September 2019

Analytical survey

ASSOCIATION OF BANKS OF RUSSIA

Russian banking system today

Interaction of real and financial sectors in terms of digitalization of the economy

CONTENTS

1. Modern trends in interaction between real and financial economies 4

1.1. «The fourth industrial revolution» and major ways forward for the global economy 4

1.2. Conditions and drivers for transition of the russian economy to a pathway to innovative growth 10

2. Role and significance of the banking system in promotion of digital technologies and boosting of the russian economy growth 18

2.1. Position of banks in the financial Intermediation system and their role in digital transformation of the community 18

2.2. Current trends in landing of the real economy 20

3. Digitalization of society and a new framework of interaction between the real and financial sectors of economy 31

3.1. Financial technologies as drivers for digitalization of economy and social sphere 31

3.2. Transformation of banking at the digital age 33

3.3. Ecosystems as a new format of interaction between the real and financial sectors of economy 41

4. Cyber threats and information security: problems and solutions 48

4.1. The scale of cybercrime in economy sectors and spheres 48

4.2. Information security threats in the digital space: current situation review 52

4.3. Biometric identification and the practical aspects of its use 56

4.4. The main challenges of cyber security 60

5. Development of regulatory environment for the banking activities in transition to digital technologies 66

5.1. Current tasks faced by the incentive-based regulation 66

5.2. Regulatory and oversight technologies under digitalization of the financial sector 73

5.3. Practical issues of competition in banking sector under digitalization 79

5.4. Fostering an trust environment as the driver of banking digitalization 82

1

Modern trends in interaction between real and financial economies

1.1. «The fourth industrial revolution» and major ways forward for the global economy

- *The present time sees the development of major digital ways forward for the global economy for a long time to come. The pace, timeframe and completeness are however not set automatically for the delivery of digital civilization benefits.*
- *The current situation in the global economy demonstrates the decaying cyclical upswing potential and growing protectionism. The world, in general, experiences the decline in business and investment activities.*
- *Vague prospects of the global economy development are largely due to persisting global imbalances and a high level of the leading world economies' public debt.*
- *A trade policy truce achieved at the moment is too fragile and can most likely break down, taking its toll on the other sectors, specifically, software applications and automotive industry.*

We now take it for granted that the key determinant for the way real and financial economies will interact in the long term will be an increasingly deepening penetration of digitization into various business and economic sectors. «Disruptive» technologies, such as these of Internet of things, analysis of data bulks, quantum calculations, artificial intelligence, blockchain, robototronics and other such technologies, are setting up the conditions for the transition to digital ecosystems, new management and accounting methods that fundamentally change not only the business models but also the forms in the which the life of community, and operation of government and governmental bodies are organized.

The first industrial revolution began with invention of the steam engine followed by the transition from manual to machine-aided labour. The second relied on the electric traction and opened up the age of mass production. The third introduced automatics into the production process, aided by electronics and information technologies. The Fourth Industrial Revolution (Industry 4.0. Society 5.0) is a digital age in the history of mankind, the period erasing boundaries between physical, virtual and bio technologies.

A 'platform' paradigm underlying the digitization gave rise to emergence of fundamentally new ways forward for the global economy, only shaping up at the moment, but given the favourable geopolitical environment, eventually determining its development.

Firstly, the integration of cyber-physical systems into the plant processes will free the latter from any human involvement. Profit centres will continue to shift from production stages to R&D and design focuses. Improving conditions for development of start-ups and spread out of 'fluid' employment will be conducive to strengthening of inclusivity which will multiply the new global value-added chain creation processes. Digitalisation and access to data bulks will exponentially extend the opportunities for customisation of goods and services, accounting for customer individual specifics and, using these two as a basis, transition to a client-oriented business model.

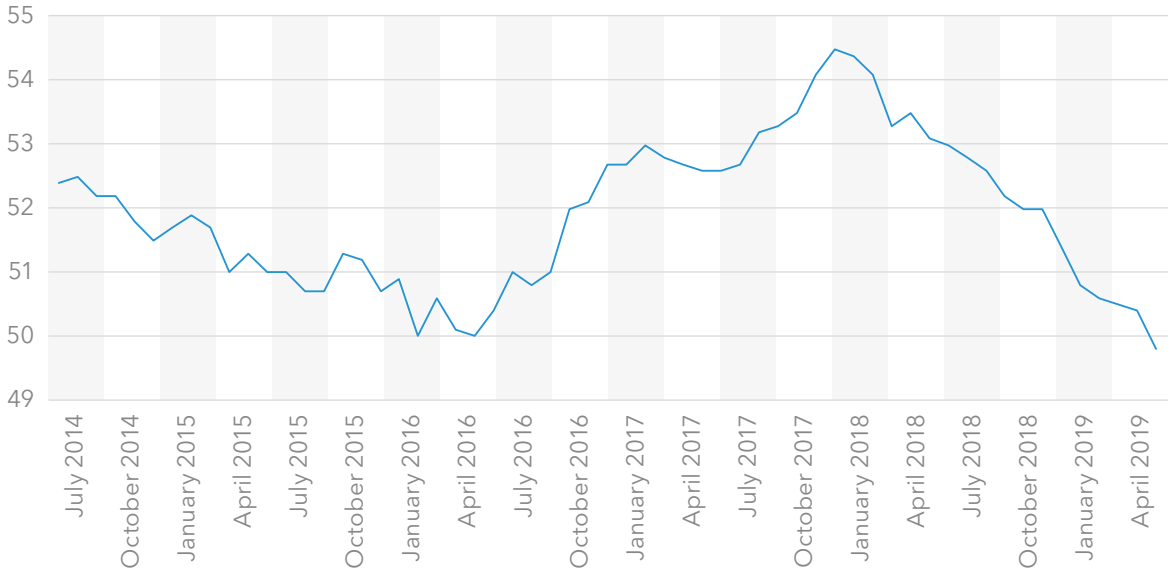
Secondly, the development of cyber-financial space and building of e-commerce platforms (marketplaces) will also fundamentally change its architecture and operational environment. Instead of using the conventional access channels via financial intermediaries, the companies and individuals will be able to build their relationships via the online access platforms, thus decreasing the number of intermediary links separating financial service providers from service receivers. A trend from interaction between real and financial economies to their integration will take shape based on digital ecosystems. Hybrid financing forms will be dominating the market. At the same time, alternative financing methods, such as crowd funding and crowd-investing and especially, crowd-lending, will get further development.

Thirdly, as information is becoming a key asset of the digital economy there is a necessity, on the one hand, in creating conditions for data free flow and, on the other hand, in protecting data from cybercrime. The solution of these inter-related problems requires coordination of actions between all countries and creation of a relevant institutional environment set out in international treaties.

The pace, timeframe and completeness are not automatically set for the delivery of digital civilization benefits. Scenario conditions for the development of 'platform' technologies are still very controversial, being greatly influenced by the current situation in the global economy that keeps demonstrating decaying cyclical upspring potential, which first commenced in 2016–2017, and further shift of risk balances towards the decline. Short-term forecasts from international financial institutions and leading analytical centres suggest more conservative, if not pessimistic conclusions.

Main threats are attributed to a possible failure of US-China negotiations regarding the trade warfare termination, no-deal Brexit as well as an increase in the share of corporate bonds rated below the investment-grade (in developed economies) and a continuing trend towards the increase in the corporate sector's external debt (in emerging-market countries). Such conditions amplify the probability for a decline in the global investment activity that has reached its three-year minimum as it can be seen from the current PMI behaviour. The IMF forecast suggests that by the end of 2019, 70% of the global economy will experience the slowdown in the growth rate.

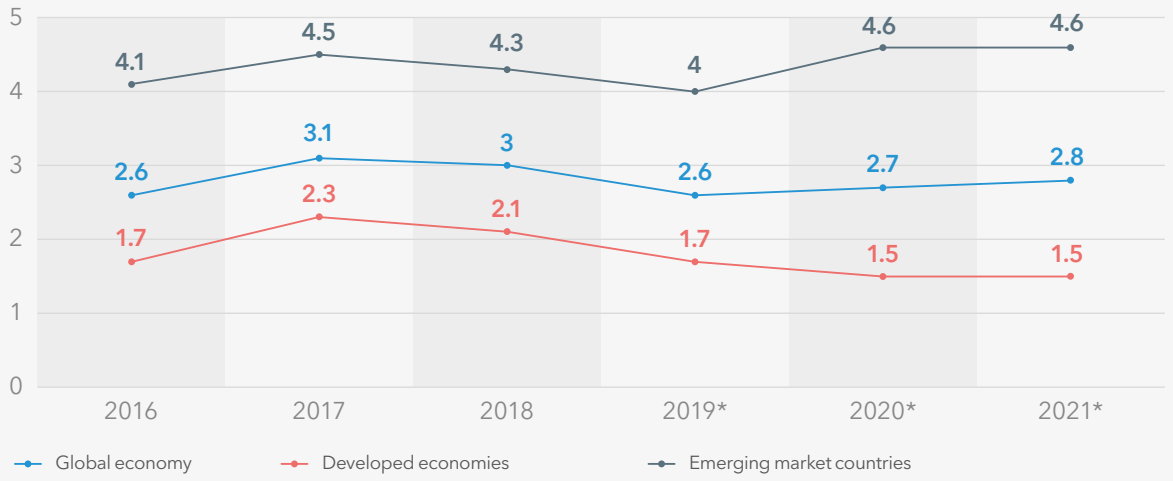
Purchasing managers' index (PMI) in global perspective



Source: http://www.marketeconomics.com/

Mid-term forecasts of the global economy development prove its inertial trend. Developed economies are expected to retain the growth at a level close to the potential due to ageing of the population and low rates of the factor productivity increase. Mind that a number of such countries are now passing through the technical recession. For emerging market countries, the macroeconomic trend is now at some sort of a plateau when economic growth rates are stabilized at a level that makes it impossible to ensure employment of the population and the rise in the standard of living in full measure. A decline in the Chinese growth rate is a matter of a particular concern.

