projects. In Russia about 26% of all banks use this approach.

The second approach *Digital is a business* helps to digitalize the bank by creating a subsidiary that takes into account all the needs of the digital economy. The advantage of this approach is that teams are created within the organization, including various specialists in the areas of IT, data analytics, marketing, and due to this, a high flexibility of the organizational structure is achieved, as well as prospects for new activities appear. The majority of Russian banks, 42% of them, use this approach.

The third approach recognizes *digital technology as the main value* of the organization. This method is sometimes combined with other approaches, but it includes *'a more complete implementation of the digital strategy through the transformation of all internal and external processes of the bank'* (Kosheev, Tsvetkov 2018, p. 41).

Russian banks use all three approaches to digitalization, depending on what share of the costs of digitalization in the bank and what role it plays. Nevertheless, this process currently has some barriers. Some of them have already been noted in the text of our work, but now we would like to once again draw attention to the main barriers.

One of the most important barriers is cyber security and data protection. Moving further and further along the steps of digitalization, society exchanges more and more data, stores information in the clouds, has digital signatures and electronic document management. All this, of course, carries a threat, since attackers may want to steal, use or change data for their own purposes. This threat seems to us the most important, and therefore will be considered in a separate chapter of this work.

Another obstacle to the development of digital banking in Russia and other countries is legislation system that does not allow starting a customer service without the physical identification. In the current reality, it is not possible to change the banking system completely. The client must be identified, therefore either he goes to the branch, or a bank employee comes to him. The possibility of the emergence of exclusively digital banks may happen only after the population will be fully identified, through a single digital signature or other mechanisms. Digital banks which already exist in Russia, such as Tinkoff Bank (an Internet bank, an analogous to German N26), cannot yet deny offline communication with customers, although they have been minimized. Bank agents perform the identification process, and it has reduced the costs of the company a lot. Tinkoff tried to refuse its own ATM network by switching to partners' terminals, but realized that it could lead to lose a large number of customers, and then returned its ATMs.

The next weak point of banks without offices is the low capacity for resolving emergency situations. In addition, there are times when *'the client must exchange original documents with the bank - then you have to rely on postal services of varying degrees of reliability'* (Digital Banking Report 2016).

Another problem is depositing cash. For this, online banks use partner cash-in terminals and, less often, their own ATM network with the cash-in function. But it is not enough for needs such as depositing large amounts - most terminals have restrictions on the sum of money a person can deposit. In this case, *'the client will have to look for branches of partner banks with physical cash registers in order to deposit cash with a minimum commission'* (Digital Banking Report 2016). It is definitely not convenient, especially for Russian clients which are got used to good level of service.

But the most serious is that online banks are more likely to violate laws and receive a foreclosure or lose their license for it. This primarily concerns the laws on combating money laundering and the financing of terrorism. Having a client who has never appeared at the branch of the bank, using only mobile confirmations - this generally fits into formal norms, but does not fully comply with the law.

Digital banking specialist Jim Marous, co-author of the Digital Banking Report, states *'five indisputable truths'* of new generation banks (Digital Banking Report, 2016). These theses may seem radical, but an expert substantiates each statement:

1. Banks need to invest into the development of 'digital', not offline. For example, over the past 5 years, the number of visitors to bank offices in the United States has dropped by 60%. The same trend we may notice all over the world. Opening of new offices today knowing that tomorrow they will not be needed is unreasonable.
2. Customers want to open and manage accounts online. In fact, clients have to go to the office only because they have no alternative. If there is a good banking application that allows opening an account in a few clicks, they will prefer it.
3. Attracting new customers using multi-channel always works. When a company uses targeted and bulk email newsletters, mobile messages or online advertising, investments generate income. Working with the audience always increases the number of clients.
4. Consumers want personal attention. The fact that he is well-known at the nearest coffee shop, airline or hotel that he uses strengthens his bond with this business entity. But nobody knows him at the bank where he keeps his savings, and it does

not improve the level of confidence. Non-financial organizations pay much more attention to personalized service than banks.

5. Simplicity always wins. In the new era of digital banking, those organizations that can offer customers the easiest way to buy a product will win. The apps that have gained the most popularity allow the customer to get goods or services in a few clicks: Uber, Amazon, Google, PayPal. Banking applications should be just as simple and understandable.

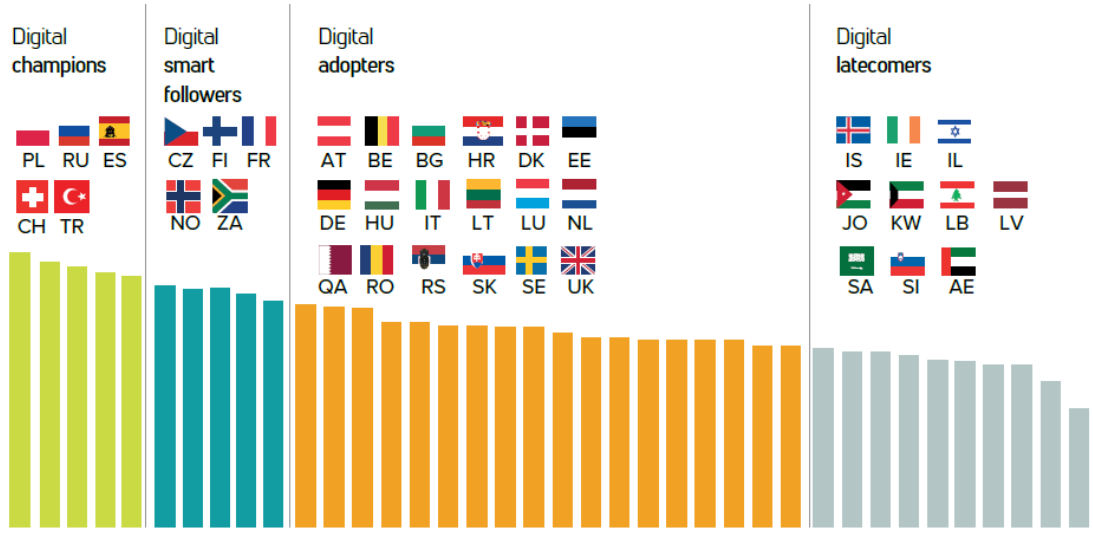
According to Jim Marous, until these 'five truths' are accepted by the banking community, it is not possible to step into the digital banking era. As the main barrier for banking digitalization he names the inertia of the industry.

It is difficult to argue with this: on the one hand, banks are implementing digital solutions, interacting with customers online, and on the other hand, the established banking structure has not changed, it has just added a digital part. Banks create the basis for the functioning of the entire market economy; therefore any abrupt changes are fraught with additional risks for the whole society.

It turns out, that on the one hand we have agile, machine learning and big data. On the other hand: the existing bureaucratic difficulties fading in additional remote control.

But it should be noted that digitalization is developing very quickly. Turning back 10-20-30 years ago, the banking sector simply could not be recognized. Summing up this chapter, we can say that digital transformation of the financial sector in Russia is advancing rapidly, acting as an example in terms of transformation for other sectors and placing Russia among the leaders of digital development. It is confirmed by the Figure 32, which shows the state of maturity of digital banking in different countries.

Figure 32:
Groups of countries in Terms of Digital Banking Maturity



Source: Deloitte Digital (2019).

In this chapter, we got acquainted with the structure of the banking sector, and also examined the history of digitalization channels in Russia, their current state, trends and barriers. Now we would like to move on to numbers: why are banks focusing on digitalization? Is it just to keep up with global trends, or does digitalization bring them additional income? In the next chapter we will try to answer this question.

Chapter 4. Practical aspects of measuring the digitalization impact on the performance of the financial sector organizations on the example of banks: parametric modeling (Samsonova, Voronina)

In this chapter, we will describe a model that measures the impact of digitalization on the efficiency of the banking sector: first, we will talk about the parameters and data used, then we will go on to describe the model itself, and at the end we will move on to the results and conclusions.

4.1. Methodology and parameters selection

The analysis has considered two regression models and these models will measure what the financial performance of the selected banks in Russia depends on. The technique of analysis we will use is multiple linear regression model and the data which will be used is pooled cross-sectional. The variables of the research are divided into two categories: dependent and independent variables. To start with, we would like to provide the definitions of both types: dependent variable is something that depends on other factors, while independent variable is something that cannot be changed by the other variables we are trying to measure. The data for both of them are introduced to the regression model. We are going to build two models which differ in dependent variables. First, we will talk about the dependent variables in our research and then about the independent ones.

Dependent variables

The dependent variable of our study should be profit, since it is it that reflects the efficiency/inefficiency of the bank. Choosing a proxy and having read the sources from Chapter 2, we realized that profit is one of the most important estimates, but it does not always give objective information about the level of a bank's efficiency. The indicators of the bank's performance are the indicators of profitability. Their economic meaning is that they characterize the return of a bank's financial resources, i.e. profit received from each ruble of funds.

The dependent variables we have chosen for our models are Return on Assets (ROA) and Return on Equity (ROE). According to the European Banking Federation (EBF), *'The return on equity (ROE) and the return on assets (ROA) are key indicators*

to assess the bank sector's attractiveness' (2018). Another reason for choosing them is that they have been widely used in most recent research which were discussed in the literature review above.

Return on assets (ROA) measures the internal-based financial performance. It shows how much profit is received for each monetary unit invested in the property of the organization, reflects the ability of the organization to generate profit. The return on assets is determined as the quotient of dividing the net profit (or loss) received for the period by the total amount of the organization's assets for the period.

$$ROA = \frac{Net\ Income}{Total\ Assets} * 100\%$$

The second model will be regressed on the main indicator of profitability used in the practice of analyzing banking activities - **return on equity (ROE)**. ROE measures the amount of a bank's income that is returned as shareholder equity. It shows how effectively the capital is invested in the business, how effectively the company uses its assets to make a profit.

$$ROE = \frac{Net\ Income}{Total\ Equity} * 100\%$$

One of the main differences between ROE and ROA is debt. If there is no debt, the company's equity and total assets will remain the same. But if the company decides to take out a loan, ROE will be greater than ROA. It is advisable to look at both ROE and ROA in order to get to a conclusion about the financial health and performance of a company. They have different perspectives, but when the results of both are combined, they provide a clear picture of the management effectiveness of any organization.

Independent variables

There are 7 independent variables in our model called factors, which are demonstrated in Table 2.

Table 2: Variables of the regression model and their formulas

Variable	**Formula**
KRBR (The key rate of the Central Bank of Russia)	*ready data is taken*

GDP per capita (annual) *	*ready data taken (with a predicted value for 2020)*
BS (Bank Size)	*log(Total Assets)*
AM (Asset Management)	*Operational Income / Total Assets*
OE (Operational Efficiency)	*Total Operating expenses / Interest Income*
CR (Credit Risk)	*Reserves for doubtful loans / Credit facilities*
DIG (digitalization):	
• Average mobile banking rank	*= AVG(mobile banking rank)*
• Amount of ATMs	*= log(Sum of the ATMs in Russia)*
• Amount of terminals	*= log(Sum of the terminals in Russia)*
• Percentage of electronic orders in transfers in total	*= Electronic orders in transfers in th. rubles / All transfers in thousands Rubles*
• Electronic payments for goods and services in thousands rubles	*= Sum of electronic payments for goods and services*
• IDI (ICT Development Index)	*= ready data taken*

Source: made by authors.

Below we want to discuss the Table 1 more detailed, giving some information about the factors and our opinion on why we took them into the model and how they can presumably affect the profitability of the banking sector.

1. **KRBR** (The key rate of the Central Bank of Russia) is the main instrument of monetary policy. The key rate of the Central Bank of the Russian Federation is the interest rate at which the Central Bank is ready to provide loans to commercial banks on credit for the next 7 days. In addition, the key rate is also the rate at which the Central Bank accepts funds for deposits from banks. We assumed that it could affect the profitability of banks, since a decrease in the key rate reduces the cost of loans, the profitability of deposits and securities. In fact, this means that the bank's assets generate less interest income, and the cost of raising funds becomes cheaper.

2. **GDP per capita** (Gross domestic product). *'The annual indicator characterizes the economy as a whole and its institutions. This indicator can act as a proxy variable for such invisible factors as the presence of business ethics, correct behavior of market participants, transparency of the banking system, etc. The higher this factor, the lower the costs incurred by the bank and the higher the profitability it receives from its operations'* (Kriebel, Debener, 2020).
3. **BS** (Bank Size). The size of a bank is determined by the amount of its total assets. In turn, the size of the bank affects profitability: on the one hand, when a bank gets larger, it gains access to new markets and increases profitability, and on the other, costs and risks increase as size increases. European Commission (1997), Berger and Humphrey (1997) and Vander Vennet (1998) believe that there is a diseconomy of scale for big banks.
4. **AM** (Asset Management) shows how effectively banks are managed, whether it helps to increase profits or, on the contrary, leads to losses.
5. **OE** (Operational Efficiency). Operating efficiency assessments provide insight into how effectively banks are managing their operating costs. Many banks pay great attention to the automation of business processes, which in some way can also be considered as the modernization of banking activities.
6. **CR** (Credit Risk) shows the level of financial stability and loan quality. It shows how the provision for loan losses relates to the total number of loans. The higher the indicator, the more risky loans the bank has, so the higher its risks of loss of profitability. At the same time, a high indicator does not always play a negative role: it can mean a high level of reserves to reduce risks and increase profitability. It is rather difficult to identify the relationship between the CP indicator and the profitability of banks.
7. **DIG** (digitalization) factor measures the level of technology development in the banking sector. We did not make it composite, hence it has several proxies.
    - Average mobile banking rank is the annual amount of points for mobile banking applications of 30 largest banks. The rating was made based on the responses of 3,270 people with experience of usage mobile banking applications and their degree of satisfaction. Each criterion in rating was assigned a weight reflecting the importance of the user task, as well as the importance of a particular function and quality of the interface in solving the user task. We suppose that the better these points are the better is the banking performance in general.

- Amount of ATMs is the average quarterly amount of ATMs in Russia. As demonstrated in the previous chapter, the number of ATMs first grew and then, after a peak in 2014-2015, began to decline sharply. We associate this with a new stage of digitalization, when ATMs are getting replaced by payment terminals, and the volume of cash in circulation has greatly decreased.
- Amount of terminals is also average and quarterly. The more terminals exist and the more payments are done by non-cash, the more digital economy is.
- Percentage of electronic orders in transfers in total shows how much people prefer to transfer money electronically.
- Electronic payments for goods and services in thousands rubles demonstrate the percentage of purchases made using terminals or in online platforms.
- IDI (ICT Development Index) is a composite index of measuring development of ICT between countries and over time. The index was created by ITU, and was explained more detailed in the Chapter 2. As it measures the development and potential for digital economy, it may be interesting to follow the relationship between the index and profit indicators of the banking sector.

In order to improve the accuracy of the study, we normalized those data that have a large variation, namely: GDP per capita, BS, Amount of ATMs and Amount of terminals.

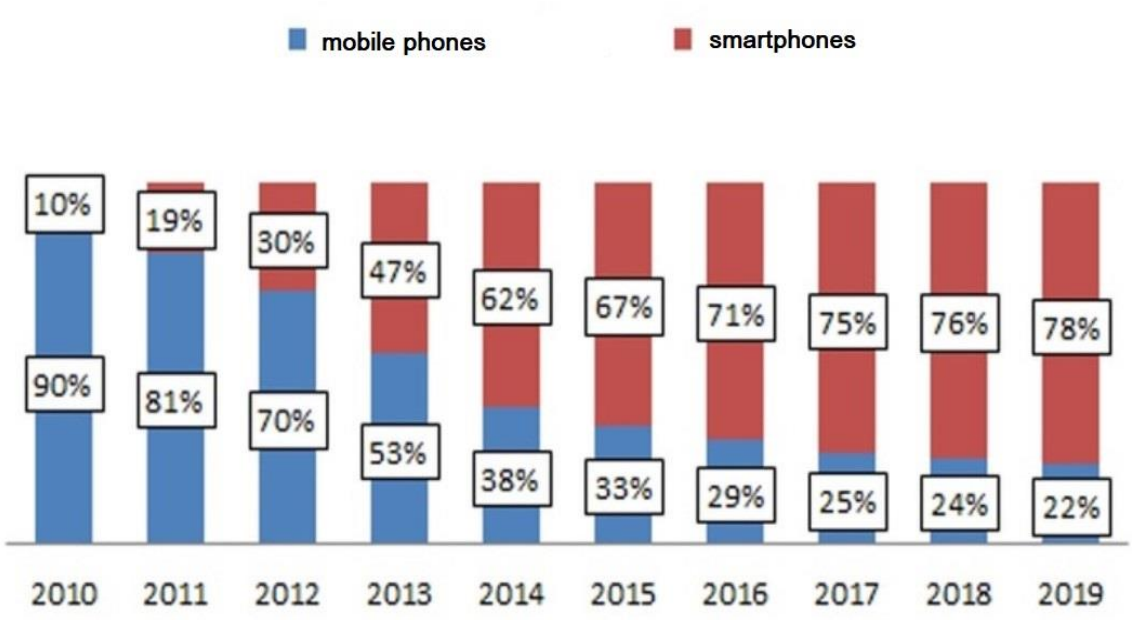
After we have talked about the importance of each specific factor and how it is calculated, we want to mention the data sources that we used for building them.

4.2. Data Sampling

Our work analyzes the banking sector in general. We did not make a sample of banks, but took aggregate data for the entire banking sector. The sample period is 2012-2020. This is due to the fact that it was during this period that the formation of the digital era in Russia took place. The 90s hit hard on the economy and political stability of the country, therefore the 2000s are considered the years of ‘recovery’, at that time high technologies were not a priority topic. In the early 2010’s, along with the rapid development of the Internet, as well as the markets for smartphones and other portable equipment, ‘high-tech banking’ found its consumer, sponsor and developer. On the Figure 33 we can see the shares of mobile phones and smartphones which were sold in

Russia during 2010 and 2019. Smartphones dominate the market by the end of the 2010s. In 2012-2015 the majority of Russians changed their usual phones to smartphones, and this has led to an increase in the popularity of applications for smartphones, which led to the fact that more and more companies, including banks, began to invest in them. In Russia, the starting point of digital banking is the creation of Sbertech in 2011, a subsidiary of Sberbank (the largest bank in Russia), which works only on digital tasks: develops a mobile application and an online bank.

Figure 33:
The shares of mobile phones users vs smartphones users in Russia, 2010-2019



Source: MVideo&Eldorado Group (2019).

We would like to show data sources for our factors, and put them in a table for convenience reason. Since data for many factors were taken from one report, we combined the 'source' fields.

Table 3: Variables of the regression model and their sources	
Variable	**Source**
ROA	Monthly overview of the banking sector of the Russian Federation (internet version), made by Central bank of Russia (2012-2020) **URL:**
ROE	
GDP per capita (annual) *	
BS (Bank Size)	

AM (Asset Management)	https://cbr.ru/statistics/bank_sector/review/
OE (Operational Efficiency)	
CR (Credit Risk)	
KRBR (The key rate of the Central Bank of Russia)	Data provided by the Central bank of Russia (2020a) on the official website **URL:** https://www.cbr.ru/hd_base/KeyRate/
DIG (digitalization):	
• Average mobile banking rank	Annual report of Mobile Banking application Index made by Markswebb agency **URL:**https://markswebb.ru/report/mobile-banking-rank/
• Amount of ATMs	National payment system statistics. Quarterly data provided by the Central Bank of the Russian Federation **URL:** https://cbr.ru/statistics/nps/psrf/
• Amount of terminals	
• Percentage of electronic orders in transfers in total	
• Electronic payments for goods and services in thousands rubles	
• IDI (ICT Development Index)	Annual Index which is calculated by ITU, the United Nations specialized agency for information and communication technologies **URL:** https://www.itu.int/en/ITU-D/Statistics/

Source: made by authors.