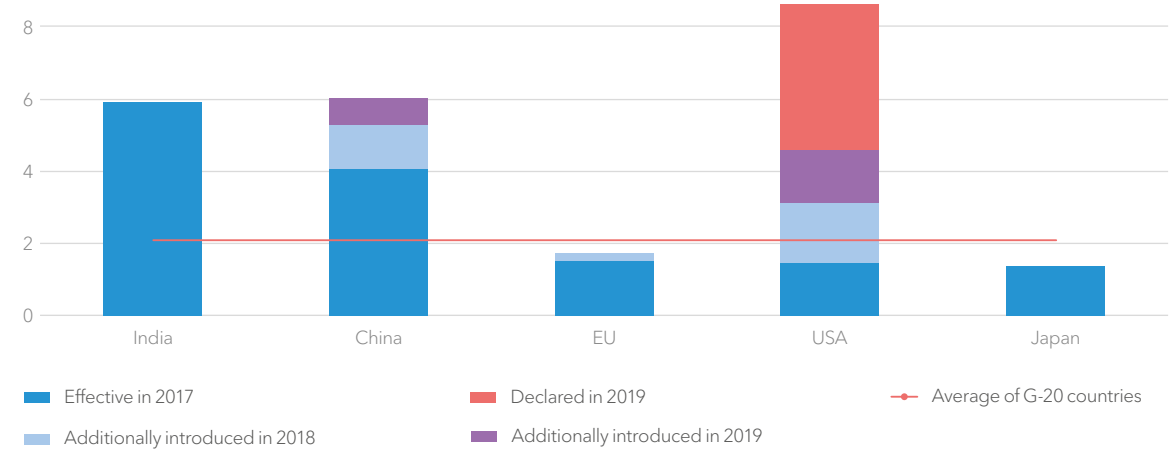
Trend in global production by countries' groups, %



Source: The World Bank, Global Economic Prospects. June, 2019

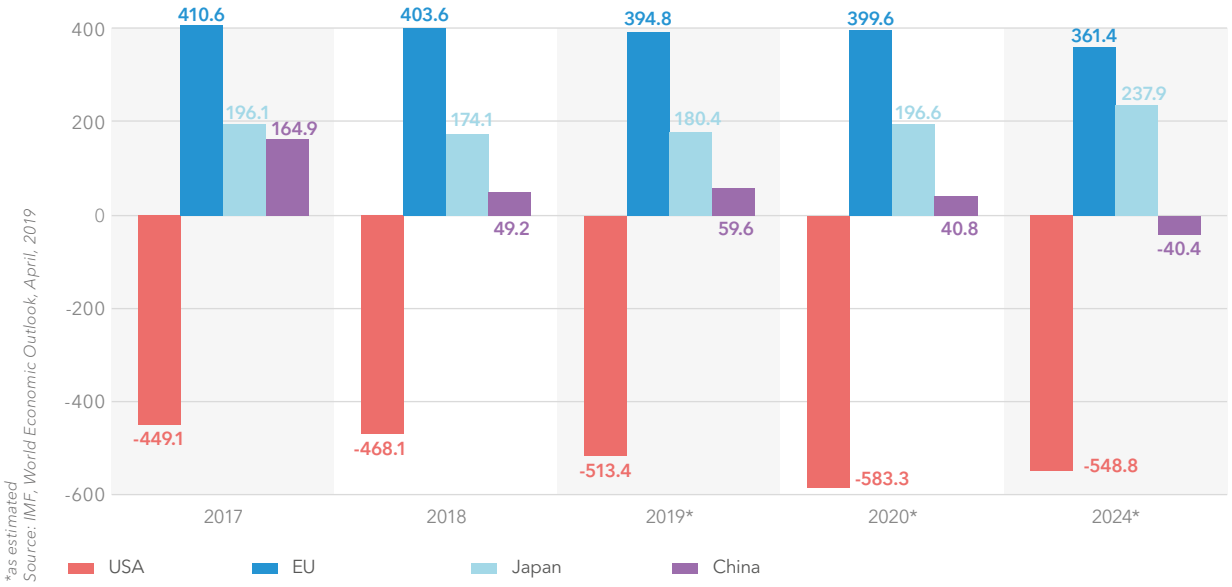
Vague prospects of the global economy development are largely due to persisting global imbalances and a high level of the leading world economies' public debt. An internal-external rebalancing task declared by IMF in 2010 is yet to be completed. Global imbalances, in a concentrated form reflected specifically in the current account balance behaviour, continue to reproduce. This gives rise to a tension between the countries in trade competition and causes some of them to take protectionist measures disrupting the global economic order established by WTO and other international treaties.

Average import duties in G-20 countries, %



Source: The World Bank, Global Economic Prospects, June, 2019, p. 6

Current account balance behaviour in countries major global GDP contributors, billion US dollars



*as estimated
Source: IMF, World Economic Outlook, April, 2019

A US-China trade row commences in January 2018 when US dramatically increases tariffs on imported solar cells and certain washing machines. China responds by increasing tariffs on US food imports. In July and August 2018, USA and China introduce new duties on import of goods against each other, totalling 50 billion US dollars for each of the contenders. In 2018, USA announces establishing additional duties on Chinese imports in the amount 200 billion US dollars for which China responds by introducing duties on imports totalling 60 billion US dollars.

In December 2018, on the G-20 summit in Buenos Aires, US and China leaders agree to a ninety-day truce refraining from increasing tariff rates for the duration of negotiations. In May 2019, a new round of trade war however begins. USA increases tariff rates on Chinese imports totalling 200 billion US dollars, from 10% to 25%, and threatened imposition of another 300 billion. If this threat is ever met, almost all Chinese imports would fall victim to high tariffs. China responds by introducing a 60 billion US dollar import duties on US goods.

In May 2019, USA also introduces an emergency regime for protection of the country's telecommunication systems, blacklisting Huawei as the national security threat. All blacklisted companies are barred from purchasing US technology without Washington's permission.

On the G-20 meeting in Osaka in July 2019, USA and China leaders agree to freeze the conflict and continue negotiations.

By the time the first round of US-declared trade war began, import duties in USA, Japan and EU countries were below the average level of the G-20 countries. After being twice increased, the level of US import duties exceeded not only Japanese and European figures but also the overall G-20 average. If US and China leaders had failed to reach a trade war truce agreement on Osaka G-20 summit in June 2019, US import duties would have now been higher than those of China and India.

However, even without this undelivered threat the current account balance behaviour forecast prepared by IMF shows that China will see degradation of the current account balance within the nearest five years to come. Bearing in mind that Chinese economic model is still in the process of rebalancing from external to internal demand, a certain decline in the country's GDP growth rate may be expected.

Some forward-looking American political scientists recognize that any confrontations in the system of international economic and financial relations lead down to a blind alley which may then take boomerang effect. One of the most prominent of them, Richard Haass, believes that the United States needs to accept special obligations in the economic realm given the role of the dollar as the world's de facto reserve currency...Regular, serious consultations between the Federal Reserve and its central bank counterparts around the world are essential. Trade disputes should be taken to the WTO rather than acted on unilaterally, as well./ Richard N. Haass, A World in Disarray: American Foreign Policy and the Crisis of the Old Order, Moscow, AST Publishing, 2019, p. 239/

Overall, a trade policy truce achieved between the major contributors to the world's production is too fragile and can most likely break down, taking its toll on the other sectors, specifically, software applications and automotive industry. It is not unlikely that exchange rate manipulations will also be on the world's agenda. In the meantime, a G-20 Leaders' Declaration from Osaka summit refers to a chance that an agreement can be reached and the Clause 8 deems it appropriate to undertake a WTO reform.

According to the IMF forecast,

70%

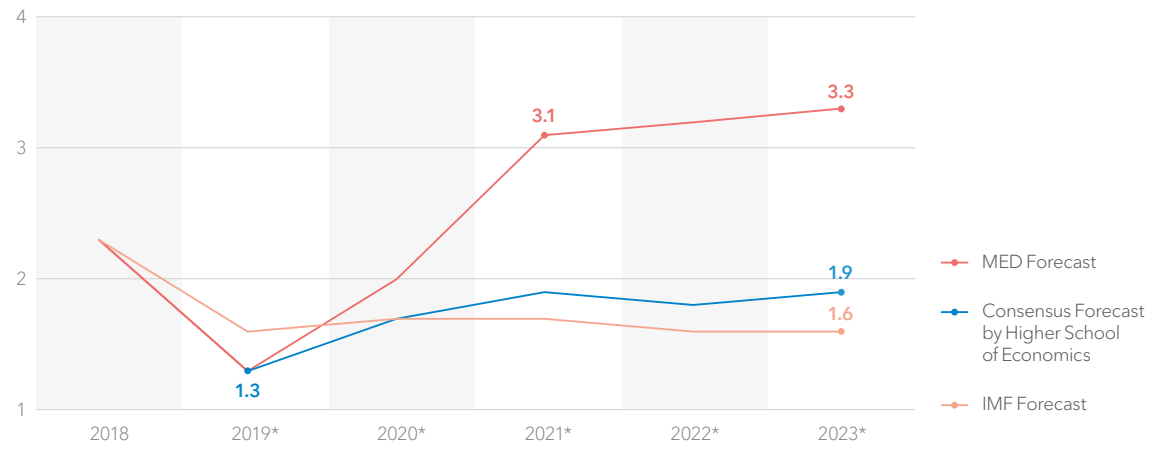
of the global economy will show a slowdown in growth based on the 2019 results

1.2. Conditions and drivers for transition of the russian economy to a pathway to innovative growth

- *At the end of the first half of 2019, the Russian GDP trend is in the zone close to 'technical' recession and even stagnation. There is a consensus in most mid-term forecasts that the economy's growth rate will not exceed 2-3% a year. The actual output will be constrained by the narrow bounds of domestic savings and the population's real income growth.*
- *Government support can only partially help in stimulating the investment activity. Hence, the priority is currently given to establishing transparent conditions for the state-private partnership and the comfort conduct of business.*
- *Currently, we can see favourable conditions for the transition from the moderately tough to neutral monetary policy. Unless any dramatic deterioration of external conditions take place for the Russian economy, the Bank of Russia key rate will be at 6.75-7.0% by early 2020 with a potential for decreasing further down to 6.0-6.5% over the year.*
- *The main reason behind the Russia's sagging business activity lies in internal rather than external factors, both of cyclical and institutional origin. For variety of reasons, Russia is dominated by 'paternalistic' rather than 'inclusive', i.e. based on the 'open access arrangement', model of the community business life organisation. Meanwhile, the success of transition to the innovative development will directly depend on how actively the business environment stimulating a taste for investments and assumption of reasonable risks will be created.*
- *'Disruptive' technologies underlying a foundation for digital transformation in economic and social life are closely linked with transition to the inclusive growth model. One of principal conditions for delivering the benefits of this model is the creation of a comfortable investment environment.*

After an accelerated GDP growth rate demonstrated as of the end of 2018 (compare 2.3% versus the predicted 1.7%), that was partially accounted for the revision of the methodology and update of statistical data by Rosstat, the Russian economy of the first half of 2019 shown a close to zero, albeit positive, growth trend. The analysis of data for the first six months of 2019 allows to make an annualized estimation for the GDP growth at around 0.8–1.0% (mainly due to the industrial production increase). This means that with account taken of statistical errors, the Russian economic growth returned to the values that can be described as close to 'technical' recession and even stagnation.

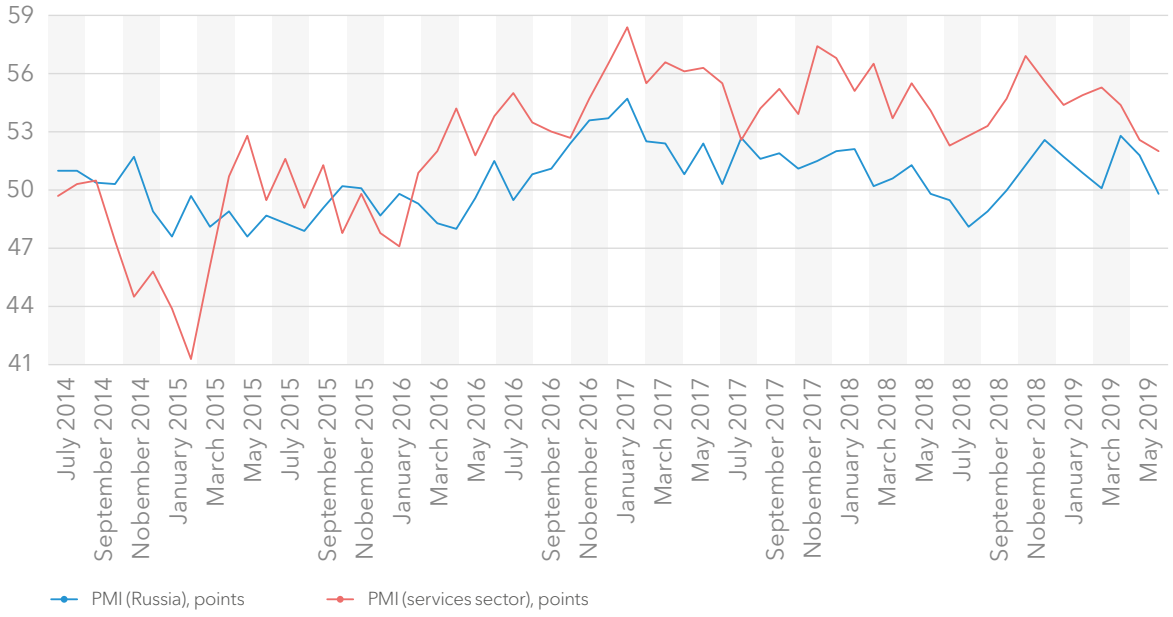
Mid-term forecast of GDP trend, %



Source: Scenario conditions for the forecast of 2019-2024 socioeconomic development, Ministry of Economic Development, April 2019; Comments on the State and Business, No.210, 2019; Centre of Development, Higher School of Economics; IMF, World Economic Outlook, April, 2019

There is a consensus in most forecasts, except for those in the RF Ministry of Economic Development, that the next years will see a two-fold decrease in the Russian economy's growth rate against the world average figures. IMF, World Bank, OECD and leading analytical centres' experts give close figures for the period until 2024. According to the Bank of Russia estimates, provided that national projects are successfully delivered, the active budget expenditure policy is implemented and the global hydrocarbon prices remain at the existing level, the expected loosening of monetary policy may increase the growth rate to 2–3% by 2021. A net export increase will not have any serious impact. The actual output will be constrained by the narrow bounds of domestic savings and the population's real income growth.

Purchasing managers' index PMI (Russia as a whole) and PMI (services sector), points



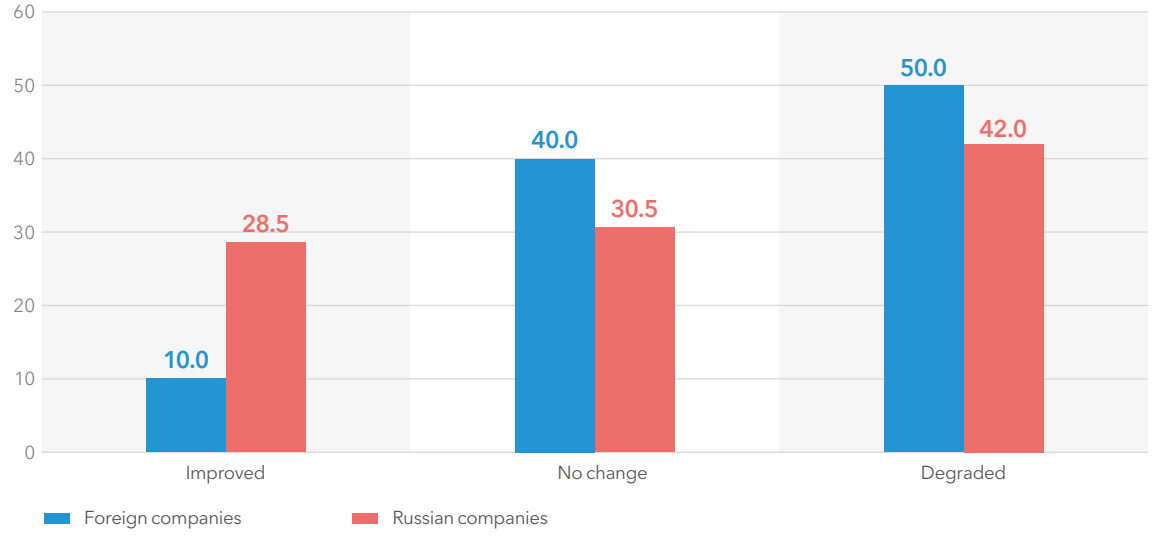
Source: http://www.marketeconomics.com/

Capital investments are one of the key drivers of economic growth. Over the past five years, Purchasing Managers' Indices remain at the low level. As at the end of Quarter 1, 2019, the growth of capital investments decelerated down to 0.5% in annualized figures. The decelerated investment activity was the result of poor growth in its operative indicators, such as the volume of construction works, investment imports and production of domestic engineering products of investment use.