We would like to mention that while collecting the data we faced several limitations:

1) The index of the key rate of the Central Bank of Russia was created in 2013. Before that time the Central Bank used the Refinancing rate – 'the amount of interest on an annualized basis payable to the Central Bank of Russia for loans that the central bank has provided to credit institutions'. (Garant 2020) Since January 1, 2016, the value of the Refinancing Rate is equal to the value of the Key

Rate set by the Central Bank. Due to the lack of data on the key rate for 2012, it was necessary to aggregate the key rate data, which led to a deterioration in data quality.

2) While collecting data for factors AM (Asset Management) and OE (Operational Efficiency) from the Monthly overview of the banking sector of the Russian Federation, we faced the problem of the significant change in reporting. During the period 2012-2020 some of the indicators appear and disappear in reports, which make difficult calculating Operational Income and Interest Income, which could affect the factors.

3) IDI (ICT Development Index) and GDP are calculated once a year, so the impact on monthly profitability may also not be very pronounced due to the discrepancy in the granularity of the data.

4.3. Model building and quality checking

The following regression models are estimated for ROA and ROE, through the R studio software. With this model, we want to measure the impact of digitalization on banking performance.

The first model we have created is:

$$ROA = \alpha_0 + \beta_1 * KRBR + \beta_2 * logGDPpc + \beta_3 * logBS + \beta_4 * AM + \beta_5 * OE + \beta_6 * CR + \beta_7 * DIG(EO) + \beta_8 * DIG(MR) + \beta_9 * logDIG(EP) + \beta_{10} * logDIG(ATM) + \beta_{11} * logDIG(TER) + \beta_{12} * DIG(IDI) + u$$

The second model is:

$$ROE = \alpha_0 + \beta_1 * KRBR + \beta_2 * logGDPpc + \beta_3 * logBS + \beta_4 * AM + \beta_5 * OE + \beta_6 * CR + \beta_7 * DIG(EO) + \beta_8 * DIG(MR) + \beta_9 * logDIG(EP) + \beta_{10} * logDIG(ATM) + \beta_{11} * logDIG(TER) + \beta_{12} * DIG(IDI) + u$$

Where β_N, (N=1-12) are coefficient of the regression model. ROA and ROE are dependent variables.

DIG parameters are 6 proxies which we have chosen for measuring the Digitalization factor:

- Percentage of electronic orders in transfers in total
- Average mobile banking rank

- Electronic payments for goods and services in thousands rubles
- Amount of ATMs
- Amount of terminals
- IDI (ICT Development Index).

In order to understand that the model is working correctly and the data is selected correctly, we have to do several tests and check a couple of basic assumptions. According to Woolridge (2013, p. 83), there are 4 Multiple Linear Regression (MLR) assumptions, which make it unbiased for the population parameters. We will discuss them all to be sure that our model correctly plays the role that we assigned to it.

The first MLR assumption is '*model should be linear in parameters'* (Woolridge 2013, p. 83). It means that parameters β_1, β_2, … β_n should be linear, not logged, squared etc. This criteria is met in our model, it means that we can go further.

The second MLR assumption is *random sampling*. It means that observations should be randomly drawn. It is true for our model: the second criteria is met as well.

The third assumption is *no perfect collinearity*. '*If an independent variable is an exact linear combination of the other independent variables, then we say the model suffers from perfect collinearity, and it cannot be estimated by Ordinary Least Squared'* (Woolridge 2013, p. 84). The best way to check it is to check the **correlation**. Correlation coefficient is '*a natural measure of the association between two random variables'* (Woolridge 2013, p. 34). We used Pearson correlation coefficient, which varies from -1 to +1. The closer the coefficient to 1, the stronger correlation is, and vice versa: the closer the coefficient to 0, the weaker it is. +-1 means the perfect correlation, 0 means that there is absolutely no linear dependency between two variables. *'Positive correlation means that both variables change in the same direction, negative correlation means that they change in the opposite direction'* (Woolridge 2013, p. 84). According to Woolridge (2013, p. 84), independent variables in the model can be correlated, but they cannot be perfectly correlated. Below the correlation tables for both models are demonstrated (Figure 34, Figure 35).

According to both tables, there is no perfect correlation between variables, so independent variables are not exact linear combination of the other independent variables (Woolridge 2013, p. 84).

Figure 34:
The correlation between the variables in the regression model 1 with ROA as dependent variable

	(Intercept)	KRBR	gdpper	BS	AM
(Intercept)	1.000000000	-0.27889483	-0.48943009	-0.43674352	-0.008626525
KRBR	-0.278894832	1.00000000	0.48393000	-0.26915545	-0.028656225
gdpper	-0.489430087	0.48393000	1.00000000	0.40828782	-0.008964640
BS	-0.436743520	-0.26915545	0.40828782	1.00000000	0.080348697
AM	-0.008626525	-0.02865622	-0.00896464	0.08034870	1.000000000
OE	0.018852229	0.25343306	0.36653791	-0.34640843	-0.133238607
CR	-0.801857242	0.22301376	0.35471038	0.25168329	-0.019630468
EO	-0.290022341	0.32910493	0.15586834	-0.11133840	0.130488504
MR	0.092413176	-0.24147029	-0.42832101	-0.06346451	-0.011382229
EP	0.462946058	0.12409912	-0.14886540	-0.37711779	-0.081545951
ATM	-0.686791645	0.23164803	-0.06757672	-0.16197178	-0.068852197
TER	-0.075804225	0.19732968	-0.18376765	-0.40728778	0.058291597
IDI	0.619721774	-0.20668722	0.10294683	-0.18991322	-0.083135541

	OE	CR	EO	MR	EP
(Intercept)	0.01885223	-0.80185724	-0.29002234	0.09241318	0.462946058
KRBR	0.25343306	0.22301376	0.32910493	-0.24147029	0.124099121
gdpper	0.36653791	0.35471038	0.15586834	-0.42832101	-0.148865395
BS	-0.34640843	0.25168329	-0.11133840	-0.06346451	-0.377117786
AM	-0.13323861	-0.01963047	0.13048850	-0.01138223	-0.081545951
OE	1.00000000	0.19388199	0.26055200	0.10486984	0.412935147
CR	0.19388199	1.00000000	0.60131439	0.18366533	-0.258029947
EO	0.26055200	0.60131439	1.00000000	0.18629890	-0.090097997
MR	0.10486984	0.18366533	0.18629890	1.00000000	0.161687769
EP	0.41293515	-0.25802995	-0.09009800	0.16168777	1.000000000
ATM	0.16799825	0.75319536	0.42211065	0.27684006	0.007972255
TER	-0.27427496	-0.17389683	-0.04988346	-0.35280439	-0.581040225
IDI	0.30608300	-0.47565018	-0.30049943	0.02747683	0.306974028

	ATM	TER	IDI
(Intercept)	-0.686791645	-0.07580422	0.61972177
KRBR	0.231648034	0.19732968	-0.20668722
gdpper	-0.067576725	-0.18376765	0.10294683
BS	-0.161971778	-0.40728778	-0.18991322
AM	-0.068852197	0.05829160	-0.08313554
OE	0.167998247	-0.27427496	0.30608300
CR	0.753195356	-0.17389683	-0.47565018
EO	0.422110652	-0.04988346	-0.30049943
MR	0.276840059	-0.35280439	0.02747683
EP	0.007972255	-0.58104022	0.30697403
ATM	1.000000000	0.03108072	-0.60813318
TER	0.031080720	1.00000000	-0.29765009
IDI	-0.608133180	-0.29765009	1.00000000

Source: made by authors, using R Studio.

Figure 35:
The correlation between the variables in the regression model 2 with ROE as dependent variable

	(Intercept)	KRBR	gdpper	BS	AM
(Intercept)	1.0000000	-0.19639429	-0.708675153	-0.41406128	0.054844804
KRBR	-0.1963943	1.00000000	0.519115594	-0.32105745	-0.047013677
gdpper	-0.7086752	0.51911559	1.000000000	0.43809708	-0.000409687
BS	-0.4140613	-0.32105745	0.438097078	1.00000000	0.065985301
AM	0.0548448	-0.04701368	-0.000409687	0.06598530	1.000000000
OE	-0.2286464	0.34000439	0.353797779	-0.30842585	-0.113619883
CR	-0.7345288	0.14489549	0.461365820	0.18682976	-0.067504694
EO	-0.1386634	0.28611149	0.196902039	-0.17984077	0.111003171
MR	0.0960902	-0.24108600	-0.433616371	-0.05934838	-0.009132980
EP	0.3651052	0.20141030	-0.190635660	-0.34120315	-0.059072251
ATM	-0.4974461	0.13641757	-0.006295889	-0.35600283	-0.150943808
TER	0.1450198	0.14539654	-0.161252192	-0.49484165	0.035261033

	OE	CR	EO	MR	EP
(Intercept)	-0.2286464	-0.73452877	-0.138663389	0.09609020	0.365105200
KRBR	0.3400044	0.14489549	0.286111493	-0.24108600	0.201410301
gdpper	0.3537978	0.46136582	0.196902039	-0.43361637	-0.190635660
BS	-0.3084259	0.18682976	-0.179840765	-0.05934838	-0.341203153
AM	-0.1136199	-0.06750469	0.111003171	-0.00913298	-0.059072251
OE	1.0000000	0.40537833	0.388246478	0.10136092	0.352054661
CR	0.4053783	1.00000000	0.546356308	0.22373951	-0.133806166
EO	0.3882465	0.54635631	1.000000000	0.20406042	0.002365815
MR	0.1013609	0.22373951	0.204060416	1.00000000	0.161088682
EP	0.3520547	-0.13380617	0.002365815	0.16108868	1.000000000
ATM	0.4686002	0.66439477	0.316143940	0.36992637	0.257645991
TER	-0.2015385	-0.37566951	-0.153013955	-0.36112401	-0.538938421

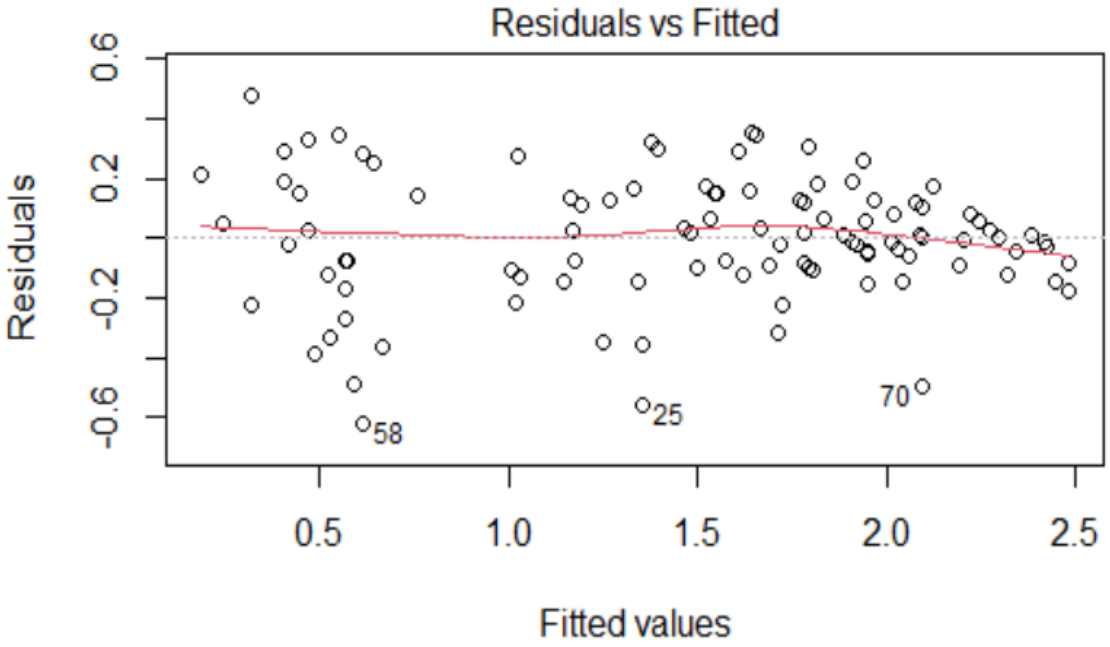
	ATM	TER
(Intercept)	-0.497446053	0.14501979
KRBR	0.136417568	0.14539654
gdpper	-0.006295889	-0.16125219
BS	-0.356002831	-0.49484165
AM	-0.150943808	0.03526103
OE	0.468600211	-0.20153850
CR	0.664394772	-0.37566951
EO	0.316143940	-0.15301395
MR	0.369926365	-0.36112401
EP	0.257645991	-0.53893842
ATM	1.000000000	-0.19783504
TER	-0.197835044	1.00000000

Source: made by authors, using R Studio.

As we can see, there is no perfect correlation between parameters, it means that the third assumption is met.

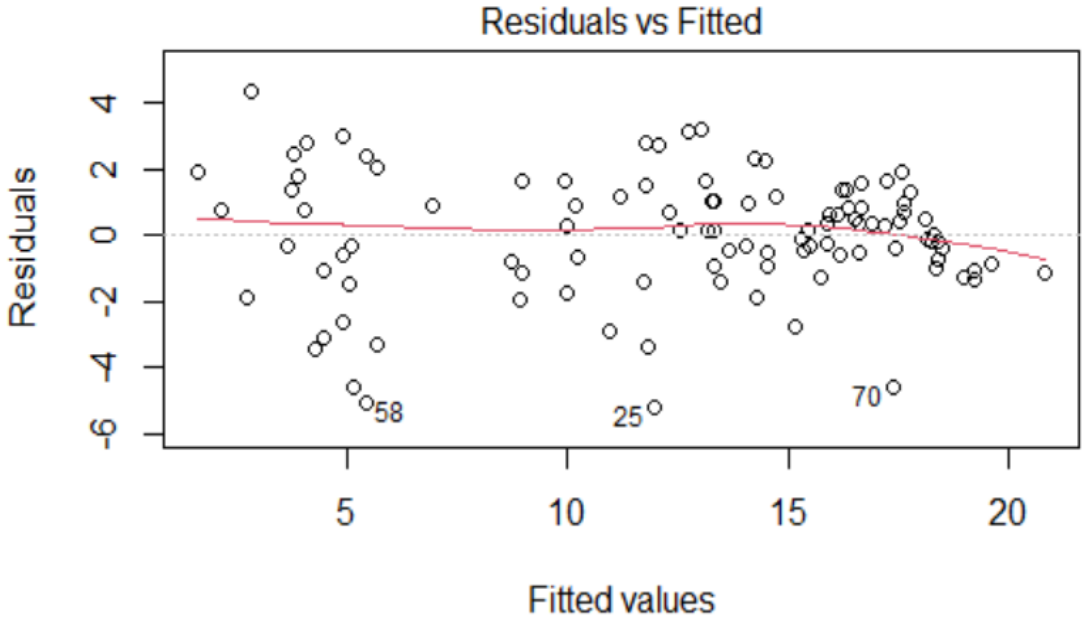
The fourth MLR assumption is *Zero conditional mean.* There are several ways to check it, but the easiest one is to check it we need to plot the residuals of both models and to check visually if the mean is close to 0. On the Figure 36 and Figure 37 the results of the plotting are demonstrated. As we can see, the error is about 0: the fourth assumption is met.

Figure 36:
The residuals plot which demonstrates the assumption of 'Zero conditional mean' for the regression model 1 with ROA as dependent variable



Source: made by authors, using R Studio.

Figure 37:
The residuals plot which demonstrates the assumption of 'Zero conditional mean' for the regression model 2 with ROE as dependent variable



Source: made by authors, using R Studio.

The MLR 1-4 assumptions make the model unbiased. Now to check is our model is BLUE (Best Linear Unbiased Estimator), we need to check the MLR 5 –

heteroscedasticity and autocorrelation, both are very important issues for regression analysis.

According to Gauss-Markov assumption, '*Conditional on X, the variance of* u_t *is the same for all t:* $Var(u_t \mid X) = Var(u_t) = \sigma^2$, $t = 1, 2, \ldots, n$' (Woolridge 2013, p. 80). That means that Var(u) cannot depend on X, u_t and X have to be independent and Var has to remain constant all the time. When we fail to follow this statement, it means that the errors are heteroscedastic. Verification of the fulfillment of the requirement of homoscedasticity of random residuals can be performed visually, based on the residual graph, or using special criteria. The tests that allow revealing the presence of heteroscedasticity of random residuals include the Goldfeld - Quandt, Park, Glazer, White, Breusch - Pagan tests, Spearman's rank correlation, etc. We have chosen Breusch - Pagan tests.

Breusch - Pagan tests has two hypotheses to analyze:

H_0: the model contains homoscedasticity of random residuals;

H_1: the model contains heteroscedasticity of random residuals.

The test gave us the following results for two regression models:

Figure 38:
Breusch-Pagan test for the regression model 1 with ROA as dependent variable

```
        studentized Breusch-Pagan test

data:  reg1
BP = 25.354, df = 12, p-value = 0.01323
```

Source: made by authors, using R Studio.

Figure 39:
Breusch-Pagan test for the regression model 2 with ROE as dependent variable

```
        studentized Breusch-Pagan test

data:  reg2
BP = 23.405, df = 11, p-value = 0.01549
```

Source: made by authors, using R Studio.

As our critical value for n – k – 1 (90) degrees of freedom is 1.658, we reject we H_0 at 5% significant level for both models (Figures 38 and 39). It means that our model has heteroscedasticity of random residuals: it fits the fourth criteria.

Now we want to talk about autocorrelation. According to Woolridge, one of the assumptions says that *'Conditional on X, the errors in two different time periods are uncorrelated'* (2013, p. 381). If it is false, the model has autocorrelation or serial correlation. Series correlation exists in scientific research for which the order of observations is important. Therefore, most often autocorrelation occurs on a set of data described by time series. Essentially, it follows from the correlation of data series that the stochastic error term for one time period symmetrically depends on the stochastic error term for another time period. In order to check our model for autocorrelation, we will run the Durbin-Watson test.

Figures 40 and 41 give us the results of Durbin-Watson test. We work with the two hypotheses:

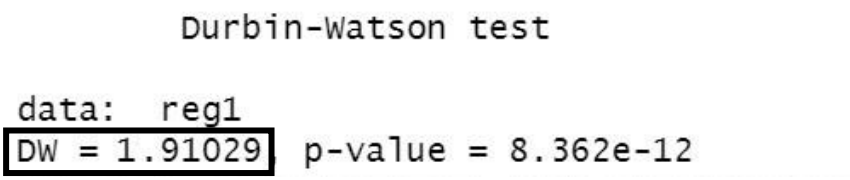
H_0: no first order autocorrelation;

H_1: first order correlation exists.

For both models we have the critical values of $d_1 = 1.335$ and $d_2 = 1.765$. DW coefficient can range from 0 to 4. If our DW value is less than d_1, it means that we have positive first order autocorrelation, if DW is between d_1 and d_2; it means that we cannot reject the H_0 and we should check the model using a more powerful criteria. If DW is bigger than d_2 but smaller than 2 is means that we can reject the H_0 and the model is considered as adequate according to this criteria. If DW is bigger than 2, it means that we have negative autocorrelation of residuals. In this case, the calculated value of the criterion must be converted according to the formula: $DW_1 = 4 - DW$.