Government support can only partially help in stimulating the investment activity. A launch of a 26 trillion RUB worth national project programme will definitely create drives for the revival of investment and consumer demands and solution of priority issues in the country's economic and social development. An amount of 18 trillion roubles is expected to be allocated from the budget sources while 7.5 trillion roubles will be attracted from off-budget sources. The execution timeframe and efficiency will be largely determined not by the hard management style but rather by establishing transparent conditions for the state-private partnership and the comfort conduct of business.

Worthy of note in this respect are the results of businessmen's polling contained in the Russian Union of Industrialists and Entrepreneurs' Report "On the State of Russia's Business Environment". A regular 2018 polling of RUIE's member companies demonstrated a certain decline in the estimation of business environment against 2017. The polling of Russian and foreign investors shown that the share of respondents noting degradation of the Russian business environment has increased against 2017 irrespective of the capital origin country. At the same time, 28.5% of Russian companies believe that the business environment has improved while only 10% of foreign respondents gave the same answer.

Changes in the Russia's business environment in 2018: as seen by Russian and foreign companies



Source: On the State of Russia's Business Environment in 2018, RUIE's Report, Moscow, March 2019, p. 109

While the physical GDP volume shows poor growth rate, an improvement in the financial sector is seen. From Quarter 2, 2019 and on, a decelerated inflation trend becomes sustainable. While mid-term risks of an upward inflation deviation from the target level still dominate, inflation expectations have stabilized in the current period. This allowed the Bank of Russia to go down with the 2019 annualized inflation forecast to 4.2–4.7%, further reaching the close-to-the-target level of 4% for 2020. Currently, we can see favourable conditions for the transition from the moderately tough to neutral monetary policy. Unless any dramatic deterioration of external conditions takes place for the Russian economy, which looks very unlikely at the moment, the Bank of Russia key rate will be at 6.75-7.0% by early 2020 with a potential for decreasing further down to 6.0–6.5% over the year.

The budget sector performance demonstrates positive changes. At the end of the first half of the current year, the federal budget surplus increased almost twice against the same period of 2018, exceeding 1.5 trillion roubles (3.1% of the GDP). At the same time, a considerable budget surplus is partially accounted for the fact that a number of budget payments are scheduled for the year end.

Non-petroleum revenues demonstrated faster growth which made it possible to decrease the non-petroleum shortfall. The share of non-petroleum revenues reached 56.8% of the overall federal budget revenues. The number of Russia's subsidized regions has decreased. A decrease in the revenue on federal loan bonds against the increasing volume of their flotation is seen.

Key parameters of the federal budget performance, billion roubles

	1st Half 2018	1st Half 2019	% y/y
Revenues	8,627	9,548	10.7
% of GDP	18.3	18.7	
Expenditures	7,751	7,987	3.0
% of GDP	16.4	15.7	
Surplus/shortfall	875	1,561	78.3
% of GDP	1.9	3.1	

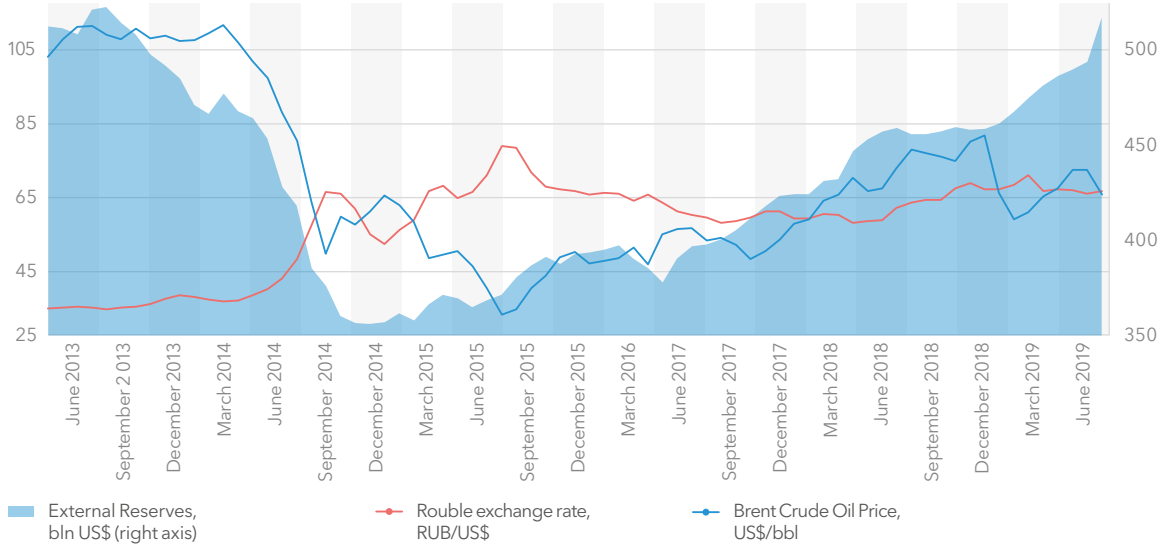
Balance of petroleum and non-petroleum revenues, billion roubles

	1st Half 2018	1st Half 2019	% y/y
Petroleum revenues	3,935	4,122	4.8
% of GDP	8.3	8.1	
% of revenues	45.6	43.2	
Non-petroleum revenues	4,692	5,426	15.7
% of GDP	9.9	10.7	
% of revenues	54.4	56.8	
Non-petroleum shortfall	(-) 3,060	(-) 2,561	(-) 16.3
% of GDP	(-) 6.5	(-) 5.0	

Source: Ministry of Finance of the Russian Federation

Thanks to the fiscal rule, the Russian economy and state finances are becoming less dependent on fluctuations in global energy prices. Generally favourable energy market conditions attained in 2016 made it possible to increase the external reserves of the Russian Federation which had exceeded an important benchmark of 500 billion US dollars by mid 2019. The purchase of the foreign currency in the domestic currency market by the RF Ministry of Finance through the Bank of Russia contributes to the growth of National Welfare Fund reserves and prevents the rouble exchange rate from excessive appreciation.

External reserves of the Russian Federation, billion US dollars



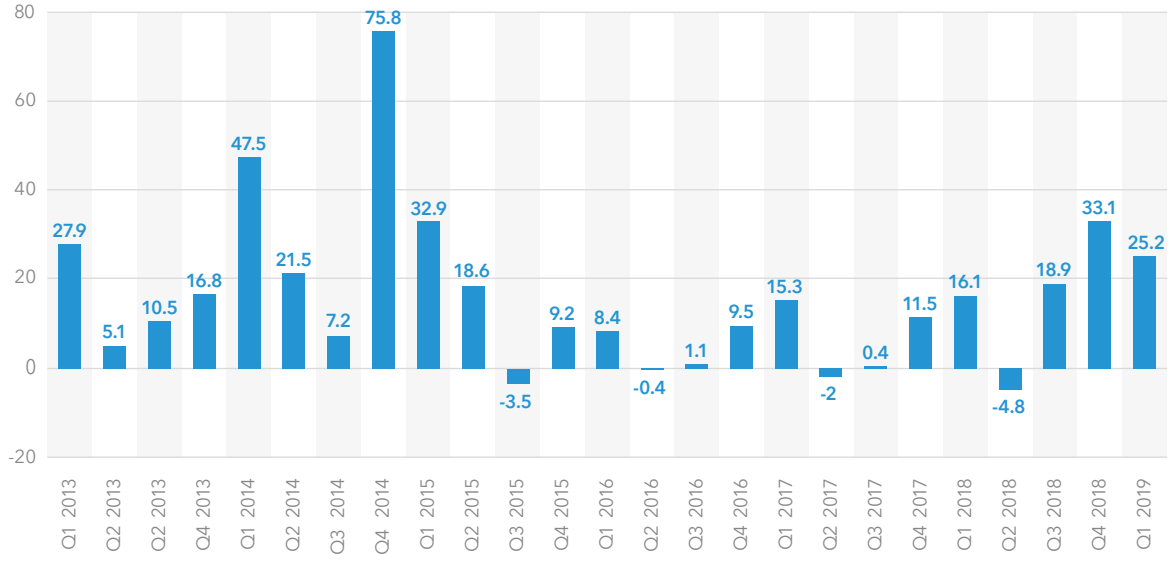
Source: Bank of Russia

Consequently, external conditions, even under pressure of sanctions, tough monetary conditions and budget constraints are not to blame for the low growth rate of the Russian economy. Mostly internal, both cyclical and institutional, rather than external factors are the main reason behind the Russia's sagging business activity. And it's not about the Russian economy being resource-based, although this adds to the dependence from external shocks and makes extended reproduction more capital consuming. The world's experience shows that a number of countries are successfully using the 'oil curse' to raise the performance of national economies.