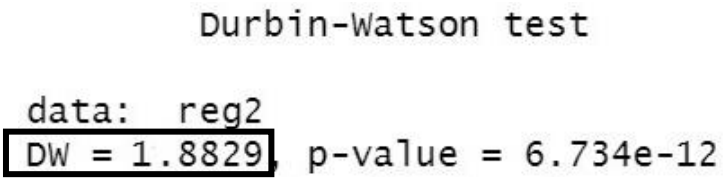
Now we want to look at the results. Figure 40 has a DW value which is greater than d_2, but smaller than 2. It means that for the first model we can reject the H_0 at the 0.05 significance level. The same situation we can observe on the Figure 41: DW value which is greater than d_2, but smaller than 2. Again, we reject the H_0 about autocorrelation of residuals at the 0.05 significance level. As our p-values in both cases are very significant, we can say that we do not need further tests to check the models deeper.

Figure 40:
Durbin-Watson test for the regression model 1 with ROA as dependent variable



Source: made by authors, using R Studio.

Figure 41:
Durbin-Watson test for the regression model 2 with ROE as dependent variable



Source: made by authors, using R Studio.

According to our data checks, the model is adequate and we can use the data for further analysis.

Now that we have talked about the factors which will be included in our model, what they will measure and where we got the data from, and after demonstrating the model, it is time to show the results we have got at and discuss them.

4.4. Results analysis

In this part of the work, we will talk about the results we obtained.

Now we would like to talk about confidence interval for the regression coefficients. Confidence intervals sometimes are called interval estimates due to the fact that they give us a range of values for the population parameter which are more likely to appear, but not just a point estimate. The meaning of a confidence level is as following: '*If random samples were obtained over and over again, with bj computed each time, then the (unknown) population value bj would lie in the interval (bj) for (for instance) 95% of the samples*' (Woolridge 2013, p. 138). The standard level of confidence which is applied to most of the regression packages nowadays is 95%, in case we do not specify it, it remains 95%. Below we can see the results:

Figure 42:
Confidence Intervals (CI) for the regression model 1 with ROA as dependent variable

	2.5 %	97.5 %
(Intercept)	64.93243749	122.730077228
KRBR	-0.05680812	0.035351566
gdpper	0.16115841	2.151976879
BS	-15.01133619	-5.259628389
AM	-3.80604038	10.547224214
OE	-0.03976200	0.005717674
CR	-1.04643522	-0.619926385
EO	-3.66801741	1.720710022
MR	-0.02795495	0.005414083
EP	-0.27081123	1.270354711
ATM	-9.76828731	-5.664376330
TER	1.65531309	4.272262547
IDI	-0.48596639	1.165493854

Source: made by authors, using R Studio.

Figure 43:
Confidence Intervals (CI) for the regression model 2 with ROE as dependent variable

	2.5 %	97.5 %
(Intercept)	535.4567986	932.51287028
KRBR	-0.3961060	0.39317445
gdpper	-0.2676199	17.06598297
BS	-126.0580865	-42.25212850
AM	-31.7541818	93.44902748
OE	-0.3519583	0.02703131
CR	-8.6650075	-5.38102302
EO	-29.0159622	15.97301643
MR	-0.2240232	0.06795500
EP	-1.8388762	11.00004211
ATM	-75.4823563	-46.96567501
TER	16.2429373	38.11157344

Source: made by authors, using R Studio.

Figures 42 and 43 show that in 95% cases our parameters' values are within the presented intervals. There are significant differences in confidence level between two models, although all factors are the same. But the dependent variables, ROA and ROE,

are different, and ROE is quite bigger, so it is responsible for differences in CI. These two tables give us an understanding of how the factors vary and what to expect from them.

Moving to the regression results analysis, we should clarify some moments. As ROA and ROE, our proxies for banking performance, are measured in percentage, the impact of the factors will result an increase/decrease in percentage. Additionaly, according to our data description in the previous subchapter, some of the factors are logged, while others are not. It was done in order to normalize the data. The values of the indicators of some factors do not differ greatly among themselves, while for others (for example, GDP per capita or the number of ATMs) they differ significantly. This complicates the regression analysis; hence we decided to normalize the data using logarithms. Now we would like to look at the results.

The Figure 44 contains the results of the regression. Below, we will explain them using the methods, described in online information resource Infocenter (Infocenter 2020). The first column contents the names of our factors which we have already showed. The second column is called 'Estimate' and it shows the coefficients of each factor. It is the most informative column for our research. All the coefficients' descriptions below should be considered on average.

First model Coefficients (Figure 44):

1) Since β_1 is negative, the Key Rate of the Central Bank of Russia has a negative impact on the bank performance. If KRBR increases by one unit (the rest of the x-variables remains the same, thus ceteris paribus, the same for the following factors), the ROA is absolutely decreased by 0.0137. As the ROA is in percentage it will effectively decrease by 0.0137%.
2) β_2 is positive, so logged GDP per capita has a positive impact on the bank performance. If log(GDPpc) increases by one percent, the performance will increase by approximately 0.0118%.
3) β_3 is negative, it means that logged Bank Size has a negative impact on the bank performance. When it increases by one percent, the performance will decrease by approximately 0.1%. The strong impact is explained by the fact that the Bank Size is a logged variable that is formed from the bank's assets. In the process of data normalization, the values decreased by about 16 thousand times, it means that a decrease in it by 1 unit is commensurate with 16,000 billion rubles.
4) Since β_4 is positive, Asset Management has a positive impact on the bank performance. If AM increases by one unit, the performance will absolutely

increase by 3.335. As the performance is measured in percentages, it will effectively increase by 3.335%. The impact is very strong.

5) β_5 is negative, it means that Operational Efficiency has a negative impact on the bank performance. If OE increases by one unit, the performance will decrease absolutely by 0.016. As the performance is measured in percentages, it will effectively decrease by 0.016%.
6) β_6 has a negative sign, it means that if Credit Risk increases by one point, the bank performance decreases absolutely on 0.84, but as ROA is measured in percentages, it will effectively decrease by 0.84%. This is because the Credit Risk factor refers to the amount of provisions for possible losses. That is, the greater its value, the more the bank expects to incur losses, the more risky assets it has.
7) β_7 is negative. According to the model, if percentage of Electronic Orders increases by one unit (as it is measured in percentages, meaning that it increase by one percent), the bank performance will decrease absolutely by 0.94, and effectively by 0.94%, which is relatively big impact.
8) β_8 is negative, it means that Mobile Ranking increases by one unit, the ROA will decrease absolutely by 0.009. As the performance is measured in percentages, it will effectively decrease by 0.009%.
9) Since β_9 is positive, the logged amount of Electronic Payments has a positive effect on the bank performance. When EP increases by 1 unit, ROA increases by approximately 0.005%.
10) β_{10} is negative, it means that one percent increase of logged amount of ATMs leads to 0.08% decrease in bank performance.
11) Since β_{11} is positive, the logged amount of Terminals has a positive impact on ROA. It means that 1% increase of TER leads to 0.415% increase of the bank performance.
12) β_{12} is positive. According to the model, if IDI increases by one unit, the ROA will increase absolutely by 0.229. But as IDI is measured in percentages, the performance will increase effectively by 0.229%.

Figure 44:
Regression results of the model 1 with ROA as dependent variable

```
Residuals:
     Min       1Q   Median       3Q      Max
-0.63204 -0.10243  0.00411  0.13986  0.48538

Coefficients:
             Estimate Std. Error t value Pr(>|t|)
(Intercept) 28.609564  21.966510   1.302 0.196097
KRBR        -0.013719   0.023302  -0.589 0.557508
gdpper       1.182905   0.505002   2.342 0.021367 *
BS         -10.009403   2.480772  -4.035 0.000114 ***
AM           3.335015   3.643969   0.915 0.362524
OE          -0.015824   0.011506  -1.375 0.172467
CR          -0.839307   0.108686  -7.722 1.52e-11 ***
EO          -0.940465   1.367828  -0.688 0.493498
MR          -0.009132   0.008347  -1.094 0.276837
EP           0.499440   0.396858   1.258 0.211471
ATM         -7.996926   1.041863  -7.676 1.89e-11 ***
TER         41.508039   9.690202   4.284 4.60e-05 ***
IDI          0.299534   0.423828   0.707 0.481557
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 0.2241 on 90 degrees of freedom
Multiple R-squared:  0.9039,    Adjusted R-squared:  0.8911
F-statistic: 70.57 on 12 and 90 DF,  p-value: < 2.2e-16
```

Source: made by authors, using R Studio.

The third column shows the standard errors of the coefficients. This column can be used to build the confidence intervals, which we demonstrated before. '*The standard error is also used to test whether the parameter is significantly different from 0. If a coefficient is significantly different from 0, then it has impact on the dependent variable'* (Infocenter 2020). It should be compared with the second column – Estimate. The bigger coefficient is, the bigger standard error may appear in the model.

The fourth column is t-value. *'The t-value is the ratio of the regression coefficient β to its standard error (t = coefficient ÷ standard error)'* (Infocenter 2020). It tests the hypothesis that population regression is equal to zero. In case it is higher than zero, the coefficient has an impact on the dependent variable. The t-value is used to calculate the p-value.

The fifth column p-value shows if the independent variable has predictive capability which is statistically significant or not. It indicates the probability that the

coefficient will be attributed to random variation. Lower probability means higher significance of the coefficient. For example, a significance level of gdpper is 0.021367 and it indicates that there is a 0.2% chance that the coefficient is equal to zero = it is insignificant. In other words, we can be 99.8% sure that it is significant. According to the results table, not all factors are equally significant. Bank Size, Credit Risk, ATMs and Terminals are the most significant. Gdpper is also relatively significant. ATMs and terminals are our proxies for measuring digitalization. Therefore, we can say that digitalization affects the profitability of the banking sector in terms of ROA. The larger the number of terminals, the higher the profitability (since the process of digitalization is associated with an increase in their number, as we showed in Chapter 3), at the same time, digitalization leads to the process of a decrease in the number of ATMs, and therefore a decrease in their number leads to an increase in profitability of banking sector.

The Figure 45 which demonstrates the results of the second regression, as the previous one, consists of five columns. The first column is the name of the coefficients. Below we will explain the results in the second column called 'Estimate' more detailed. All the coefficients' descriptions below should be considered on average.

Second model Coefficients (Figure 45):

1) β_1 is negative. It means that the Key Rate of the Central Bank of Russia has a negative impact on the bank performance. If KRBR increases by one unit (the rest of the x-variables remains the same, thus ceteris paribus), the ROA is absolutely decreased by 0.046. As the ROA is in percentage it will effectively decrease by 0.046%.
2) Since β_2 is positive, the logged GDP has a positive impact on the bank performance. If GDP increases by one percent, ROA increases by 0.088%.
3) β_3 is negative, it means that logged Bank Size has a negative impact on the bank performance. When it increases by one percent, the performance will decrease by approximately 0.85%. The strong impact is explained the same way as in the previous model, by the fact that the Bank Size is a logged variable that is formed from the bank's assets. Due to normalization, the values decreased significantly, so a decrease in it by 1 unit has such a large impact.
4) Since β_4 is positive, Asset Management has a positive impact on the bank performance. If AM increases by one unit, the performance will absolutely

increase by 29.38. As the performance is measured in percentages, it will effectively increase by 29.38%. The impact is very strong.

5) β_5 is negative, it means that Operational Efficiency has a negative impact on the bank performance. If OE increases by one unit, the performance will decrease absolutely by 0.0138. As the performance is measured in percentages, it will effectively decrease by 0.0138%.
6) β_6 has a negative sign. It means that if Credit Risk increases by one point, the bank performance decreases absolutely on 7.27, but as ROA is measured in percentages, it will effectively decrease by 7.27%. This is because the Credit Risk factor refers to the amount of provisions for possible losses. That is, the greater its value, the more the bank expects to incur losses, the more risky assets it has.
7) β_7 is negative. According to the model, if percentage of Electronic Orders increases by one unit (as it is measured in percentages, meaning that it increase by one percent), the bank performance will decrease absolutely by 7.78, and effectively by 7.78%, which is relatively big impact.
8) β_8 is negative, it means that Mobile Ranking increases by one unit, the ROA will decrease absolutely by 0.058. As the performance is measured in percentages, it will effectively decrease by 0.058%.
9) Since β_9 is positive, the logged amount of Electronic Payments has a positive effect on the bank performance. When EP increases by 1 unit, ROA increases by approximately 0.05%.
10) β_{10} is negative, it means that one percent increase of logged amount of ATMs leads to 0.66% decrease in bank performance.
11) Since β_{11} is positive, the logged amount of Terminals has a positive impact on ROA. It means that 1% increase of TER leads to 3.701% increase of the bank performance. The strong impact is explained by the fact that we normalized the data using log, so the impact of 1% increase became higher.
12) β_{12} is positive. According to the model, if IDI increases by one unit, the ROA will increase absolutely by 1.228. But as IDI is measured in percentages, the performance will increase effectively by 1.228%.

Figure 45:
Regression results of the model 2 with ROE as dependent variable

```
Residuals:
    Min      1Q  Median      3Q     Max
-5.1557 -0.9509  0.0967  1.1889  4.4223

Coefficients:
             Estimate Std. Error t value Pr(>|t|)
(Intercept) 186.82504  193.21972   0.967 0.336183
KRBR         -0.04644    0.20497  -0.227 0.821260
gdpper        8.83109    4.44205   1.988 0.049843 *
BS          -84.80866   21.82113  -3.887 0.000194 ***
AM           29.38337   32.05273   0.917 0.361740
OE           -0.13840    0.10121  -1.367 0.174889
CR           -7.27253    0.95602  -7.607 2.61e-11 ***
EO           -7.78125   12.03156  -0.647 0.519449
MR           -0.05808    0.07342  -0.791 0.430978
EP            5.03253    3.49080   1.442 0.152870
ATM         -66.12398    9.16434  -7.215 1.63e-10 ***
TER         370.12330   85.23603   4.342 3.69e-05 ***
IDI           1.22819    3.72803   0.329 0.742584
---
Signif. codes:  0 ‘***’ 0.001 ‘**’ 0.01 ‘*’ 0.05 ‘.’ 0.1 ‘ ’ 1

Residual standard error: 1.971 on 90 degrees of freedom
Multiple R-squared:  0.8866,    Adjusted R-squared:  0.8715
F-statistic: 58.66 on 12 and 90 DF,  p-value: < 2.2e-16
```

Source: made by authors, using R Studio.

We have already discussed the third and the fourth columns related to the previous model.

The fifth column is p-value According to the results, Bank Size, Credit Risk, ATMs and Terminals are the most significant. Gdpper is relatively significant. As in the previous model, we can confirm that digitalization affects the profitability of the banking sector in terms of ROE. The further digitalization goes (the number of payment terminals grows and the number of ATMs decreases), the more the profitability of the banking sector increases.

Now we would like to discuss F-statistic. If the F-statistic is greater than the critical value, we can reject the null hypothesis about the insignificance of the model that at the 0.05 significance level. For the first model the critical values were between 2.09 and 1.94 and the F-value is 70.57, the p-value is very low, which means that it is significant. For the second model, the critical value falls somewhere in between 1.94 and 1.75 and the F-value is 58.66, the p-value is also very low, which shows its

significance. Since the F-statistics were greater in both cases, we reject the null hypothesis at a 5% level.

To check the significance of the parameters which are not significant in regressions, we decided to run the F-test for multiple linear restrictions. In both cases, according to the Figure 46 and the Figure 47, the F-statistic resulted insignificant (highlighted in the boxes), which indicates that none of the coefficients in the model is different from zero, it means that they have almost no impact on the banking performance. According to our limitations from the subchapter 4.2, it can be related to difficulties with data collecting.

Figure 46:
F-test for the regression model 1 with ROA as dependent variable

```
Hypothesis:
KRBR = 0
AM = 0
OE = 0
EO = 0
MR = 0
EP = 0
IDI = 0

Model 1: restricted model
Model 2: ROA ~ KRBR + gdpper + BS + AM + OE + CR + EO + MR + EP +
 ATM +
    TER + IDI

  Res.Df    RSS Df Sum of Sq      F Pr(>F)
1     97 4.9850
2     90 4.4419  7   0.54315 1.5722 0.1539
```

Source: made by authors, using R Studio.

Figure 47:
F-test for the regression model 2 with ROE as dependent variable

```
Hypothesis:
KRBR = 0
AM = 0
OE = 0
EO = 0
MR = 0
EP = 0
IDI = 0

Model 1: restricted model
Model 2: ROE ~ KRBR + gdpper + BS + AM + OE + CR + EO + MR + EP +
 ATM +
    TER + IDI

  Res.Df    RSS Df Sum of Sq      F Pr(>F)
1     97 382.06
2     90 343.50  7     38.56 1.4433  0.198
```

Source: made by authors, using R Studio.

Next, we would like to test our sample using the Bootstrap method. The idea behind the bootstrap is to use the results of computation on samples as a 'fictitious population' in order to determine the sample distribution of a statistic. *'Bootstrapping is a statistical procedure that resamples a single dataset to create many simulated samples. This process allows for the calculation of standard errors, confidence intervals, and hypothesis testing'* (Forst 2020). In fact, a large number of 'phantom' samples, called bootstrap samples, are analyzed. It helps researchers to statistically evaluate models where the samples are small. Usually, several thousand samples are randomly generated; from this set we can find the bootstrap distribution of the statistics of interest. *'The benefit of more resamples, then, is to derive a better estimate of the sampling distribution'* (Peixeiro 2019). In our case we took 10000 bootstrap iterations. The reason is that the number of iterations depends on the number of observations (n) in each sample, in our case it is 104. According to Efron and Tibshirani (1993), the perfect number of iterations is n*n, which is about 10000. We made the same regression with 10000 random samples which were made out of our samples, and got the standard errors of the distributions which are demonstrated on the Figure 48. We have also checked that our bootstrap parameters are normally distributed, the results are shown in alphabetical order of parameters in Appendix 1.

Figure 48:
Standard errors of the distributions after bootstraping the regression 1 with ROA as dependent variable

(Intercept)	KRBR	gdpper	BS	AM	OE
15.45884053	0.02731482	0.57690730	2.57396212	3.39805540	0.01108423
CR	EO	MR	EP	ATM	TER
0.11751867	1.24698908	0.01135135	0.39565464	1.06611977	0.83889270
IDI					
0.37899558					

Source: made by authors, using R Studio.

We did the same with the second model, the results are shown here. The standard distributions of the errors are shown on the Figure 49. The numbers are larger because ROE is larger than ROA. The distribution of the parameters is also demonstrated in Appendix 2.

Figure 49:
Standard errors of the distributions after bootstraping the regression 2 with ROE as dependent variable

(Intercept)	KRBR	gdpper	BS	AM	OE
136.04490730	0.23522694	5.18231887	22.87247002	28.77313417	0.09757176
CR	EO	MR	EP	ATM	TER
1.04259620	11.10146380	0.10249938	3.38950238	9.46043538	7.30228467
IDI					
3.27740361					

Source: made by authors, using R Studio.

Looking at the both Figures 45 and 46, we can say that the model works properly, the errors are within the normal range, and the factors are normally distributed.

Summarizing all of the above, we can conclude that our model performs the function assigned to it to demonstrate the influence of factors on the profitability of banks. Our goal was to find out whether digitalization affects the profitability of banks, and based on the results of the regressions (Figures 44 and 45) we can conclude that the relationship exists. Since we took several proxies for the digitalization factor, based on the models, we can say that the number of terminals and ATMs has the greatest influence among all. Profitability and the number of terminals are positively correlated: with an increase in the number of terminals, profitability increases. At the current period of time, the number of ATMs has the opposite tendency - profitability grows with a decrease in the number of ATMs. The explanation to it is the fact that Russian banks have a trend towards a reduction in ATMs and physical offices, as we have already discussed in previous chapters. Another fact contributing to this result is the high level

technology adoption level among Russian people, which was demonstrated in the Chapter 3. As a result, the number of points of sale which are equipped with cashless payment terminals is continuously rising.