Importantly, for variety of reasons, Russia is dominated by 'paternalistic' rather than 'inclusive', i.e. based on the 'open access arrangement', model of the community business life organisation. Meanwhile, the success of transition to the innovative development, that amongst other things prioritises digitisation of the community's economic and social life, will directly depend on how actively the business environment stimulating a predilection for investments, assumption of reasonable risks and removal of inefficient business entities from the market will be created.

Only by diversification of funding sources can we successfully accomplish the task of the flow of capital and input of skills into high value-added and high factor productivity innovative sectors. The modern world's constraints of the domestic-financed capital formation can be overcome by attracting foreign investments and undertaking unconventional (alternative) forms of financing. In this, Russia however lags behind many emerging market countries. What is more, over the past two years Russia is experiencing a steady trend towards net outflow of capitals that cannot be attributed to purely technical reasons (debt management and repayment, transfer of funds, capital transfers and so on).

Financial operations of the private economy
(up to december 2018 – net capital import/export by the private economy), billion US$



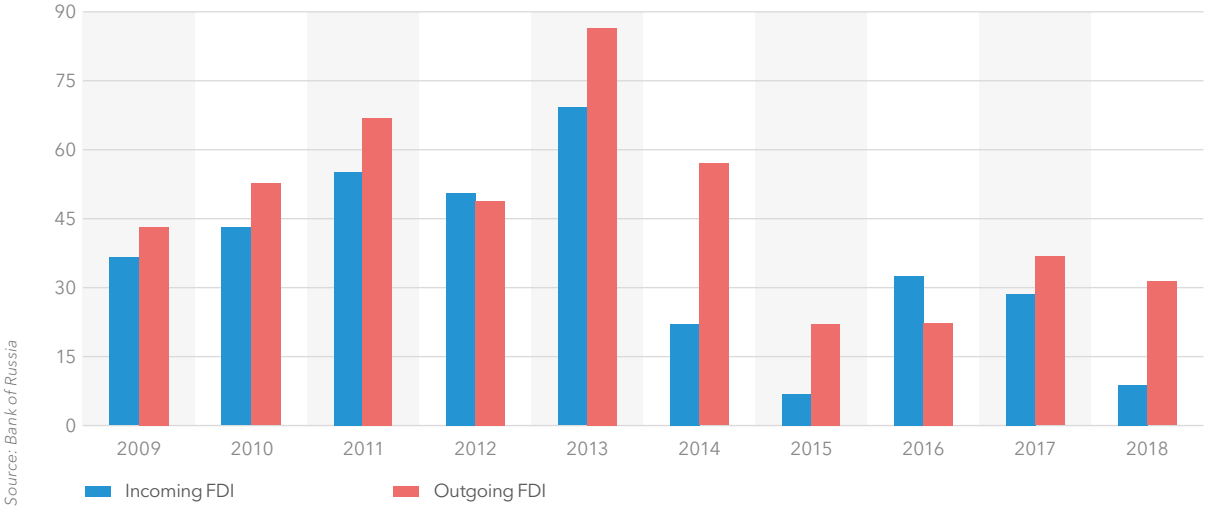
Source: Bank of Russia
«+» – net lending (earlier, capital exports),
«–» – net borrowing (earlier, capital imports).

While in late 2014 – early 2015 net export of capital from Russia could be considered as a natural reaction to the acute phase of currency crisis and introduction of economic sanctions, after 2016 this process has become indicative of the investment environment condition. A considerable decline in the foreign direct investment (FDI) flows starting from 2014 speaks in favour of this. Moreover, only in 2016 the amount of incoming FDI flows exceeded outgoing flows.

by mid-2019 Russia's international reserves exceeded

> $500 bln

Foreign direct investment flows in Russia in 2009-2018, billion US$



Source: Bank of Russia

'Disruptive' technologies underlying a foundation for digital transformation in economic and social life are closely linked with transition to the inclusive growth model. One of the principal conditions for delivering the benefits of this model is the creation of a comfortable investment environment. Russia now needs to keep actively moving on its pathway continuing already-commenced structural and institutional reforms. The protection of private property (including that from illegal seizure) and minority rights, independent court proceedings on business disputes, development of the codes of conduct by Russian businesses, development of self-regulation, establishment of an environment of trust and conditions for fair competition, all these make only a part of a list of priority issues waiting for its resolution.

For the sake of fairness, it is worth noting that in recent years, governmental bodies of the Russian Federation take steps to improve the country image in most often quoted international organisations' ratings. A comparative analysis of business environments published in a World Bank's annual study of «Doing Business» is a leading publication amongst them. An Ease of Doing Business Ranking published in this annual and based on measuring aggregated data from 10 topics with each consisting of several indicators is one of the most unbiased and trustworthy descriptions of the investment environment condition and changes. Taking 2011 as reference year, by May 2018 Russia had lifted up from 124th to 31st position, leaving behind such countries as China and India. At the same time, one should not overestimate this data. A higher position, or rank, means that the country's regulatory environment is more conducive to opening and doing business. This however in no way means that such conditions are fully established in practice. What is more, this rating mainly covers small sized and medium sized businesses working in nonfinancial sectors. It fails to take into account the condition and structure of the financial credit system and reflects situation in only one city ('the country's largest business centre').

A popular rating published by the World Economic Forum (WEF) (Global Competitiveness Index) uses 98 indicators and 12 competitiveness pillars. The 2018 ranking places the Russian Federation on the 43rd place amongst the 140 countries of the list. The country scores 65.6 out of the total 100 which is two lines up against 2017. WEF experts explain the Russia's higher score by the stabilized macroeconomic situation, creation of conditions for the innovative development and introduction of new information technologies into the everyday life of Russian citizens. By one of 12 key pillars, namely the institutes, Russia scores only 52.7 which places it on the 72nd place in the list.

An annual competitiveness ranking prepared by the International Institute for Management Development (IMD) leaves Russia on the same 45th place out of 63 as at the end of 2018. Amongst the strengths of the Russian economy, experts noted the budget surplus, current account surplus, export of goods and introduction of data bulks. A decrease in tax evasions and bureaucracy was also noted. At the same time, the country's shown worse positions in the growth of population, number of patent applications per capita, development of venture capitals and protection of shareholder rights.

The Index of Economic Freedom, an annual index and ranking created by The Heritage Foundation and The Wall Street Journal and in existence for over 20 years, includes '12 freedoms' ranging from property rights to the financial freedom. The better you are doing with certain freedom, the higher the freedom's ranking is, with 100 being maximum and 0 minimum. As at the end of 2018, Russia occupies the 107th line the in the rating out of 186 countries, scoring 58.2. The Russia's total score is 1.1 points higher than in 2017. According to the ranking authors, the Russian economy is dominated by large state institutions and inefficient state sector. There are favourable conditions for corruption in the Russian judicial system. Property rights are poorly protected. All these factors impair the long-term prospects for the economic development.

2

Role and significance of the banking system in promotion of digital technologies and boosting of the russian economy growth

As in most emerging market economies, in Russia the development of financial sector is bank-centric. Banks hold more than 80% of the total assets of the Russian financial industry which determines their key role in the interaction between real and financial economies.

2.1. Position of banks in the financial Intermediation system and their role in digital transformation of the community

- *Lending to the real economy plays a leading role in the Russian banks' asset profile. Banks act as largest operators in all domestic financial market segments.*
- *The real-time continual maintenance of the national payment system along with support to cash transactions carried out by businesses of all ownership forms and households is one of the banking sector's top priorities.*
- *Banks are very appreciative of 'disruptive' technologies, including artificial intelligence, and go ahead of the other sectors in scale and degree of their application.*

In Russia, banks are the main suppliers of a wide range of financial services of which the financing of the real economy is of paramount importance. As of June 1, 2019, total loans granted by commercial banks with account taken of revaluations and adjustments of the loan value were in excess of 64 trillion roubles, accounting for almost 70% of the banks' total assets. At the same time, loan portfolios of nonfinancial entities and households have reached 33.6 and 16.1 trillion roubles, respectively, i.e. 53.4% of the banking system's total assets.

Banks are the largest operators in the domestic currency market with a share of 90%, repo market with 85% and bond market with a share of almost over 65%. Debt securities acquired by lending institutions worth almost 11 trillion roubles, or 11.6% of the banks' total assets.

Russia is known for a high share of banking groups that include financial (insurance and leasing companies, investment and non-governmental pension funds) and nonfinancial entities. As of January 1, 2019, there were 86 banking groups operating on the market with control of 89% of the banking sector's assets.

Banks accumulate nearly the entire organised savings of households. Household deposits exceeding 28 trillion roubles, i.e. 31% of the banking sector's total liabilities, are the main driver of the sector's active operations. At the same time, bank deposit accounts held only by legal entities less loan institutions contain an aggregate of over 22 trillion roubles, or 24% of all the liabilities, which greatly contributes to the growth in the banking system's resource base.

The banking sector ensures real-time continual operation of the national payment system and supports cash transactions carried out by businesses of all ownership forms and households. Remote banking has become a widespread practice – 93% of personal accounts with capability of electronic payments and 98% of corporate accounts are now accessible via the Internet.