Chapter 5. Cyber threats as one of the main challenges of the Russian financial sector digitalization. (Samsonova, Voronina)

Fast development of digitalization inextricably linked with the raise of cyber crimes. As we saw in the Chapter 2, according to global trends, cyber risk is the most serious risk for the financial sector. The threat of it is so serious that it can turn all the advantages of digitalization into disadvantages. According to Figure 9, Russia is among the top countries in terms of the number of cyber attacks on banking institutions, but at the same time, according to Figure 11, Russia has a very high level of cyber security. This suggests that there is a daily struggle between the attacking and defending sides, which certainly leads to the dynamic development of cyber security in the country. That is why we would like to talk about cyber security in Russia and its problems in more detail.

In this chapter, we will first look at the current situation with cyber attacks in Russia. We will analyze the amount and dynamics of material damage to banks and people from cyber attacks. Then we will consider the different types of cyber attacks, talking in particular about social engineering, as it occupies a leading position among all attacks. Next, we turn to the motives and methods of attacks, and then move on to the main vulnerabilities in the internal networks of Banks in Russia. We conclude by looking at the cyber security level of mobile banking, which is also a factor in digitalization, and was considered as a factor in our model in Chapter 4. Secondly, we will talk about cyber security. We will discuss the role of the Central Bank of Russia in cyber risks regulation and then we will show and analyze legislative regulation related to cyber attacks in Russia at the international and local levels. We conclude with looking at the actual measures of protection from machine- and human-based vulnerabilities.

Banking companies tend to be the most exposed to cyber risks due to their specific features. They are dependent on highly interconnected networks, and most of their inner processes are automatized. The most vulnerable banking systems include payment and money transferring systems and internal networks. Once a hacker intervenes in a one of the banking process, he can immediately spread his influence on many other processes and even other banks.

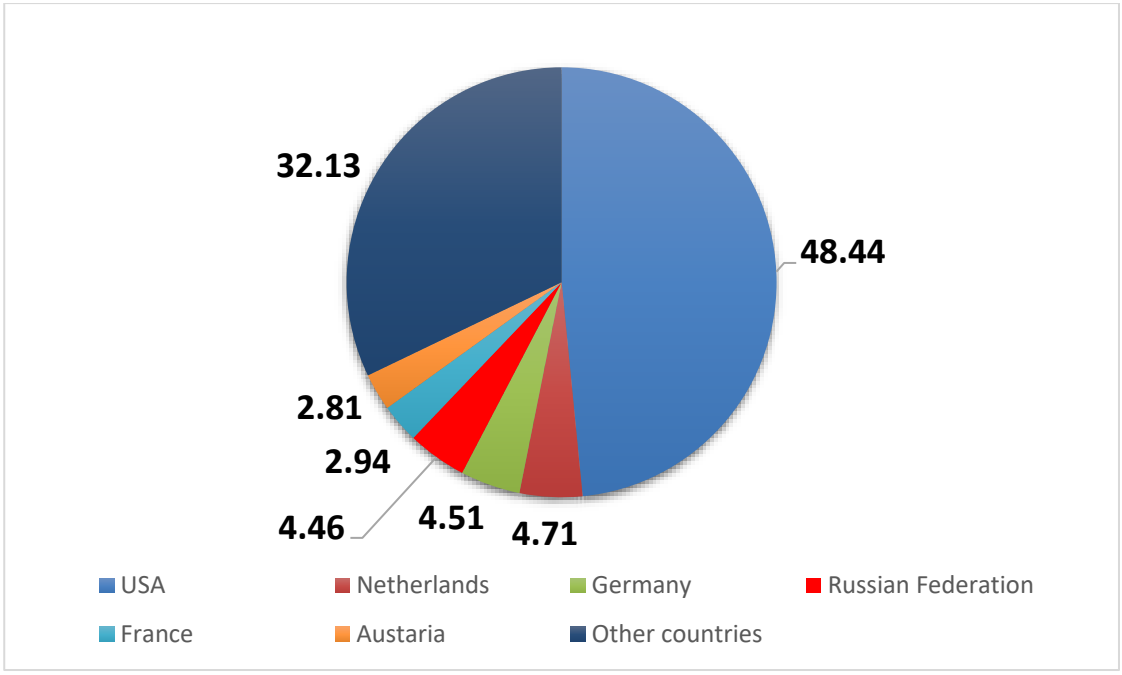
As we have discussed in previous chapters, cyber risks and cyber security are very hard to measure leaving alone the statistics for financial sector. However, in addition to

the metrics based on the amount of publications devoted to cyber risks, which we talked about in the second chapter, there are also more specific ways to build cyber risk ratings.

According to the Central Bank of Russia (2018a), in 2018, the Group-IB Threat Intelligence system detected and analyzed more than 1.9 million unique phishing (Internet fraud attack) links (Figure 50), which is 85% more than in 2017. More than 26% of them are in the financial sector. Most of the financial phishing attacks are related to US companies (48% of all attacks). However, Russia also accounts for a significant part of attacks (4.46%) and takes the fifth place in this rating. As we will see further, phishing and social engineering in general takes a big part of all cyber attacks in Russia.

Figure 50:

Phishing in the financial sector (top 6 countries)



Source: Central Bank of Russia (2018a).

Cyber attacks are one of the most dangerous threads of the modern banking sector. The damage is counted in millions, apart from losing customers' trust and good reputation. In Russia this problem has already attracted the attention of the regulator. "Protecting banks and their clients from cyberattacks is one of the key tasks of the Bank of Russia" (Rambler News 2017), said the head of the Central Bank Elvira Nabiullina.

5.1. Current situation

In this subchapter we would like to show the current situation of cyber risks in the Russian banking sector. We will talk about the amount and volume of cyber attacks on the Russian banking sector to draw the picture of the severity of the situation. We will try to reveal the trends that are present in the Russian banking cyber reality. Then we will show the methods, types and targets of the attacks. The importance of this chapter is that we will not only describe them, but also analyze the causes, prevalence and dynamics.

To get the data about the current state of cyber risks in Russian banking sector, we approached FinCERT reports. FinCERT stands for Financial Sector Computer Emergency Response Team, a special division of the Central Bank of Russia. The main task of the Center is to ensure information security of credit and financial institutions by mutual informing of financial market participants about the vulnerabilities, threats and risks they face, and about methods of preventing them. Some of the reports are only available for 2018 that is why we have to build some of our graphs only up to this date.

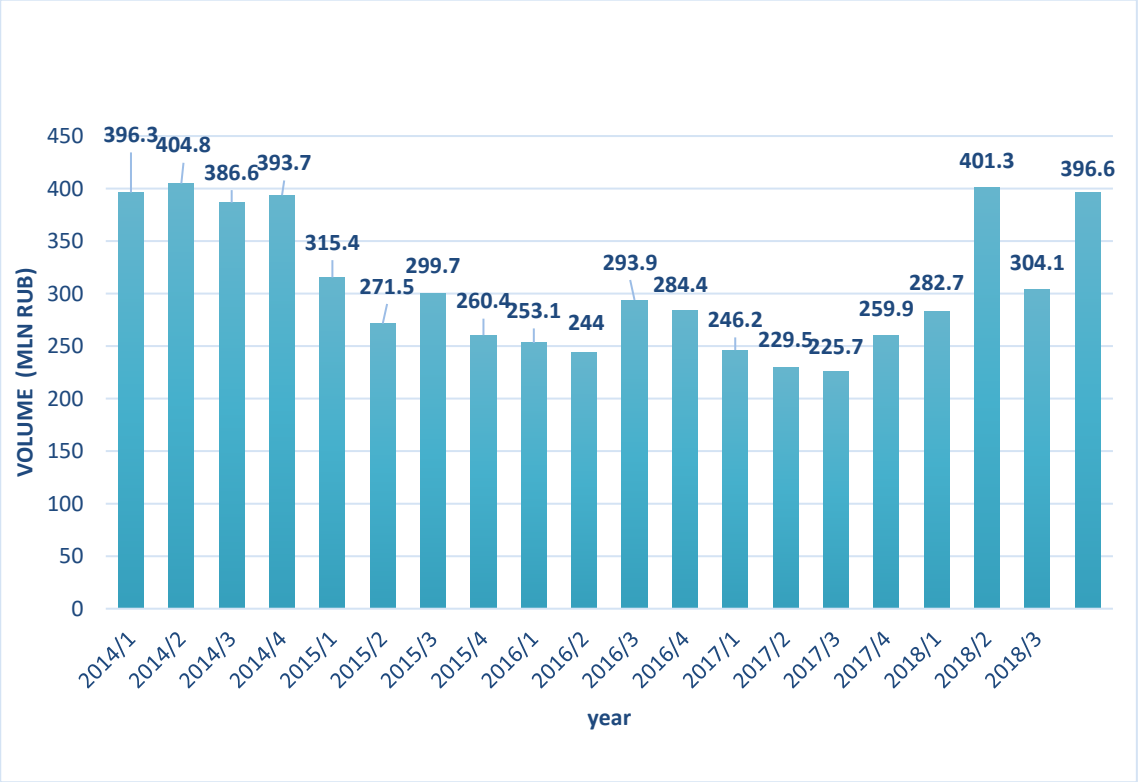
The data in the charts is mainly presented on a quarterly basis, so that we can track the trends more clearly. At the same time, in some parts of the text, we summarize the data for 4 quarters and use the annual values, as this helps to make a comparison with the previous years.

According to the Central Bank of Russia (2018b), the number and volume of transactions using payment cards issued in the territory of the Russian Federation is steadily increasing. Unfortunately, the same trend has the volume of frauds with payment cards (Figure 51).

'The volume of all unauthorized transactions performed using payment cards issued in the Russian Federation amounted to 1,384.7 million rubles in 2018, which is 44% more than in 2017 (961.3 million rubles)' (Central Bank of Russia 2018b). This could be caused not only by the growth of fraud in this sector, but also by the development of detecting technologies of the Central Bank of Russia, as well as an increase in the number of participants in the information exchange program. These factors have increased the quality of unauthorized transactions detection.

Figure 51:

The volume of unauthorized transactions using payment cards in million rubles



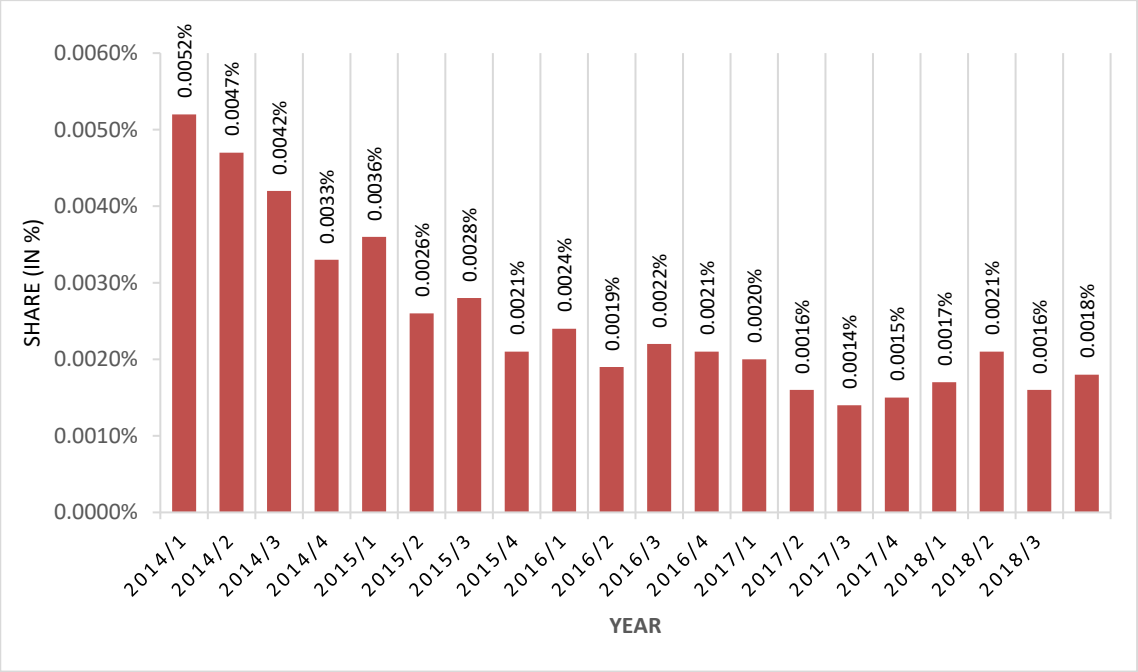
Source: made by authors, based on data from Central Bank of Russia (2018b).

Most of the thefts from individual accounts are committed through fraudsters obtaining unauthorized direct access to electronic means of payment or encouraging the owners of funds to make a transfer in favor of fraudsters independently by deception or abuse of trust (using social engineering methods). We will talk about it more detailed in further subchapters.

According to the Figure 52, *'the share of the volume of unauthorized transactions in the total volume of transactions performed'* (Central Bank of Russia 2018b) with the use of payment cards has a downside trend. Together with the results obtained by the Figure 0 means that the amount of transactions with payment cards is growing faster than the number of fraudulent transactions. The downtrend in this case may indicate an increase in user awareness of cyber crime. Moreover, it means that despite the fact that the volume of unauthorized transactions got a positive trend in the last presented years, the amount of cashless transactions as it is shown in the Figure 25 keep rising significantly. That shows us that cyber threats do not stop the process of digitalization.

Figure 52:

Share of unauthorized transactions using payment cards in the whole amount of transactions



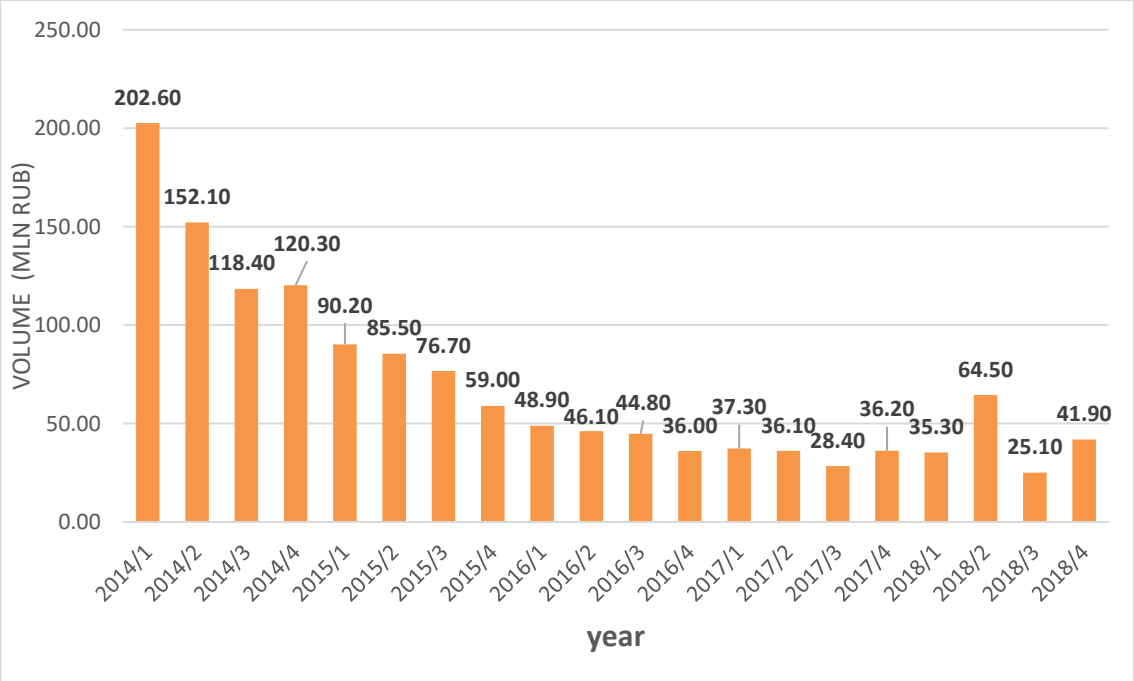
Source: made by authors, based on data from Central Bank of Russia (2018b).

In accordance with the requirements of the Central Bank of Russia (2018b), unauthorized transactions are divided into groups based on the conditions of their execution: 1) transactions through ATM and 2) CNP (Card not present) transactions.

On the Figure 53 we can see that the indicator of *'unauthorized transactions carried out through ATMs and payment terminals in 2018 amounted to 174 million rubles, which is 20.7% more than in 2017 (138 million rubles)'* (Central Bank of Russia 2018b). This growth is partially technical in nature, due to the improvement in the quality of the data provided by banks. If we look at the entire presented time period from 2012 to 2018, we can see a pronounced downtrend, which means that ATM fraud is steadily decreasing.

Figure 53:

Dynamics of unauthorized transactions using payment cards through ATMs and payment terminals in million rubles

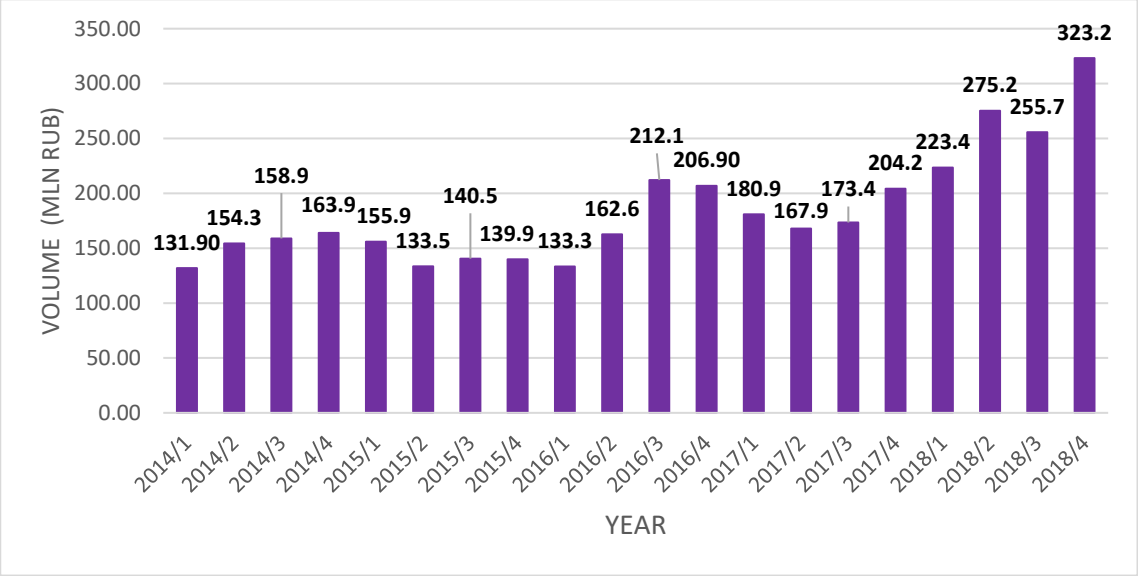


Source: made by authors, based on data from Central Bank of Russia (2018b).

In the next chart (Figure 54), we can see the opposite situation. The number of unauthorized transactions carried out via the Internet and mobile devices increases every year. If in 2017 the volume of such transactions amounted to 726.4 million rubles, then in 2018 this number increased by 32.6% and amounted to 1,077.5 million rubles.

Figure 54:

Dynamics of unauthorized transactions using payment cards through internet and mobile devices in million rubles



Source: made by authors, based on data from Central Bank of Russia (2018b).

Summarizing the information from the Figures 0 and 0, we can say that the volume of financial fraud via mobile phones and the Internet, on average, already exceeds the fraud associated with ATMs by 5-6 times. Moreover, they have opposite trends that make it possible to expect an even greater gap between ATM and CNP transactions in the future. This phenomenon can be attributed to the growing availability of payment services via the Internet. This leads to a shift in the interest of cyber criminals from ATMs and trade organizations towards CNP-transactions.