Banks issue and process (acquiring services) bank cards which as at the beginning of 2019 totalled in excess of 272 million units. By mid 2019, the Russian acquiring had on average overcome an important milestone when the share of bank card purchases exceeded 50%. In January 2019, the Bank of Russia launched an express payment system. In the second half of 2019, a QR-code payment system will be undergoing testing. It is anticipated that the share of electronic payments will be close to 80% in the foreseeable future which will bring the Russian payment service on a par with the most developed electronic banking countries. This is how the Russian banks are carrying out a very important social mission aimed at making financial services available for households and entities of all ownership forms irrespective of population densities and geographical distances.

At the same time, the banking sector is known to be very appreciative of 'disruptive' technologies, including artificial intelligence, going ahead of the other industries and social sectors in scale and degree of their application. It is the banks who champion digital transformation of the entire financial services industry most of all and create ecosystems that fundamentally modify the format and methods of interaction between the real and financial economies.

> 50%

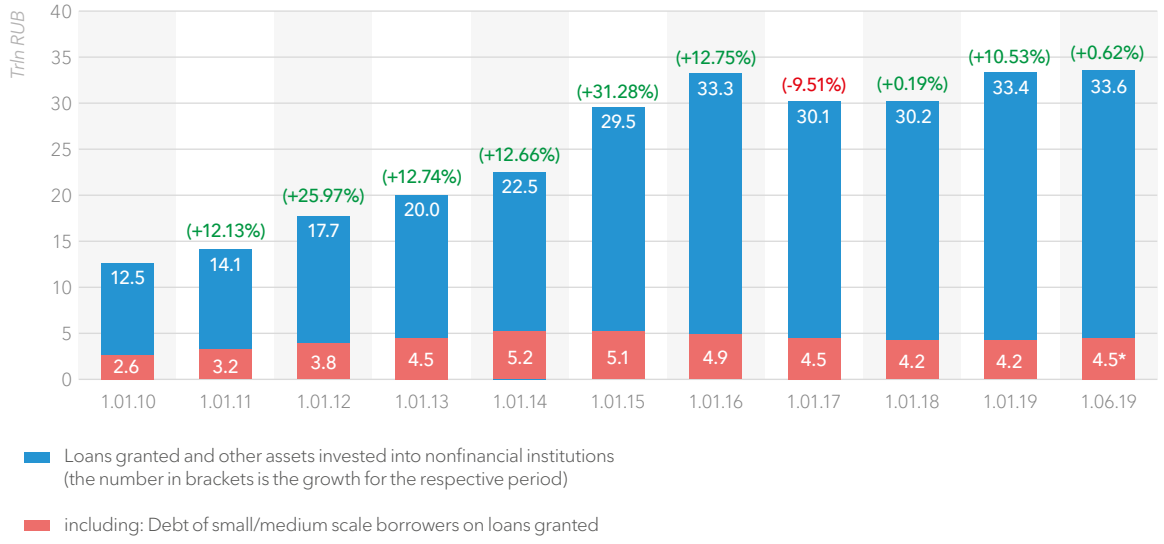
of purchases in Russia are paid for by payment cards

2.2. Current trends in landing of the real economy

- *The real economy financing in the current period continues to demonstrate a fast growth of household debts on loans. An increase in the interest in the first half of 2019 had only a slight impact on the amount of loans in the retail lending segment.*
- *Lending to nonfinancial institutions showed slower growth and unstable dynamics in some months. One of the main reasons behind this is a high share of bad and overdue debts on banks' balance sheets.*
- *A decrease in the interest rates originating from the transition to the neutral monetary policy will boost the loan demand which will need to be correlated with the borrowers' debt burden.*

In 2019, lending to nonfinancial entities and households remains on the upward cycle path. Lending to households under mortgage and unsecured personal loan schemes is still growing at a faster pace. According to the Bank of Russia, total household loans in this January-June grew by 9.7%[1] while total corporate loans grew only by 2.9%. Moreover, in mind with the growth in overdue debts, the financing of legal entities demonstrates an unstable behaviour in some months.

Lending to nonfinancial institutions, trillion RUB



Source: calculated from the Bank of Russia's data
** forecast*

[1] *In its published summaries, the Bank of Russia notes that relative indicators of the banking performance are influenced by the rouble rate behaviour and revocation/cancellation of the licenses from some loan institutions, except for those where revocations/cancellations are due to the reorganisation. Therefore, for a more correct picture of the actual banking performance in key indicators, growth rates are taken without the influence of the currency rate for loan institutions being in operation as of the last report date, including earlier reorganised banks. The absolute values of changes in performance indicators are provided by the Bank of Russia with account taken of the currency rate influence.*

In terms of loan coverage and amounts, corporate lending has attained the early 2016 performance. The quality of loan portfolios should however be taken into account too. Of note also is that the growth in lending to legal entities relies on the increasing loan debt of large businesses while lending to small and medium scale businesses remains on the same level since 2013.

After an increase in the Bank of Russia key rate to 7.75% per annum, market interest rates demonstrated a slight increase in December 2018 which had no significant impact on the amount of the loan debt in the retail lending segment in the first half of 2019. Concerning lending to nonfinancial institutions, it remains under stronger influence of macroeconomic factors.

The polling conducted by the Centre for Business Tendency Studies, Higher School of Economics, has revealed that albeit adversely influencing the industrial production performance, the level of interest rates is ranked as only the fifth by criticality amongst other factors constraining the activities of industrial entities.

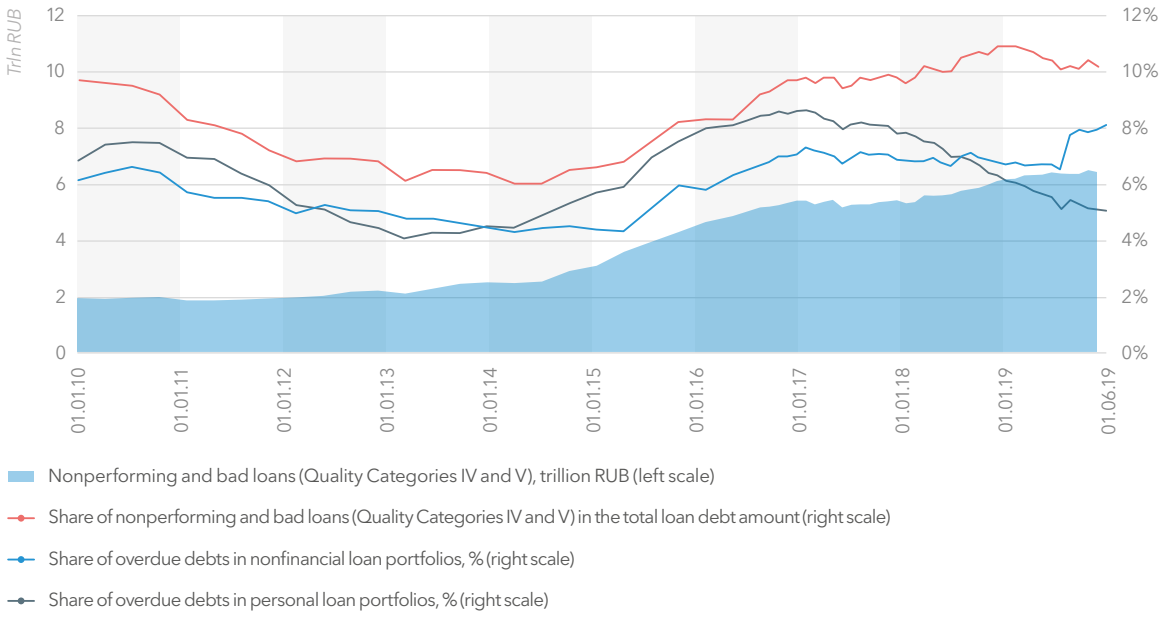
Evaluation of factors constraining the activities of industrial entities (share of the total number, %)

Source: Centre for Business Tendency Studies, Higher School of Economics

Industrial leaders believe that the main factors are those of the macroeconomic origin, such as the uncertainty of economic situation and insufficient demand for products in the domestic market as well as tax expenses.

Another important reason behind the low pace of lending to nonfinancial institutions apart from low profitability is a high share of bad and overdue debts. The need to establish extra reserves for potential bad debts increases the burden on the banks equity and, where such reserves are insufficient, may either lead to revocation of a license or make the banks face financial restructuring. Restructuring and other similar «technical arrangements» can work for settling bad debts only up to a certain time, although for various reasons such period may last fairly long for some banks. After all, one will have to choose between cleaning up balance sheets and losing the business.