We have examined the amount and damage from cyber attacks and now we would like to talk about other characteristics of these attacks. Next, we want to consider the main types, goals and motivation of cyber attacks.

On the Figure 55 we can see the percentage of the unauthorized transactions which were made with the help of social engineering. Over the time period from 2015 to 2019, the vast majority of them occurred due to the use of an electronic means of payment without client's consent due to the following reasons:

- illegal actions;
- loss or violation of confidentiality;
- violation by the client of the procedure for using an electronic mean of payment;
- inducement to independently perform an operation by deception or abuse of trust.

These unauthorized operations are associated with the use of social engineering.

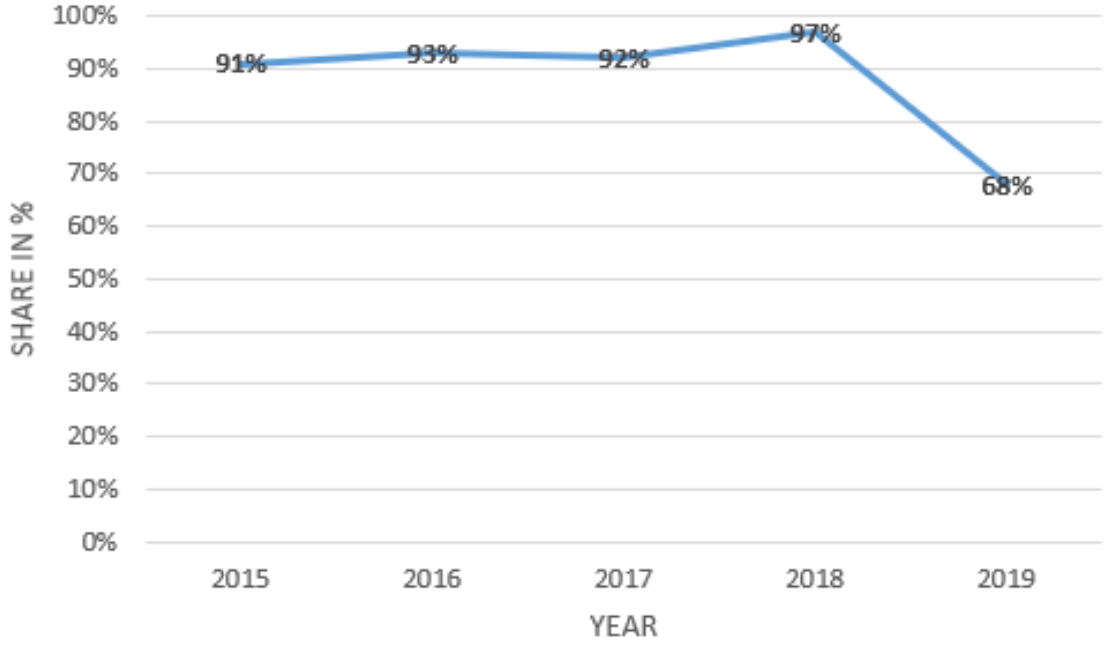
However, in 2019 we can see a sharp decline in this indicator by 29 percentage points. This decrease can be explained in two ways:

- on the one hand, by a change of methods for calculating basic indicators (transition from reporting form 0409258 to form 0403203 (Central Bank of Russia (2019b))), which was carried out at the beginning of 2019;
- on the other hand, by increasing the level of cyber awareness of the population as a result of special trainings carried out by the Central Bank of Russia and banks themselves.

These trainings educate bank customers about the risks of using electronic means of payment and about the delineation of liability between the bank and the client in case of payment card data compromising.

Figure 55:

Percentage of unauthorized transactions due to the use of social engineering



Source: made by authors.

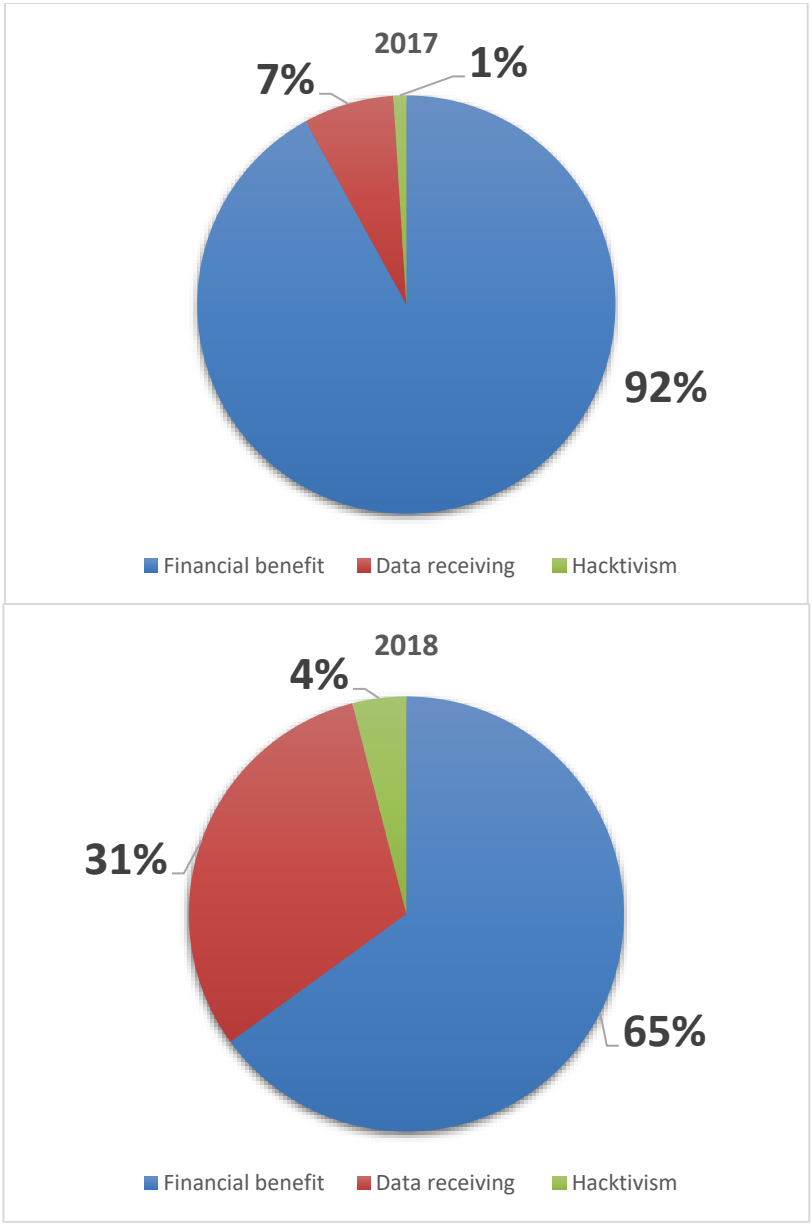
In the Figure 56 we can see the motives for attacks on organizations in Russian banking sector in 2018. The main motive of cyber criminals is financial gain (65% of incidents in 2018 and 92% in 2017). The share of incidents aimed at obtaining data (information about payment cards, personal data, user credentials for accessing personal accounts and others), increased from 8% to 31% from 2017 to 2018.

The key motive of hackers attacking financial institutions is direct financial gain. And even attacks aimed at obtaining information about payment cards, personal data,

user credentials for accessing personal accounts, and others, can be monetized in the future due to the subsequent theft of money from accounts or their resale in the shadow market. This type of information accounts for up to 83% of all data sold and bought on the dark web. The least popular motive for attacks is hacktivism is '*the use of computer-based techniques such as hacking as a form of civil disobedience to promote a political agenda or social change'* (Mikhaylova 2014).

Figure 56:

Motives for attacks on organizations in Russian banking sector in 2017 and 2018



Source: made by authors, based on data from Central Bank of Russia (2018b).

In the figure 57 the most popular methods of attacks against organizations in the financial sector are presented. At the end of 2018, among the methods of attacks, the leaders were: the use of malicious software, social engineering, hacking, brute-forcing and the exploitation of web vulnerabilities. Bank of Russia employees identify

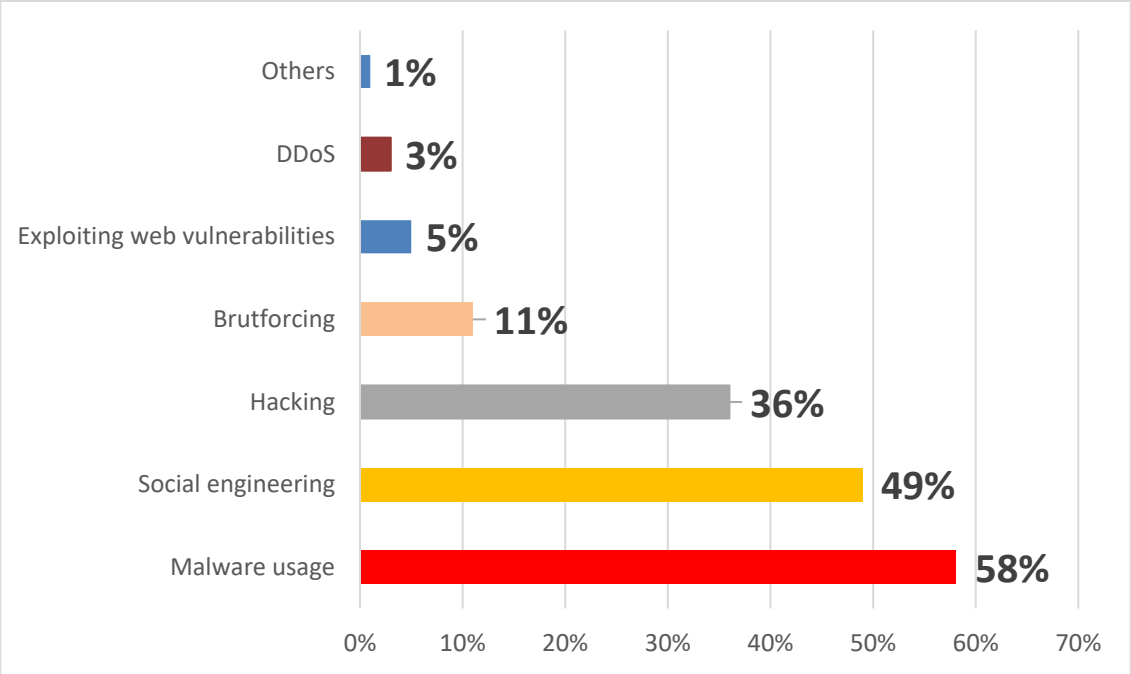
'hacking' as a separate type of attack, implying *'exploitation of vulnerabilities in connection-accessible network services'* (Central Bank of Russia 2018a, p. 2), separating it from brutforcing for greater specification.

In general, the situation for 2018 repeats the trends of 2017 (Central Bank of Russia 2018a). In a Figure we can see that the most popular method was usage of malicious software, in 2018 it had a share of 58%, which is 10% more than in 2017 (Central Bank 2018a). This is facilitated by the fact that harmful software becomes more accessible every year. That decreases the entry barrier to the cyber criminal business. The security system in financial institutions is usually well organized, as a result, social engineering remains the main vector of infiltration into infrastructure, used in 49% of attacks. Phishing is the most efficient way to deliver malicious software. 90% of cyber criminal groups in 2018 used it at the first stage of attack (Central Bank of Russia 2018a). Search and exploitation of vulnerabilities in publicly available services (hacking) is used in 36% of attacks on financial institutions, and brutforcing and exploitation of web vulnerabilities - in 11 and 5% of attacks, respectively.

In this case, middle-level banks can be the main aim of attackers, as these banks are not always ready to invest large budgets in ensuring their own security. Smaller banks can act as an intermediary in an attack: for example, their employees' computers can send phishing emails to their colleagues from larger banks. It is not uncommon for attackers to combine these methods in an attack, that is why percentages on a graph do not add up to 100%.

Figure 57:

Methods of attacks against organizations in the financial sector in 2018



Source: made by authors, based on data from Central Bank of Russia (2018a).

The security of the internal network of credit and financial institutions has space for improvement. Figure 58 shows the most common vulnerabilities in the internal network of banks and the share of banks in which these vulnerabilities are present. As we can see, the use of dictionary passwords comes across in 100 percent of banks. This problem occurs when the password set by the user or administrator is so non-unique that it can easily be found in special hacker dictionaries which include the most common passwords. In almost 50% of cases, weak passwords are set by users, but more often standard accounts are left by administrators while installing new software on computers.

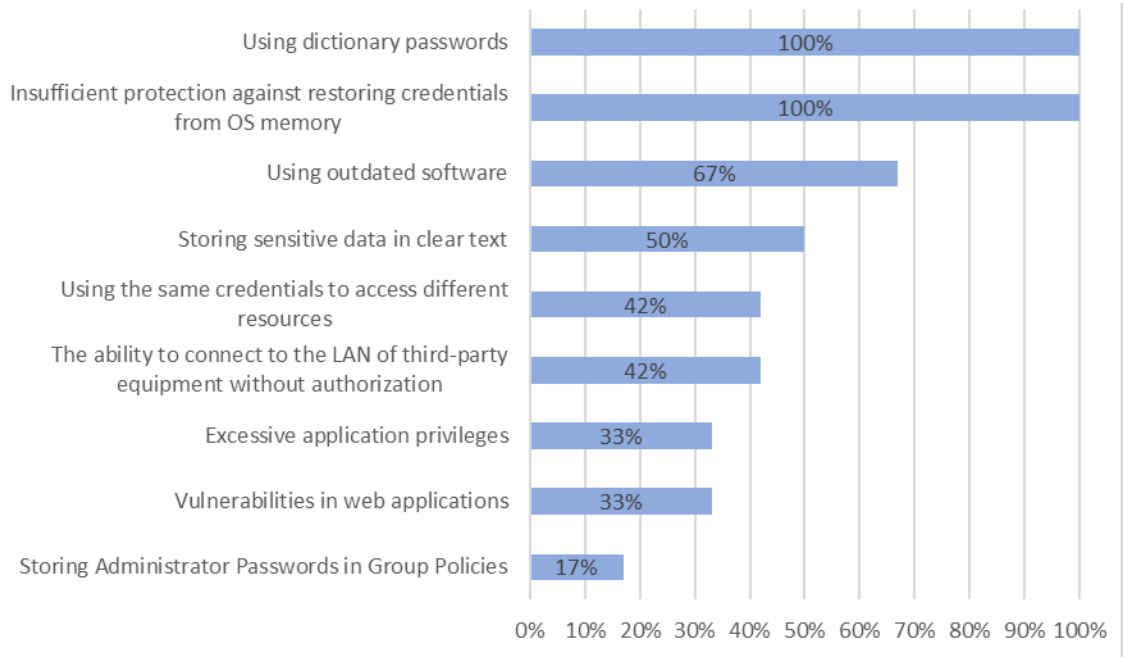
Another common problem that occurs in 100% of cases is insufficient protection against restoring credentials from the operating system memory. This happens when, for example, the browser prompts you to remember your login and password. In addition, a common vulnerability is the use of outdated software (67%) and storage of sensitive data in an open (not encrypted) form (50%). By sensitive data we mean information the unauthorized disclosure or modification of which can result in serious monetary or other loss. In 42 % of banks, vulnerabilities such as using the same credentials to access different resources and the ability to connect third-party devices to a company's local area network. The responsibility for the first vulnerability lies with the bank employees. They usually use the same password for different accounts to make it easier to

remember. The second vulnerability is more likely associated with an error of system administrators, as they incorrectly organize the network security system.

For 33% of banks applications had excessive privileges. Unreasonable assignment of elevated privileges to users in various information systems leads to the massive use of accounts with local administrator privilege. This happens when, for example, an employee, entering a banking application, has access to the accounts of other employees or to databases which he does not need. The last in this list - the vulnerability of web applications - is found in 17% of the surveyed banks. In fact, this vulnerability is much more common. But usually professional checks are needed to identify it, for example, penetration tests. We will discuss it more detailed in following paragraphs.

Figure 58:

Most common internal network vulnerabilities (percentage of banks)



Source: made by authors, based on data from Central Bank of Russia (2018a).

Looking at the Figure 0, we can see that a large number of vulnerabilities, even in the internal network, are based on human factors and, as a result, they can be vulnerable to social engineering.

The most vulnerable element in the security system of a credit and financial institution is its personnel. The test performed by FinCERT in 2018 (Central Bank of Russia 2018a) showed that in 75% of financial institutions, employees clicked on the link in a phishing email, in 25% they entered their credentials in a false authentication form, and in another 25%, at least one employee launched a malicious program on his or her office computer. In this case, it is enough that only one user performs an unwanted action and then the intruder will gain access to the corporate network. The

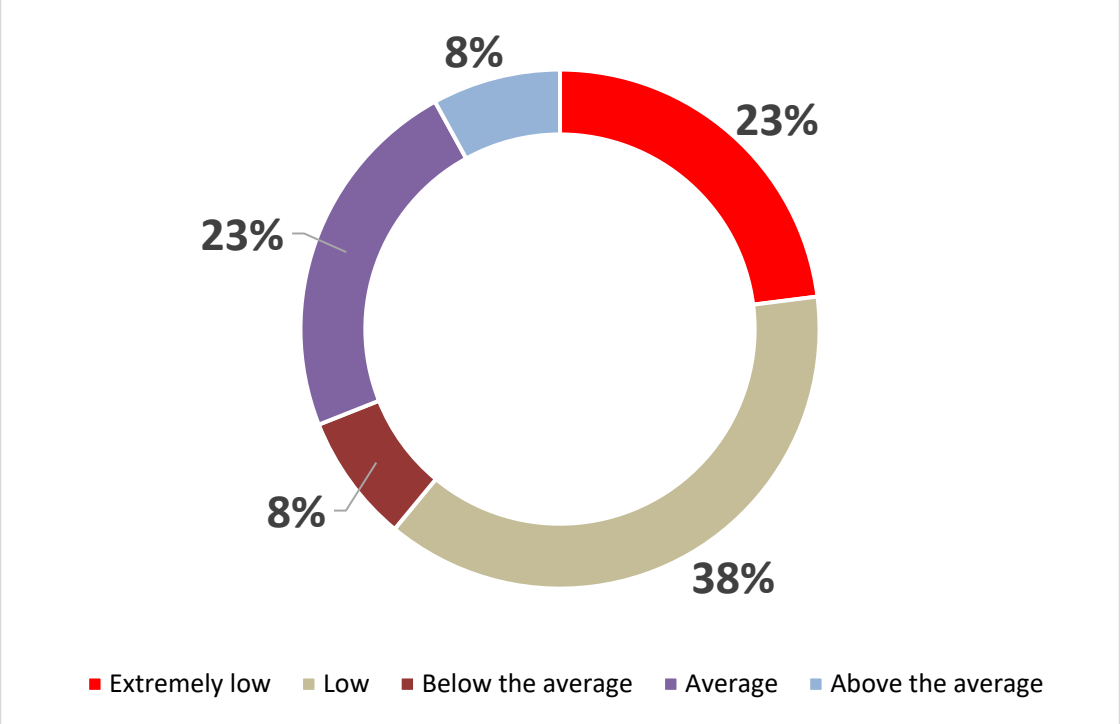
reason human factor is so powerful lies in the fact that the level of cyber literacy is very low not only among users, but also among bank employees. Thus, three-quarters of banks are vulnerable to social engineering attacks.