Loans of quality categories IV and V in banking sector's portfolios

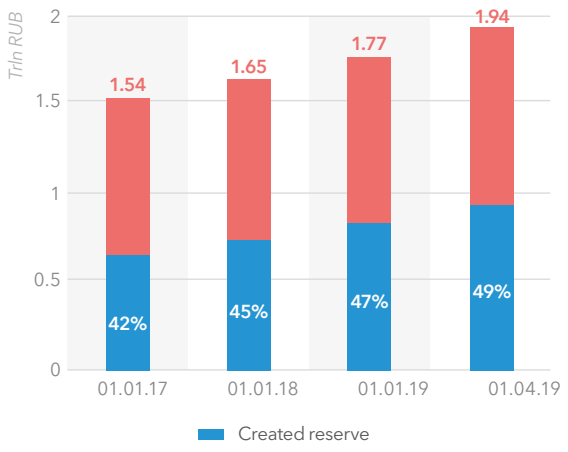


Source: calculated from the Bank of Russia's data

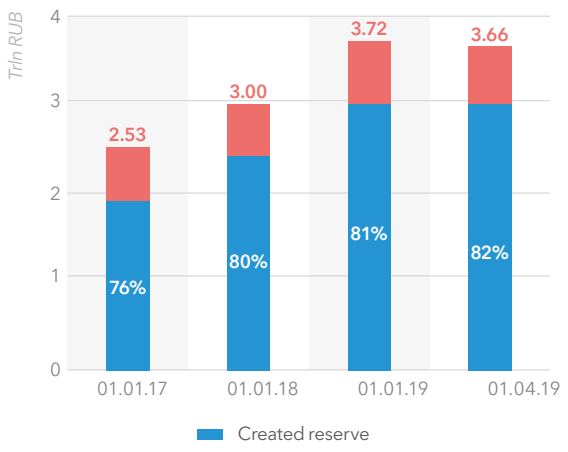
Shares of loans of Quality Categories IV and V estimated by the Bank of Russia look more optimistic than the figures in the publications by prominent rating agencies. According to the Russian rating agency ACRA's data, troubled debts account for 12 to 15% of the total loans granted by Russian banks. Despite of the revived economic activity , the share of nonperforming loans has been growing on the banks' balances since 2013. Only by the end of 2018 had the growth stabilized around the 2010 level.

In June 2019, S&P Global Ratings presented analytical report «Will banks in Russia and neighbouring countries be able to cope with high stocks of nonperforming loans?» The Agency's analysts estimate the share of nonperforming loans in Russia as of the end of 2018 at 16.7% or 10.4 trillion roubles. This figure remains steadily high for the past six years ranging between 12.9 and 17.5%. They also note that the bank reserves cover only 60% of such loans in total, which analysts believe is insufficient. They predict that the situation will be better in the future, but only insignificantly. Nonperforming loans will account for 16% of total loans in 2019 and 15.5% in 2020.

Nonperforming loans



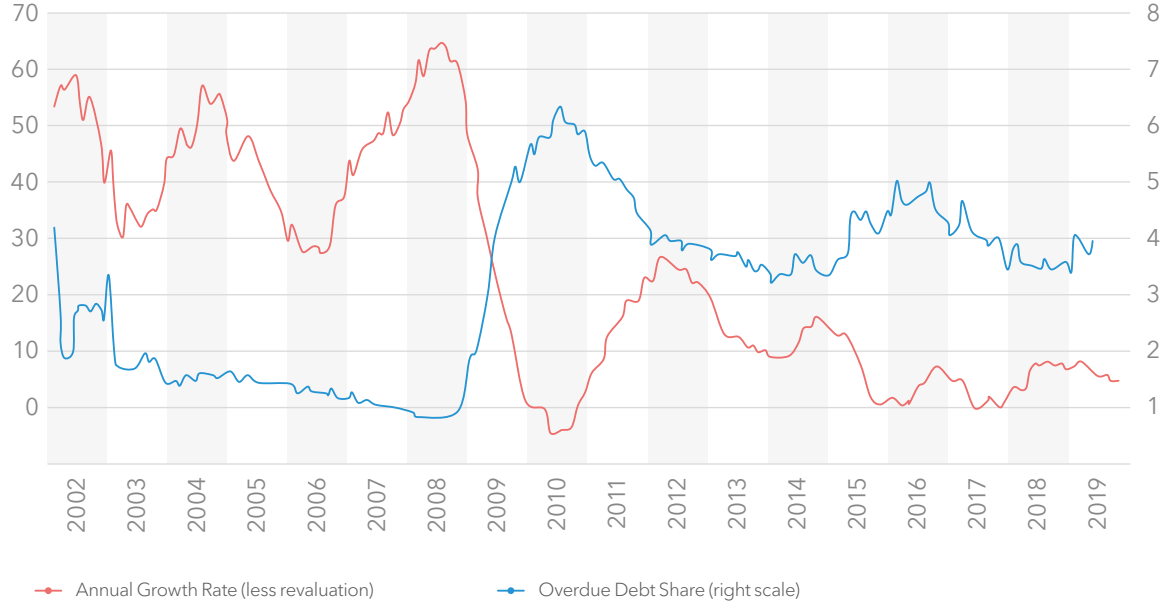
Bad loans



Source: calculated from the Bank of Russia's data

Long-term trends of lending and overdue debts prove that the credit squeeze can only partially be accounted for price and nonprice banking lending terms. The main reason is not tough monetary conditions but rather a high share of 'bad' assets that were not dealt with when they formed in a timely manner by microprudential and macroprudential controls for a number of reasons.

Growth rates in lending to nonfinancial entities and changes in overdue debt share (less restructured banks), %



Source: Accelerated growth of household loans in overall bank loans: reasons, risks and measures by the Bank of Russia. Report, Bank of Russia, June 2019, p.20

Two periods in the Russian banking system can be distinguished between 2002 and 2019. They differ in the behaviour pattern of nonfinancial lending growth curves and the share of overdue debts.

The first period spans the time between 2002 and 2009 when, favoured by growing oil prices and generally good business conditions, loan portfolios were swelling in size but no evaluation of their quality was undertaken. Technically, overdue debts remained at a low level and by mid 2008 had even dropped down to a historical low.

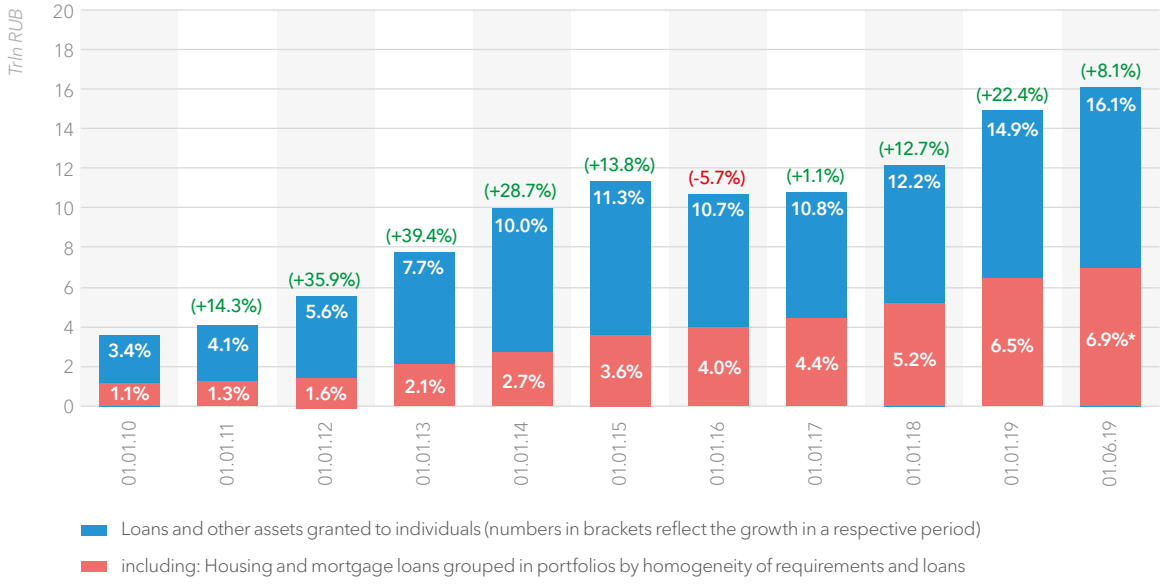
The second period, between 2010 and 2019, is the time when high share of overdue loans led to a long-term balance sheet recession in banks. For various reasons and factors, no systematic efforts were undertaken up until 2016 to reveal and cut out the ballast of delinquent loans in all bank groups. The authorities elected to proceed with the simplest solution – recapitalization of large banks (in 2010 and 2015) and creation of an inefficient institute of bridge banks. For many years, nonperforming loans and technical assets remained on banks' balance sheets. However, without such efforts, balance sheet recession may take very long time and obstruct positive effects gained from easing of the monetary policy.

Driving inflation to the close-to-target level creates conditions for the transition from moderately tough to neutral monetary policy that has been declared by the Bank of Russia management. It is reasonable to expect that the Bank of Russia key rate may drop down to 6% per annum or even lower within the next two years provided no shock impacts occur.

The world practice shows that when lending to households, the easing of price conditions is always accompanied with expanded demand for loans not only for economic but also for psychological reasons. Interested in the increase of their market shares, banks at first support the growing demand for retail loans. For a number of banks, another driver for approval of loan applications is the maximisation of profits as even with reduced interest rates, their level is still higher than the lending rates offered to corporate clients. Up to a certain time, all this serves as an extra driver for the economic growth, contributing to the expansion of consumer purchasing power. Thus, conditions form for consumer loans to boom.