As we can see in the Figure 59, the security of mobile banking is not fully protected. 23% of bank applications have extremely low level of security, this means that the sensitive data can easily be stolen. Insecure data storage is the main problem, it was identified in 76% of mobile applications (which is 11% higher than in 2017). Passwords, financial information, and personal data of users are not stored safely and face the risk of stealing. An attacker rarely needs physical access to a smartphone to steal data: *'89% of vulnerabilities can be exploited using malware'* (Central Bank of Russia 2018a).

Based on the data from the previous chapters, we can say that even if there are some security related problems in Russian mobile banking, the rating of banks mobile applications keeps rising (Figure 29). It means that cyber risks do not have a significant effect on consumer behavior in terms of using mobile banking applications.

Figure 59:

Security level of online banks (share of systems)



Source: made by authors, based on data from Central Bank of Russia (2018a).

One more important problem in mobile banking applications is that some of the online banks do not use two-factor authentication mechanisms, for example, one-time passwords for critical actions (authentication, changing credentials, etc.). Another

problem is that the validity period of passwords is too long. The reason of such behavior can be that banks are striving to find a balance between security and application usability.

The recent problem with Sberbank (the biggest bank in Russia) can be considered as a good example of this situation. A couple of weeks ago, a user of the 'Sberbank Online' banking application discovered that the password in the application works regardless of the font case. For example, the password 'PasSwOrd' was equal to 'password', hence the account could be entered successfully using them both. Sberbank confirmed that both the login and the password fields in the application are not case sensitive. This is done for the convenience of users (Tjournal 2020).

However, it is dangerous to abandon even some of the security measures in favor of convenience as it increases the risk of fraudulent transactions. If the credentials are not case sensitive, then it is much easier to guess it by brutforcing. If there is no need to confirm the operation with a one-time password, the attacker no longer needs an access to the victim's mobile phone which makes it easier and faster.

In this subchapter we have found that the share of unauthorized transactions using payment cards in Russia has a negative trend. The reason of this can be an increase in user awareness of cyber crime. The vector of these attacks shifts its focus from ATMs and trade organizations towards CNP-transactions. Although, the percentage of unauthorized transactions due to the use of social engineering dramatically decreased in 2019, it remains the main reason of cyber crimes in this area. Talking about the volume of unauthorized transactions, we can look at the share of these transactions, and even in the period of time when it had a positive trend (2017-2018), it did not affect the growth of cashless payments which maintains growth rates (Figure 25). The changes in the percentage of unauthorized transactions do not have much effect on companies' and people's use of cashless payments. The same situation exists in the field of the mobile banking: cyber security problems do not stop the raise of average application rating. In the previous chapters, we saw the trend that mobile banking is becoming more and more important for users, and therefore for banks, hence it can be assumed that for users technological development and improvement outweigh the disadvantages of risks, which reflects the growth of ratings. Financial benefits are the main motive for attacks on organizations in Russian banking sector. Although malicious software has a large percentage, social engineering remains the main method of infiltration into banks infrastructure. Even internal network vulnerabilities (using dictionary passwords, storing sensitive data in a clear text, using the same credentials for different accounts

and others) are based on human factors, and consequently they can be vulnerable to social engineering. One of the main reasons for the importance of the human factor can be the low level of cyber literacy not only among users, but also among bank employees.

5.2. Protection methods

In this subchapter we are going to discuss the Russian government regulation measures and actions which are aimed to protect the banking sector. First we will talk about the organization which was created by the Central Bank especially for monitoring and controlling cyber attacks in banking sector, its aims and methods, we will describe the operation process and show the results. Then we will discuss the legislative framework, mentioning the international standards and Russian Federal Laws which together form the basis for the functioning of the state control's system of Russian cyber security. After that we will demonstrate the actions which are undertaken by the regulator in the fight against human-based and machine-based vulnerabilities in the banking sector.

In 2015, the Central Bank of Russia created the Center for Monitoring and Responding to Computer Attacks in the Credit and Financial Sector - FinCERT. The main task of FinCERT is to organize information exchange and consolidation of financial and information security market participants in the fight against cyber crime.

FinCERT receives information about cyber threats from supervised financial institutions, integrator companies, anti-virus software developers, foreign financial organizations and regulators, incident response teams (including foreign ones), providers and telecom operators, as well as law enforcement and other government agencies, overseeing the information security of the industry.

FinCERT also cooperates with foreign partners. In 2018, the Central Bank of Russia signed agreements on cooperation in the field of information security with all members of the EAEU (Eurasian Economic Union) (Figure 60).

Figure 60:

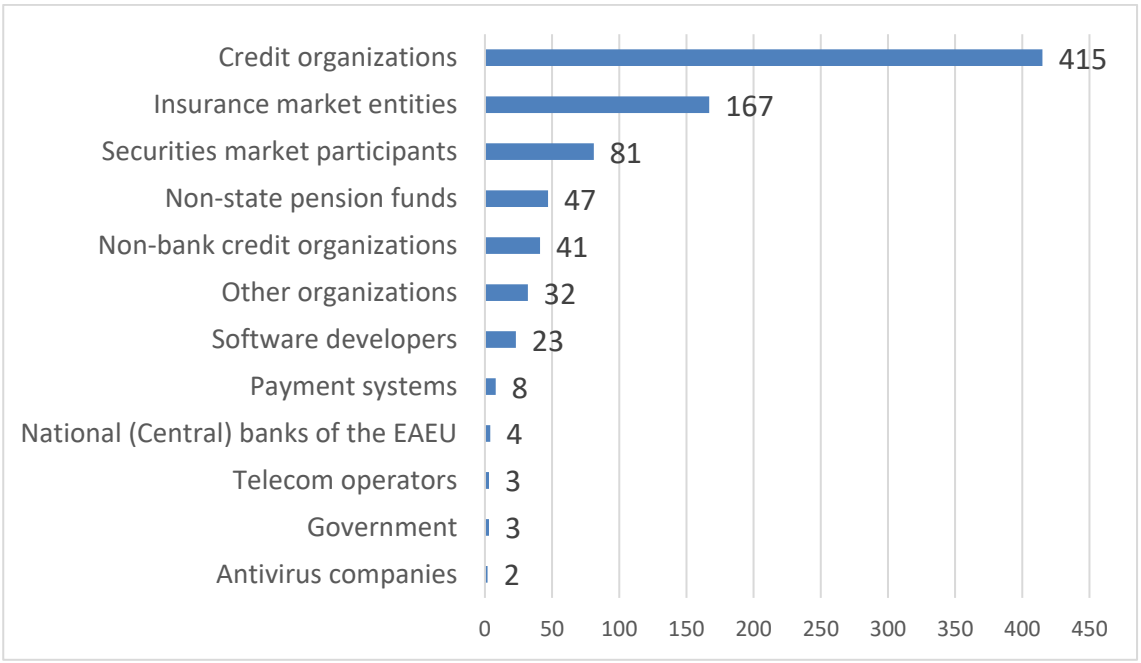
FinCERT international cooperation

Source: Central Bank of Russia (2019a).

To simplify the process of information exchange, as well as to increase the efficiency and level of its security, an automated incident proceeding system - AIPS FinCERT was created. All banks of the Russian Federation, many insurance organizations and others are currently connected to this system. In total, 826 organizations are connected to the system (Figure 61). Interaction with organizations is carried out free of charge.

Figure 61:

Structure of AIPS FinCERT information exchange participants by type of activity



Source: made by authors, based on data from Central Bank of Russia (2019a).

As we can see that the biggest group of participants consists of credit organizations. Compared to the share of other participants, we can say that the main focus of FinCERT is on them.

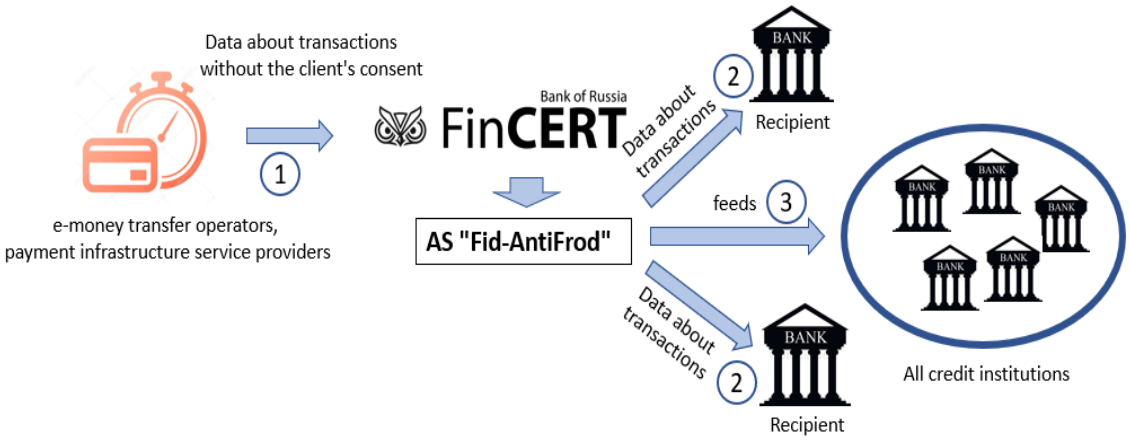
Connection to this information exchange system gives each participant the right to get the help of FinCERT specialists at any time. Such assistance may be required in cases of detection of malicious software, attempts to exploit software vulnerabilities, suspicious network interactions and in any other cases of computer attacks.

On the basis of AIPS FinCERT, the Central Bank of Russia has created the AS (automated system) ‘Feed-AntiFrod’. This is a database that includes information about cases and attempts to transfer funds without the consent of the client. The unusual name of the system appeared as a result of the letter-by-letter translation of the term Antifraud from English into Latin.

AS ‘Fid-AntiFrod’ is designed to accumulate and quickly exchange information about transactions without the client's consent. The main participants in this exchange are e-money transfer operators, payment infrastructure service providers and the Bank of Russia. In the Figure 62 we can see, how the whole process goes. Below we comment on each step on the scheme.

Figure 62:

Scheme of AS "Fid-AntiFrod" operation



Source: made by authors.

Information about transactions without the client’s consent is transferred to FinCERT (1). Further, with the help of the AS ‘Fid-AntiFrod’ system, the information is transferred to credit institutions that are recipients of funds for these transactions (2). Then, as a result of the analysis of information on such transactions, special messages are generated for all credit institutions (the so-called ‘feeds’ containing traits of

transactions performed without the client's consent), which allow credit institutions to apply both preventive and response measures (3).

As a result of the functioning of the AS 'Feed-AntiFrod' the participants of the information exchange receive various information about recipients of funds for transactions carried out without the consent of the client:

- the hashed data of the passport numbers;
- the hashed data of SNILS (Individual insurance account numbers);
- the TIN (Taxpayer identification numbers) of organization;
- the bank accounts numbers;
- the card numbers;
- the phone numbers;
- electronic wallet numbers.

Today the system has already collected nearly 19 thousand messages about the unique features of transactions performed without the client's consent.

The important point is that passwords and personal insurance numbers are stored in a hashed form. Hashing is a process of mapping data of arbitrary size to fixed-size values. It should not be confused with encryption, as hashed information is almost impossible to decrypt. Such a way of storing sensitive data, makes more protected against stealing and changing in case of cyber attacks.

FinCERT is a fairly new subdivision created by the Central Bank of Russia. Nevertheless, it has already deeply integrated into Russian financial sector. As we have seen, it has a wide network of international cooperation and a large number of cooperating domestic credit institutions. But in order to achieve such results, serious work has been done.

FinCERT's main problem at the time of its creation was the lack of trust among banks. Banks did not want to share information about incidents with the Central Bank of Russia subdivision and there were good reasons for it. Banks were afraid because of the fact that the Central Bank of Russia was actively withdrawing licenses and thinning the number of banks during that time, as shown in Figure 17 in the third chapter.

To 'encourage' more banks to participate in the information exchange some legislative measures have been taken and we will discuss them more detailed in the following part.

5.2.1. Legislative regulation of the cyber security

Ensuring information security in the financial sector requires the formation of a legal regulation mechanism. First, we will look at the international information security standards, which are applied in Russia.

Payment Card Industry Data Security Standard (PCI DSS) is a standard developed by an organization established by international payment systems: Visa, MasterCard, American Express, JCB and Discover.

'*The PCI Data Security Standard (PCI DSS) applies to all entities that store, process, and/or transmit cardholder data. It covers technical and operational practices for system components included in or connected to environments with cardholder data. If you accept or process payment cards, PCI DSS applies to you'* (The PCI Security Standards Council 2020).

Since September 2006, the standard has been introduced by the international payment system Visa on the territory of the CEMEA region (Central and Eastern Europe, the Middle East and Africa) as mandatory, and accordingly, it now applies to Russia. Therefore, service providers (processing centers, payment gateways, Internet providers) working directly with VisaNet must comply with the requirements of the standard.

There exists another international standard - ISO/IEC 27001. '*It is an international standard on how to manage information security. The standard was originally published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in 2005*' (Bsigroup 2020). ISO 27001 specifies information security management system requirements to demonstrate the ability of an organization to protect its information resources.

Although the standard is used by some banking organizations, based on an analysis of the literature, it is not particularly widespread among Russian organizations. According to information security expert Alexei Lukatsky, '*It is all about the absence of a clear result-oriented system that has specific goals and is measurable at every stage ... the process approach has firmly entered the life of many companies around the world. But for Russia it is not yet a standard - we are just beginning to introduce it into our lives. Therefore, many things and terms are still incomprehensible to us'* (2007).

In addition to international standards regulating cyber security of the banking sector, there is local legislation in Russia.

The key regulator of banking IT security in Russia is the Central Bank of Russia.

The objectives of the Central Bank of Russia in the context of information security are:

- ensuring cyber resilience (by monitoring the risk indicators of the implementation of information threats, ensuring the continuity of the provision of financial and banking services, controlling the level of fraudulent transactions);
- protecting consumers of financial services (by monitoring and controlling indicators characterizing the level of financial losses);
- promoting the development of innovative financial technologies (by controlling the risk of implementing information threats and implementing the required level of information security) (Central Bank of Russia 2019b).

The main document regulating the protection of information of Russian banks is Federal Law No. 161 'On the National Payment System'. In accordance with the Article 27 of this Law, money transfer operators and other participants in the payment infrastructure are obliged to ensure the protection of information when making money transfers in accordance with the requirements established in the Regulation of the Central Bank of Russia dated 09.06.2012 No. 382-P. In addition, money transfer operators and other participants of the payment infrastructure are required to send information to the Central Bank of Russia about all cases and attempts to make money transfers without the client's consent in the way established by Central Bank of Russia Ordinance No. 4926-U. Banks are also obliged to implement measures to counter such transfers.

Though, according to these regulations, banks are obliged to participate in information exchange process with FinCERT, that explains why all the banks in Russia are connected to the ASOI FinCERT.

Another fundamental document in the field of ensuring information security of the banking sector in Russia is the Central Bank of Russia Regulation No. 382-P 'On Requirements for Ensuring Information Security when Making Money Transfers ...'.

The document is a set of requirements that must be met by a banking organization to comply with the information protection standards specified in Federal Law No. 161. According to it, the main requirements of this Regulation are:

- assignment and distribution of access rights for employees of financial institutions;
- information protection at all stages of the life cycle of information infrastructure objects;
- information protection while accessing information infrastructure objects;

- protection against malicious code;
- information protection while transferring funds over the Internet;
- information protection while using ATMs and payment terminals;
- information protection while using payment cards;
- protection of information processing technology when transferring funds;
- creation of an information security service centre;
- conducting training sessions to raise awareness in the field of information security for employees of financial organizations;
- identifying, analyzing the causes of occurrence and responding to information security incidents associated with violations of the requirements for securing security information when transferring funds (Central Bank of Russia 2012).

5.2.2. Actions undertaken by the Central Bank of Russia

In this subchapter we will demonstrate actions which are undertaken by the Central Bank of Russia to fight human-based and machine-based vulnerabilities.

Human-based vulnerabilities

As human-based attacks we consider social engineering. As it was explained in the Chapter 2, it consists of 3 parts: phishing, vishing and smishing. However, all three parts have the same mechanism, but the tools are different.

The Central Bank of Russia, represented by FinCERT, notifies domain name registrars about malicious domain names and asks to block them. The malicious category can include sites from which malicious code is sent and fraudulent actions are performed using payment cards. This process takes a long time, as Central Bank can only advise domain names registrars which domain should be blocked. A positive decision on the blocking of domains proposed by FinCERT in 2018 was made for 85% of the resources; in 2017 the figure was 76% (Central Bank of Russia 2018a). The increase in the share of positive decisions may be the consequence of the high quality of FinCERT examination in the assessment of fraudulent resources. If the malicious resource is located outside the Russian domain zones, FinCERT cannot contact the registrars, but it sends the information to the General Prosecutor's Office of the Russian Federation, which initiates an administrative case and sends it to court. Due to the fact

that there is such a big difference between blocking sites with Russian and foreign domains, it is more convenient for cyber criminals to use foreign domains. Therefore, many of the already existing malicious sites move to foreign space, and new ones are initially created there (Central Bank of Russia 2019a).

Moreover, government is planning a new bill № 605945-7 ‘On Amendments to the Federal Law on Information, Information Technologies and Information Protection’ and the Civil Procedure Code of the Russian Federation. After its adoption the procedure for blocking sites located in foreign domain zones will be significantly simplified. The Central Bank of Russia will be empowered to extrajudicially block malicious sites through direct interaction with Roskomnadzor (Federal Service for Supervision of Communications, Information Technology and Mass Media) on the inclusion of sites in the register of information prohibited from distribution in the Russian Federation. This bill also involves the introduction of a pre-trial mechanism for blocking sites that distribute malicious software.

On the one hand, this can be viewed as a positive trend, since the Central Bank of Russia will be able to directly block malicious sites, which will make this process faster and more efficient. On the other hand, such a bill gives the Central Bank of Russia more power. Moreover, there is currently no official document containing the criteria for malicious sites. This means the Regulator will make a decision based on its own assessment, which is also alarming.

The main factor determining the success of social engineering fraud is the low level of ‘computer hygiene’ of the victim. Below low ‘hygiene’ identifiers for different channels are presented.

- Smishing: clicking links from unverified sources to infected sites in SMS.
- Vishing: giving personal data without checking by phone.
- Phishing: clicking on links from unverified sources to infected sites, downloading ‘customized’ applications and free analogues of well-known programs on mobile phones, ignoring the installation of antivirus and its warnings.

All of them make it possible for attackers to obtain a login and password from a personal account or primary data on a bank card.

In order to lower the human risk factor, FinCERT conducts trainings to improve the cyber literacy of the population. These trainings are mostly aimed at elementary and high school students, as well as elderly people since these parts of the population are most vulnerable to social engineering.

It is also important to pay attention to the cyber literacy of financial sector workers. The effectiveness of phishing against the banking sector is above the market average because phishing mailings are usually better prepared. Bank-targeted phishing emails are 60% more likely to include personification - addressing the victim by name, mentioning the employee's real job responsibilities etc. This increases the level of trust to the letter and the likelihood that the link will be opened. (Central Bank of Russia 2018a)

To increase the cyber literacy of employees, in addition to conducting numerous trainings, it is planned to create a cyber laboratory (cyber testing ground) for practical training of personnel for the credit and financial sector and the Central Bank of Russia. The cyber polygon is planned to be created as a platform for emulating cyber attacks to develop countermeasures and prevention measures, as well as conduct training activities in the area of cyber security.

Machine-based vulnerabilities

To control vulnerabilities in software, including those associated with programming flaws that lead to computer attacks, it is necessary to create organizational and technical conditions for financial organizations to analyze application software vulnerabilities and determine which software should be analyzed.

In 2004 the certification system FSTEC (Federal Service for Technical and Export Control) was established in Russia. It has the following functions:

1) ensures the security (by non-cryptographic methods) of information that has a significant impact on the security of the state in the information sphere;

2) counteracts foreign technical intelligence services on the territory of Russia;

3) provides protection (by non-cryptographic methods) of information containing information constituting a state secret, other information with limited access (Central Bank of Russia 2019b).

At the level of the regulator FSTEC is used to control the quality of software distributed by credit institutions among their clients. The software is studied, tested, checked for vulnerabilities and the presence of undeclared features. After passing all tests, a certificate is issued. Such a certificate is necessary for all companies that work with personal data; it confirms that the company's IT system is sufficiently protected.

At the level of commercial banks, penetration tests are conducted. This is a method for assessing the security of computer systems in which pentesters simulate a hacker attack on a system. According to the requirements of Central Bank of Russia

Regulation No. 382-P, starting from 01.07.2018, banks must annually conduct penetration testing and analysis of vulnerabilities of information infrastructure facilities (Central Bank of Russia 2012).

Next, we would like to talk about ensuring the security of data transmission and processing. Ensuring the security of data processing using digital technologies is a task, the solution of which is supposed to be carried out individually – in relation to each specific financial technology.

According to the Central Bank of Russia, the key information security methods are:

- use of means of electronic signature (cryptography);
- the principle of 'double control' when processing protected information;
- multi-factor authentication of clients, including the use of cryptographic information protection tools;
- implementation of mechanisms for additional confirmation of clients' financial transactions (2019b).

An important factor in the fight against unauthorized transactions can also be the introduction of antivirus software into banking applications installed on client devices and more accurate methods of client authentication.

We can give an example of the successful way of protection. This technology is already being used by the largest bank in Russia - Sberbank. The Sberbank Online application has a built-in antivirus. It initializes the smartphone - scans the operating system, RAM (Random Access Memory), programs and active processes that run in the background. The main task of the antivirus is to prevent hacking of mobile banking. The check is performed several times a day, and the banking application simply will not start without scanning. If malware is found, the antivirus will warn the user about it. Such a technology can be considered as a step from the client's comfort to the client's safety. While Sberbank has demonstrated a reckless approach to data in the previous example by using case-insensitive passwords, it improves the security of its users in other ways. Using Sberbank as an example, we can say that Russian banks are trying to keep a balance between convenience and security.

In this subchapter we showed the protection methods which are undertaken by the Russian government against cyber attacks on the banking sector. The key regulator of Bank's IT security in Russia is the Central Bank of Russia. First, we have looked at its subdivision - FinCERT – which was created by the Central Bank to regulate the information exchange between financial organizations and the government. It helps

banks in minimizing future cyber risks. Then we have analyzed the regulation base of cyber security in Russia, including international standards. We found that Russian banks comply with PCI DSS standard. However, they are not yet ready to fully understand the requirements of ISO/IEC 27001 standard. In addition to international standards, Federal laws regulating cyber security are used on the territory of Russia, the main mission of which is to compel banking organizations to keep records and exchange information about cyber incidents with FinCERT. This is done in order to control the number of attacks and identify their typical features, to make it possible to detect and prevent fraudulent transactions in future. However, the increase in the degree of security of information systems of credit organizations led to the fact that the focus of criminals shifted to social engineering attacks on clients and employees of the banks. Hence, in the following part we described the actions which the Central Bank of Russia uses to fight social engineering. We have found that the Central Bank of Russia has rather an advisory role in fight against phishing. It can contact domain registrars to recommend them to block a malicious site, however, its requests are fulfilled in most cases. In the case of foreign domains, the blocking process is more complicated. That is why there is a trend in Russia for malicious sites to move to foreign space. Moreover, in order to lower the human risk factor, FinCERT conducts trainings to improve the cyber literacy of the population and bank's employees. Next, we talked about dealing with machine-based vulnerabilities. FSTEC (Federal Service for Technical and Export Control) is used to control the quality of software distributed by credit institutions. It has a right to issue the certificates which are necessary for all companies that work with personal data; it confirms that the company's IT system is sufficiently protected. Commercial banks in Russia are also required to monitor their cyber security levels and conduct penetration tests annually.

As we have found in the first subchapter, the main method of cyber attacks is social engineering, and the objective of them are banks clients and employees. In the second subchapter we found that the most common government measures are blocking fishing websites and conducting trainings to improve the cyber literacy of population and bank employees.

Concluding remarks

Currently, digitalization is penetrating all banking processes and is increasingly influencing them. In this work, we tried to show how the digitalization process developed in Russia, what were its preconditions, advantages, risks and special features.

Russian banking system consists of two levels: the first includes the Central Bank of Russia which regulates the banking system and protects the national currency; the second level has two participants: banks and non-bank commercial organizations, banks play the major role on this level. Banking sector in Russia has several special features: the number of banks has significantly decreased during the period 2012-2020 because of the actions of the Central Bank of Russia. Another feature is the high concentration in the sector: the first 200 banks owe more than 99% of all banks assets, moreover the top-5 banks has more than 60% of assets. The type of Russian banking system has significantly influenced the development of digitalization.

In this master thesis we have addressed three research questions. Based on our key findings, we can answer them and check the validity of our hypotheses. The **first research question** asked what kind of effect digitalization has on the performance of the Russian banking sector. Our initial hypothesis stated that digitalization changes the way banking services are provided, promotes the creation of new distribution channels, increases banking sector profitability in general. As a result of our analysis we can approve this hypothesis. We will explain it further by dividing the hypothesis into two parts.

First, we are going to talk about the way banking services are provided and the creation of new distribution channels. The process of digitalization changes the way of providing banking services: we have shown on the example of four types of remote banking. According to Dolgushina (2016), at the present stage, we can distinguish the following types of remote banking channels, depending on the type of technology: telephone banking, terminal banking, mobile banking, Internet banking. Telephone banking has almost disappeared; it is currently used by the elder generation to check account balances, information about connected services, and other simple actions that do not require operator participation. Terminal banking which has two forms: ATM and terminals has changed a lot. This happened due to the fact that since 2014-2015 there has been a sharp decline in interest in ATMs and physical branches of banks in Russia with the following transition to online. This led to a decrease in the volume of cash withdrawals and, consequently, to an increase in electronic payments. Internet banking

has grown significantly because of the growing number of Internet users in Russia, as well as the widespread adoption of more portable devices such as laptops, netbooks and ultrabooks. Mobile banking is the youngest participant, because it appeared recently, but it has grown a lot, due to distribution of smartphones in Russia which grew significantly in Russia in the period from 2015 to 2020. It makes mobile banking very important for Russians. As we saw from the example of our key findings, we can say that the way banking services are provided has changed, telephone banking is becoming less useful, the need for terminals decreases and the role of terminals has increased. Moreover, digitalization has created two new types of service provision – mobile and internet banking, which are becoming more and more popular in Russia. According to Markswebb (2020), the current aim of Russian banking system is to become a Digital office, to transform some tasks which are historically associated with visiting a branch: closing and opening an account, obtaining inquiries, resolving claims, etc. into digital space.

Seconly, digitalization has positive impact on banking performance. We have shown this with the example of two digitalization proxies of our model: ATMs and terminals. In order to measure the impact of digitalization on the profitability of the banking sector, we built two models and performed regression analysis. Each model has one dependent variable: ROA and ROE and 7 independent variables: KRBR, GDP per capita (annual), BS, AM (Asset Management), OE, CR and DIG. The DIG factor has several proxies: Average mobile banking rank, Amount of ATMs, Amount of terminals, Percentage of electronic orders in transfers in total, Electronic payments for goods and services in thousands rubles, IDI. Our goal was to find out whether digitalization affects the profitability of banks, and based on the results of the regressions (Figures 44 and 45) we can conclude that the relationship exists. Since we took several proxies for the digitalization factor, based on the models, we can say that the number of terminals and ATMs has the greatest influence among all. Profitability and the number of terminals are positively related to each other, that is, with an increase in the number of terminals, profitability increases. At the same time, the number of ATMs has the opposite tendency - profitability grows with a decrease in the number of ATMs. This dependence exists due to the fact that at present, Russian banks have a trend towards a reduction in ATMs and physical offices, which we have discussed in previous chapters, and due to the fact that Russians have a positive attitude towards technologies, which was also discussed above, hence there are more and more points sales terminals are equipped with cashless payment terminals.

Thereafter, we have examined our **second research question**, whether cyber crimes affect the digital growth trend. We assumed that the cyber crimes do not have a significant effect on the digitalization growth trend. We can approve this hypothesis, based on the following findings. Talking about the volume of unauthorized transactions, we can look at the share of these transactions, and even in the period of time when it had a positive trend (2017-2018), it did not affect the growth of cashless payments which maintains growth rates (Figure 25). In this example we took unauthorized transactions as a measure of cyber attacks and the cashless payments as the proxy of digitalization. We can say that the changes in the percentage of unauthorized transactions do not have much effect on companies' and people's use of cashless payments. The same situation exists in the field of the mobile banking which is also our proxy for digitalization: cyber security problems do not stop the raise of average application rating. In the previous chapters, we saw the trend that mobile banking is becoming more and more important for users, and therefore for banks, hence it can be assumed that for users technological development and improvement outweigh the disadvantages of risks, which reflects the growth of ratings. In both cases, we saw that cyber crime issues are not stopping the digitalization growth.

The **third research question** asked: what are the main methods and objectives of cyber attacks in the Russian banking sector and what are the regulator's measures of protection. The hypothesis states that the main methods of cyber attacks in the banking sector are social engineering and the use of malware, the main objectives are the people. The most effective cyber security methods which the regulator uses to protect banks are: improving the detection of fraudulent transactions by developing the information exchange system. Based on our key findings, we partially confirm the hypothesis. We will explain it further by dividing the hypothesis into three parts.

First, we are going to talk about the main methods of cyber attacks. Although, the percentage of unauthorized transactions due to the use of social engineering dramatically decreased in 2019, it remains the main reason of cyber crimes in this area (68%) (Figure 55). The same situation we can see with the attacks on the banks' infrastructure. Although attacks with the usage of malicious software was found in 58% of the observed banks, social engineering was also found in almost a half of the cases and it remains the main method of infiltration into banks. Since hymen are the weakest element in the banking security system, the majority of cyber attacks are started with social engineering. Even the most of internal network vulnerabilities (using dictionary passwords, storing sensitive data in a clear text, using the same credentials for different

accounts and others) are based on a human factor, and consequently they also can be vulnerable to social engineering. One of the main reasons of this weakness can be the low level of cyber literacy not only among users, but also among bank employees. Thus, we partially confirm the first part of this hypothesis.

Secondly, we are going to describe the main objectives of cyber attacks. The increase in the degree of security of information systems of credit organizations led to the fact that the focus of criminals shifted to social engineering attacks on clients and employees of the banks. Therefore, we confirm this part of hypothesis.

Third, we are focusing on the most effective cyber security methods which the regulator uses to protect the banks. We have found that the most common government measures are blocking fishing websites and conducting trainings to improve the cyber literacy of population and bank employees. Now Central Bank can only participate in blocking processes as an adviser but in the nearest future it is planned to make blocking fishing websites one of its direct functions. Although the main mission of Central Bank subdivision – FinCERT it is to compel banking organizations to keep records and exchange information about cyber incidents, one of the most important current tasks of it remains lowering the number of phishing websites. Hereby, we reject this part of the hypothesis.

In our work, we examined the relationship between digitalization and the profitability of the banking sector, as well as between cyber risks and digitalization. Further research could be done on making deeper analysis of the correlation between cyber risks and bank performance, which more likely requires the creation of cyber risk factor.

List of references

Ahmad, A. (2011): Financial Performance Evaluation of Some Selected Jordanian Commercial Banks, Seychelles:International Research Journal of Finance and Economics, (68), 50-63.

Alkhatib, A., Harsheh, M. (2012): Financial Performance of Palestinian Commercial Banks, International Journal of Business and Social Science, Vol. 3 No. 3; February 2012, 175-184.

Bank of England (2019): Future of finance. Review on the outlook for the UK financial system, June 2019, London/UK: Bank of England Publications, available at: https://www.bankofengland.co.uk/-/media/boe/files/report/2019/ future-of-finance-report.pdf (date of access: 01.08.2020).

Berger, A. N., Humphrey, D. B. (1997): Efficiency of financial institutions: International survey and directions for future research, Washington: Board of Governors of the Federal Reserve System, 10-16.

Boston Consulting Group (2020): Digitalization of the client way: how banks get customer trust and increase profits, available at: https://www.bcg.com/ru-ru/about/bcg-review/digitalization-client-way (date of access: 01.08.2020).

Bouveret, A. (2018): Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment, Washington: International Monetary Fund, International Monetary Fund working paper 18(143), 3-7.

Bsigroup (2005): SO/IEC 27001 International Information Security Standard published, available at: https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2005/11/ISOIEC-27001-International-Information-Security-Standard-published/ (date of access: 14.09.2020).

Central Bank of Russia (2012): On the requirements for ensuring the protection of information when making money transfers and on the procedure for the Bank of Russia to monitor compliance with the requirements for ensuring the protection of information when making money transfers, available at: https://cbr.ru/psystem/acts/382-p/_(date of access: 12.08.2020).

Central Bank of Russia (2012-2020): Monthly overview of the banking sector of the Russian Federation (internet version), available at: https://cbr.ru/statistics/bank_sector/review/ (date of access: 10.07.2020).

Central Bank of Russia (2017): The main directions of the unified state monetary policy for 2018 and the period of 2019 and 2020, available at: https://www.garant.ru/products/ipo/prime/doc/71708066/ (date of access: 10.07.2020).

Central Bank of Russia (2018a): Overview of the main types of computer attacks in the financial field in 2018, available at: http://regulation.nprts.ru/ru/upload/DIB_2018_20190704.pdf (date of access: 10.08.2020).

Central Bank of Russia (2018b): Overview of Unauthorized Funds Transfers for 2018, available at: https://cbr.ru/content/document/file/62930/gubzi_18.pdf (date of access: 12.08.2020).

Central Bank of Russia (2019a): Report of the Center for Monitoring and Responding to Computer Attacks in the Credit and Financial Sphere of the Information Security Department of the Bank of Russia, available at: https://www.cbr.ru/content/document/file/84354/fincert_report_20191010.pdf (date of access: 10.08.2020).

Central Bank of Russia (2019b): The main directions for the development of information security in the credit and financial sector for the period 2019 - 2021, available at: https://www.cbr.ru/Content/Document/File/83253/onrib_2021.pdf (date of access: 12.08.2020).

Central Bank of Russia (2019c): Overview of transactions performed without the consent of clients of financial institutions in 2019, available at: https://www.cbr.ru/Content/Document/File/103609/Review_of_transactions_2019.pdf (date of access: 28.09.2020).

Central Bank of Russia (2020a): Key Rate dynamics, 2012-2020, available at: https://www.cbr.ru/hd_base/KeyRate/ (date of access: 10.07.2020).

Central Bank of Russia reports (2020b): National payment system statistics, available at: https://www.cbr.ru/statistics/nps/psrf/ (date of access: 10.07.2020).

Chen, S. (2007): Application Denial of Service Is it Really That Easy?, OWASP Foundation, available at: https://owasp.org/www-pdf-archive/OWASP_IL_7_Application_DOS.pdf (date of access: 01.08.2020).

Cisco (2020): What Are the Most Common Cyber Attacks?, available at: https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html. (date of access: 17.08.2020).

Deloitte (2020): Cyber-risk assessment based on the organization's business objectives, available at: https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/risk/russian/Ocenka-kiberriskov-na-osnove-biznes-celej-organizacii.pdf (date of access: 10.07.2020).

Deloitte Digital (2019): EMEA Digital Banking Maturity 2018, January 2019, available at: https://www2.deloitte.com/content/dam/Deloitte/xe/Documents/financial-services/DBM-2018-EMEA-Story_ME_20190129.pdf (date of access: 04.07.2020).

Didenko, V. (2016): Effect of Digitalization Era on Banking Business Models, Moscow: Trade and economic journal, 3(2), 187-192.

Digital Banking Report (2016), available at: https://www.digitalbankingreport.com/trends/2016-retail-banking-trends-predictions/ (date of access: 10.07.2020).

Dolgushina, A. (2016): The evolution of banking services' types and models, Omsk: Publishing house finance and credit, 35-43.

Efron, B., Tibshirani, R. J. (1993): An introduction to the Bootstrap, Washington: Chapmann&Hall/CRC.

Eling, M., Wirfs J. H. (2016): Cyber Risk: Too Big to Insure? Risk Transfer Options for a Mercurial Risk Class, St. Gallen: Institute of Insurance Economics, 1-174.

European Banking Federation (2018): Banking sector performance, available at: https://www.ebf.eu/facts-and-figures/banking-sector-performance/ (date of access: 10.07.2020).

European Payment Council (2019): Payment Methods Report 2019. Innovations in the Way We Pay, Netherlands: ThePaypers, available at: https://www.europeanpaymentscouncil.eu/sites/default/files/inline-files/Payment%20Methods%20Report%202019 (date of access: 01.08.2020).

European Systemic Risk Board (2020): Systemic cyber risk, February 2020, available at: https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219 (date of access: 01.08.2020).

EY (2019): Global FinTech Adoption Index, April 2019, available at: https://www.ey.com/en_gl/ey-global-fintech-adoption-index (date of access: 01.07.2020).

Federal Law 'On banks and banking activities' (1990) № 395-1, available at: http://www.consultant.ru/document/cons_doc_LAW_5842/ (date of access: 05.07.2020).

Federal Law 'On the Central Bank of the Russian Federation (Bank of Russia)' (2002) № 86-FZ, available at: http://www.consultant.ru/document/cons_doc_LAW_37570/ (date of access: 05.07.2020).

Federal Law 'On the National Payment System' (2011) № 161, available at: http://www.kremlin.ru/acts/bank/33484 (date of access: 26.07.2020).

Federal Reserve Bank of New York (2020): Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis, Staff Report No. 909, January 2020, Revised June 2020.

Financial University under the Government of the Russian Federation (2017): Lecture material.

Forst, J. (2020): Introduction to Bootstrapping in Statistics with an Example. Statistics by Jim, available at: https://statisticsbyjim.com/hypothesis-testing/bootstrapping/ (date of access: 10.07.2020).

Garant (2020): Key rate and refinancing rate, available at: http://base.garant.ru/10180094/ (date of access: 10.07.2020).

Gartner Glossary (2020): Information Technology Glossary, available at: https://www.gartner.com/en/information-technology/glossary (date of access: 01.08.2020).

Gottlieb, J., Willmott, P. (2014): The digital tipping point: McKinsey Global Survey results, June 2014, available at: http://www.mcki nsey.com/business-functions /digital-mckinsey /our-insights/the-digital-tip ping-point-mckinsey -global-survey-results (date of access: 01.08.2020).

IDC (2020): IDC's Global DataSphere Forecast, May 2020, available at: https://www.idc.com/getdoc.jsp?containerId=prUS46286020 (date of access: 01.08.2020).

Infocenter (2020): Explanation of the Regression Model, available at: https://infocenter.informationbuilders.com/wf80/ (date of access: 10.07.2020).

ITU (2018): Global Cybersecurity Index (GCI), ITU Publications, available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (date of access: 01.08.2020).

ITU (2018): The ICT Development Index (IDI): conceptual framework and methodology and data, available at: https://www.itu.int/en/ITU-D/Statistics/Pages/publications/mis/methodology.aspx (date of access: 10.07.2020).

Kaplan, R.S., Norton D.P. (1992): The balanced scorecard - measures that drive performance. Harvard Business Review (January-February), 71-79.

Khizer, A., Muhammad, A., Hafiz, A. (2011): Bank-Specific and Macroeconomic Indicators of Profitability - Empirical Evidence from the Commercial Banks of Pakistan, Radford: International Journal of Business and Social Science, Vol. 2, 12-19.

Kosheev, V., Tsvetkov, J. (2018): Digital transformation of the banking sector, Ekaterinburg: Ural Scientific Center, 40-44.

Kotarba, M. (2017): Measuring digitalization – key metrics, Warsaw: Foundations of Management, Vol. 9 (2017), 123-138.

Kriebel, J., Debener, J. (2020): Measuring the Effect of Digitalization Efforts on Bank Performance, Muenster: SSRN Electronic Journal, 3-6.

Lukatsky, A (2007): ISO 27001 in Russia: fashionable and pointless published, available at: https://safe.cnews.ru/articles/iso_27001_v_rossii_modno_i_bessmyslenno/2 (date of access: 14.09.2020).

Markswebb (2020): Mobile banking rank (2012-2019), available at: https://markswebb.ru/report/mobile-banking-rank/ (date of access: 07.07.2020).

Mikhaylova, G. (2014): The "anonymous" movement: hacktivism as an emerging form of political participation, Texas: Texas State University.

MVideo&Eldorado Group (2019): Results of studying the demand for telecom over the past ten years (2010 - 2019), available at: https://www.tadviser.ru/index.php/smartphones_in_Russia (date of access: 10.07.2020).

Nataraja N. S., Nagaraja R. C., Ganesh L. (2018): Financial performance of private commercial banks in India: multiple regression analysis, Academy of Accounting and Financial Studies Journal, Volume 22, Issue 2, 2018, 1-12.

OECD (2014): Measuring the Digital Economy: A New Perspective, December 2014, OECD Publishing, available at: http://www.oecd.org/sti/measuring-thedigital-economy-9789264221796-en.htm (date of access: 01.08.2020).

OWASP **(**2020): community articles, available at: https://owasp.org/www-community/attacks/ (date of access: 01.08.2020).

Peixeiro, M. (2019): How Good is Your Model? — Intro to Resampling Methods, available at: https://towardsdatascience.com/how-good-is-your-model-intro-to-resampling-methods-2831e832042a (date of access: 10.07.2020).

Ross, J. A. (2020): Social Engineering, imperva community article, available at: https://www.imperva.com/learn/application-security/social-engineering-attack/ (date of access: 01.08.2020).

Sber (2020): What are mobile operators going to make money on?, August 2020, online publication, available at: https://sber.pro/publication/kak-razvivaet-ekosistemy-rossiiskaia-bolshaia-troika (date of access: 01.08.2020).

Shah S., Jan R. (2013): Analysis of Financial Performance of Private Banks in Pakistan, World Conference On Business, Economics And Management - WCBEM2013, Social and Behavioral Sciences 109 (2014), 1021-1025.

Soramäki, K., Bech, M., Arnold, J., Glass, R. J., Beyeler, W. E. (2007): The topology of interbank payment flows, Physica A: Statistical Mechanics and its Applications, 2007, vol. 379, issue 1, 317-333.

Statista (2020): Technology & Telecommunications graphs, available at: https://www.statista.com/statistics/467166/ (date of access: 10.07.2020).

Tadviser (2020): Phishing, available at: http://tadviser.com/index.php/Article:Phishing_(phishing) (date of access: 30.09.2020).

The PCI Security Standards Council (2018): PCI DSS Quick Reference Guide, available at: https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf (date of access: 28.09.2020).

Tjournal (2020): The user found that passwords in the Sberbank application are not case sensitive, available at: https://tjournal.ru/flood/209189-polzovatel-tj-obnaruzhil-chto-paroli-v-prilozhenii-sberbanka-ne-chuvstvitelny-k-registru (date of access: 28.09.2020).

UNCTAD (2013): Information Economy Report 2013: The Cloud Economy and Developing Countries. Geneva: United Nations, available at:

http://unctad.org/en/PublicationsLibrary/ier2013_en.pdf (date of access: 01.08.2020).

Vennet, V. (1998): Cost and profit dynamics in financial conglomerates and universal banks in Europe, Frankfurt: SUERF/CFS Colloquium, 15-17.

Woolridge, J. M. (2013): Introductory Econometrics: a modern approach (fifth edition), Mason: South-Western Cengage Learning.

World Bank (2010): Banking Sector Competition in Russia, Policy Research Working Paper 5449, available at: https://openknowledge.worldbank.org/handle/10986/3932 (date of access: 01.08.2020).

World Bank (2016): World Development Report 2016: Digital Dividends, Washington: World Bank Publications, available at: https://www.worldbank.org/en/publication/wdr2016 (date of access: 01.08.2020).

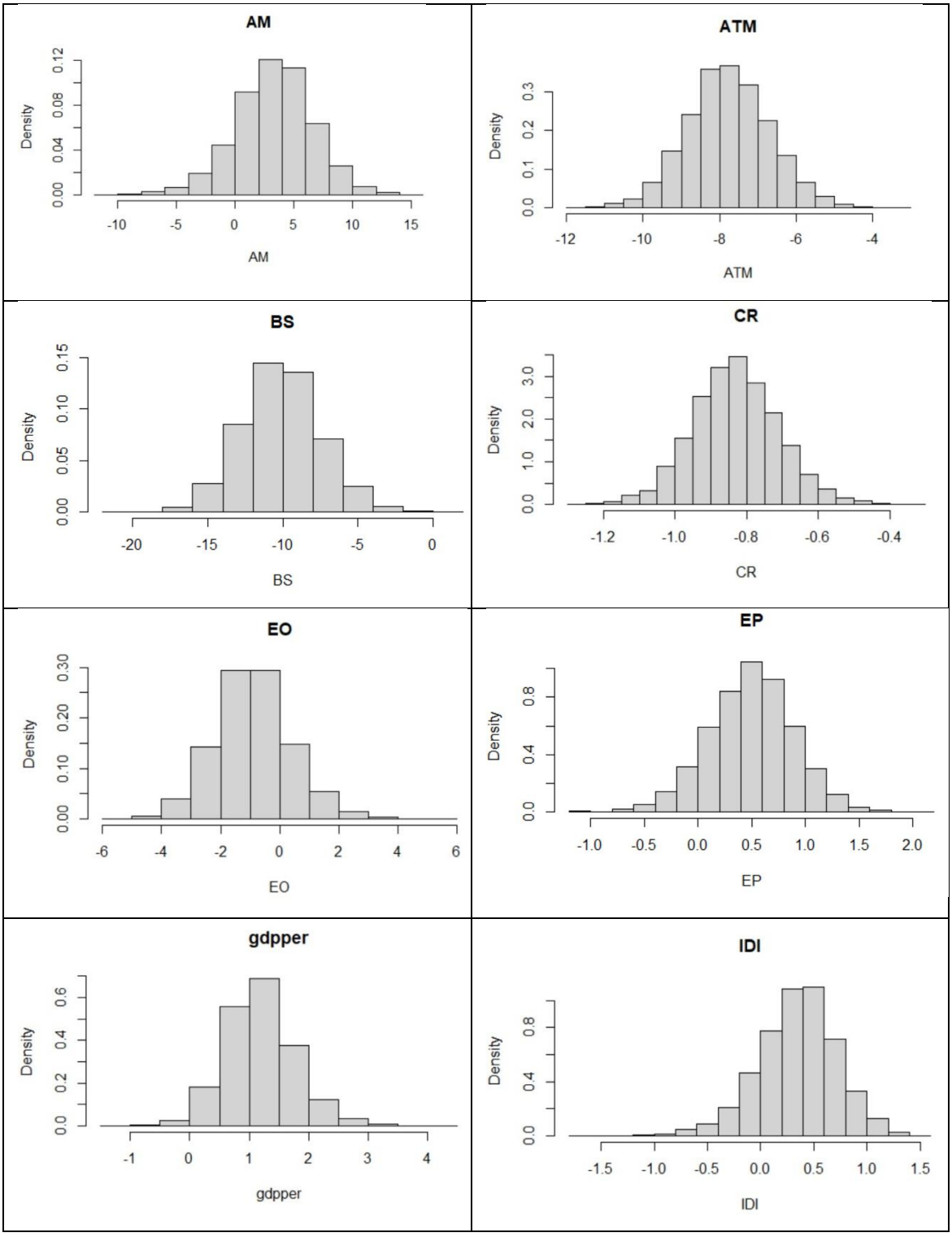
World Bank (2017): Discussion Paper 'Digital Economy Concept, Trends and Visions: Towards a Future-Proof Strategy', December 2017, Washington: World Bank Publications, available at: http://pubdocs.worldbank.org/en/513361482271099284/Digital-Economy-Russia-Discussion-paper-2016-12-20-eng.pdf (date of access: 01.08.2020).

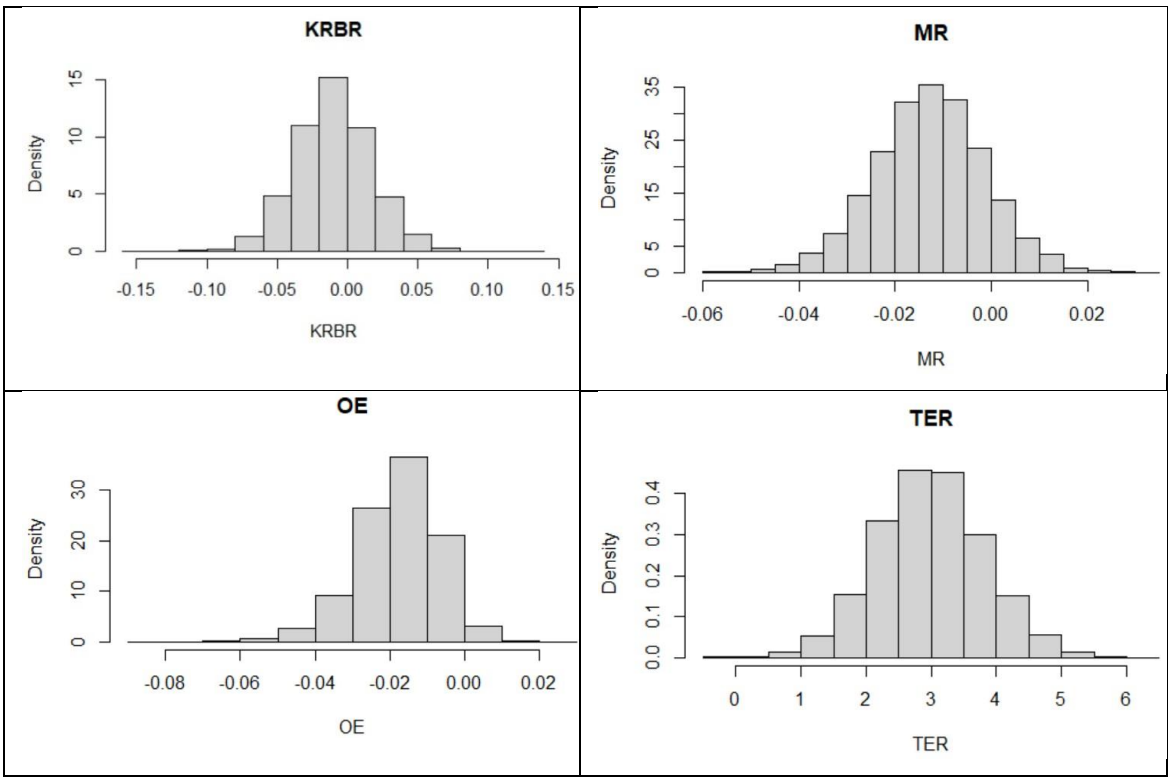
World Bank (2018): Implications for Russia, digital economy report, September 2018, Washington: World Bank Publications, available at: https://www.worldbank.org/en/country/russia/publication/competing-in-digital-age (date of access: 01.08.2020).

Zhang, T. (2018): Digitization of Money and Finance: Challenges and Opportunities, Speech for Atlanta Federal Reserve Bank Conference, available at: https://www.imf.org/en/News/Articles/2018/05/08/sp050818-digitization-of-money-and-finance-challenges-and-opportunities (date of access: 01.08.2020).

Appendix 1:

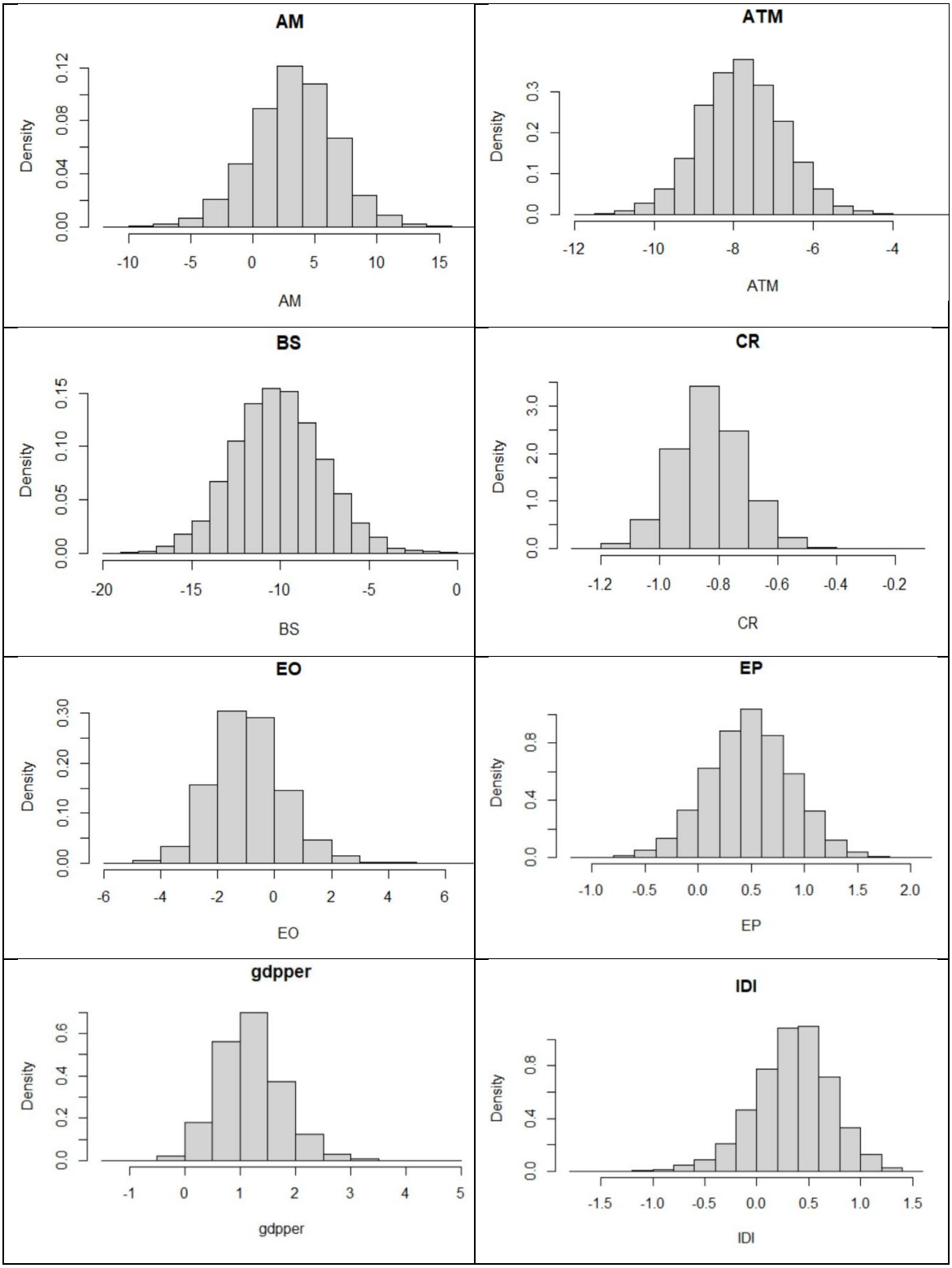
The distribution of the parameters after bootstraping the regression 1 with ROA as dependent variable

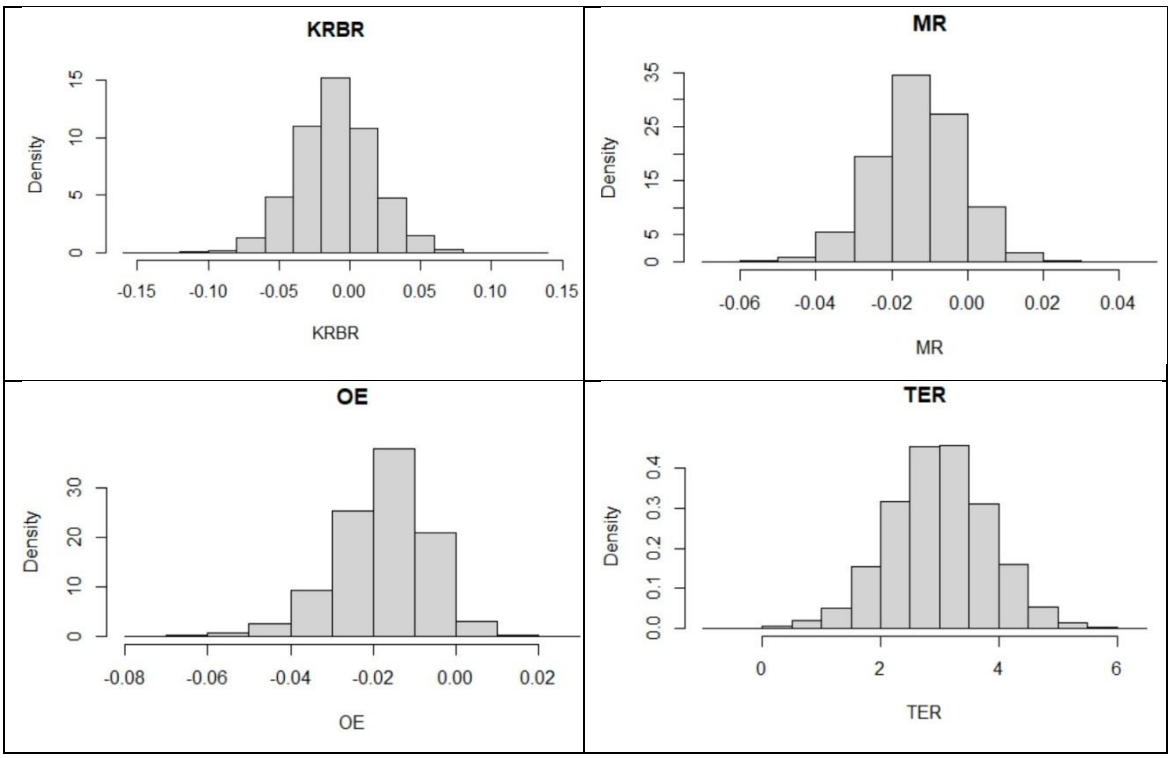



KRBR
Density
0
5
10
15
-0.15
-0.10
-0.05
0.00
0.05
0.10
0.15
KRBR
MR
Density
0
5
15
25
35
-0.06
-0.04
-0.02
0.00
0.02
MR
OE
Density
0
10
20
30
-0.08
-0.06
-0.04
-0.02
0.00
0.02
OE
TER
Density
0.0
0.1
0.2
0.3
0.4
0
1
2
3
4
5
6
TER

Appendix 2:

The distribution of the parameters after bootstraping the regression 2 with ROE as dependent variable




KRBR
Density
0
5
10
15
-0.15
-0.10
-0.05
0.00
0.05
0.10
0.15
KRBR
MR
Density
0
5
15
25
35
-0.06
-0.04
-0.02
0.00
0.02
0.04
MR
OE
Density
0
10
20
30
-0.08
-0.06
-0.04
-0.02
0.00
0.02
OE
TER
Density
0.0
0.1
0.2
0.3
0.4
0
2
4
6
TER