However, with retail loans growing too fast and real income lagging behind, any difficulties with debt servicing, especially when business conditions turn to worse, may at some stage lead to a galloping growth in nonperforming and then overdue debts. In this case, the fact that the growing share of 'bad' assets is at first concealed by new loans being actively granted creates a real danger.

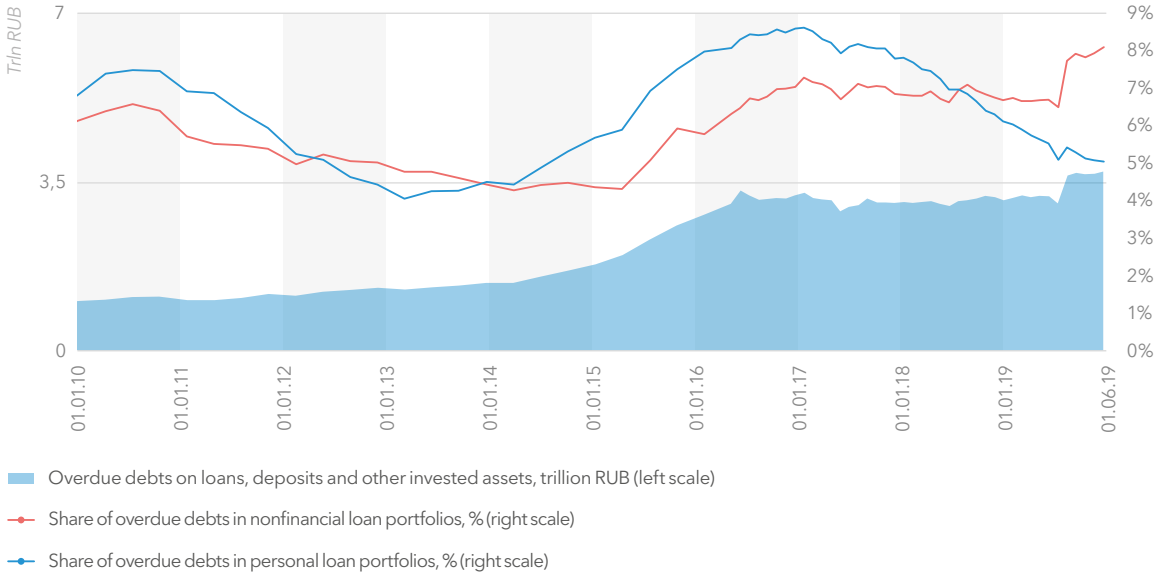
Household loans, trillion RUB



Source: calculated from the Bank of Russia's data
** forecast*

Changes in lending to households indicate worrisome tendencies currently showing up in this segment. Loan debts, especially debts on unsecured personal loans, are growing faster than the income of the overwhelming majority of the country's population. The main contributors to the growing unsecured personal loans between 2018 and 2019 were the 'cash loans' and 'credit cards' (growth by over 33 and 20%, respectively).

Overdue debts in the banking sector's loan portfolios



Source: calculated from the Bank of Russia's data

Analytical data and expert determinations unequivocally prove that there are signs of the increasing debt burden for a significant part of borrowers that grows disproportionately to the income of the borrowers. At the same time, while the amount of household loans is increasing, the share of overdue debts is so far decreasing. This can partially be accounted for a steady decrease in interest rates in recent years but more importantly, by the fact that as of yet loans are granted at a faster rate than they are becoming non-recoverable. Moreover, a part of bad debts are either refinanced with banks or microlenders or, for various reasons, not shown in balance sheet data. All in all, the above-mentioned recitals prove expediency of corrective macroprudential measures capable of maintaining the balance of risks and interests.

> *According to Bureau of Credit Histories, Combined Credit Bureau, the number and share of borrowers with the debt burden indicator of over 50% have significantly grown over 2018. This estimation was based on the information from credit histories and aggregated data on the borrowers' income provided by lenders. As of March 1, 2019, 14.6% of all borrowers, or 8.23 million people, invested more than half of their income to repay their loans. While in 2017 this figure was 12.7%, in 2018 it raised to 13.8%. Of debt-ridden individuals, 53%, or 4.33 million, earn from 20 to 50 thousand roubles a month; 26%, or 2.19 million, less than 20 thousand roubles; 21%, or 1.7 million, over 50 thousand roubles. The increase in payments to income (PTI) may become a result of the increased activity of lenders, extending the limits for borrowers. An average sum of an unsecured household loan has grown by almost 40% in 2018, exceeding 180 thousand roubles, and in some banks is 600-700 thousand roubles.*

According to the data from the household debt overview produced for the first five months of 2019 by the National Association of Collection Agencies (Self-Regulating Organisation National Association of Professional Collection Agencies), an average Russian borrower will require almost 11 monthly salaries to discharge his/her liabilities to the bank. The debt burden of individuals has grown by half since 2014. The most active borrowers are the individuals with low income who use loans as the last tools available to support their living standards. This in turn leads to the increasing burden of payment commitments, adding to the pressure on already low income of the people. This is how the debt spiral.

The overview states that around 10% of borrowers, or about 7 million people, earn less than 50 thousand roubles per month which forces them to allocate more than a half of their monthly earnings for repayment of the loan. At the same time, 2.3 million bank clients every month manage with incomes of 20 thousand roubles – after repayment they are left with the a sum close to the subsistence minimum of the region, varying between 11 and 12 thousand roubles, known in Russia as a 'poverty line'.

The degree of the debt load varies not only between the categories of individuals but also region-wise. Besides, high average loan values per capita in a Russian constituent entity do not normally reflect the level of the debt burden. The highest debt per capita values are recorded in Yamal-Nenets (436.3 thousand roubles), Khanty-Mansiisk (420.2 thousand roubles) and Nenets (328.2 thousand roubles) autonomous districts, Republic of Sakha-Yakutia (358 thousand roubles) as well as in Tyumen, Moscow and Magadan regions (over 300 thousand roubles). The country's average is 207.3 thousand roubles.

Looking at the list of regions in which the loan repayment period exceeds the country average of 11 months, we would discover other leaders. More than 20 salaries for the loan repayment, this much is required for people from Kalmykia (32), Republic of Altai (26), Chuvashia and Karachayevo-Cherkessia (24 each), Kurgan region (22) and the Jewish Autonomous Region (21). To discharge liabilities to the bank, borrowers from the Irkutsk region, Republic of Mariy El and Khakassia would need 20 monthly salaries. For Tyva citizens, it takes the longest to repay the debt. To repay the loan, they would require 124 salaries with the average loan amount of 251 thousand roubles.

In 2018, the Bank of Russia increased premiums for banks on household loan risk coefficients on three occasions. On January 1, 2019, the Bank also introduced premiums on risk coefficients for mortgage loans and loans under co-investment agreements with downpayment of 10 to 20% of the apartment's cost from 0.5 to 1.0 (which equates to a risk coefficient of 200%). On April 1, 2019, they increased premiums on risk coefficients for household loans with the true interest cost form 10 to 30%.

10% of borrowers

spend more than a half of their monthly income on loan repayment (incomes less than 50,000 rubles)

New restrictions on maximum debts of individuals on credits (loans) granted for longer than one year have become effective since July 1, 2019 whereby accrued interests, damages (fines, penalties), other sanctions related to such credits (loans) as well as payments for services provided by a lender to a borrower for a separate fee may not exceed the debt more than twice. Once this ceiling is reached, any accrual of interests, other charges, damages and other sanctions should no longer be applicable. Concurrently with it, a ceiling was established for the true interest cost of credit (loan) and a limitation of 1% a day was introduced for the daily interest. Such a restriction is primarily desirable for the so called payday loans granted by microfinance organisations (MFO), or microlenders. From July 1, 2019, the true interest cost for such loans may not exceed 365%.

Calculation of a Debt Burden Indicator (DBI) has become a mandatory requirement for loans since October 1, 2019. As a basis for the DBI calculation, the Bank of Russia has chosen a PTI method defined as a ratio of the borrower's monthly payments on all existing credits and loans and a newly granted credit to the borrower's average monthly income. The debt burden ceiling is however yet to be determined. Additionally, pursuant to the Household Credit (Loan) Law, where a borrower applies for a credit or loan in excess of 100 thousand roubles, the lender mush inform such a borrower that in case the total amount of payments on all loan liabilities exceeds 50% of the borrower's income, there is risk that he/she will default on the liabilities and become subject to penalties.

The Regulator has conducted inspection of banks to obtain data on distribution of the debt burden for borrowers of retail loans granted in Quarter 1 2019 and associated risks. A decision has already been adopted to establish premiums on risk coefficients depending on the level of Debt Burden Indicator (DBI) and the true interest cost (TIC) from October 1, 2019. According to the Bank of Russia analysis made for 24 retail bank majors, excluding Sberbank, if lending to consumers maintains the same growth rate as at present time, the accumulated capital buffer to meet new requirements for retail loans will be equal to 693 billion roubles by early 2020.

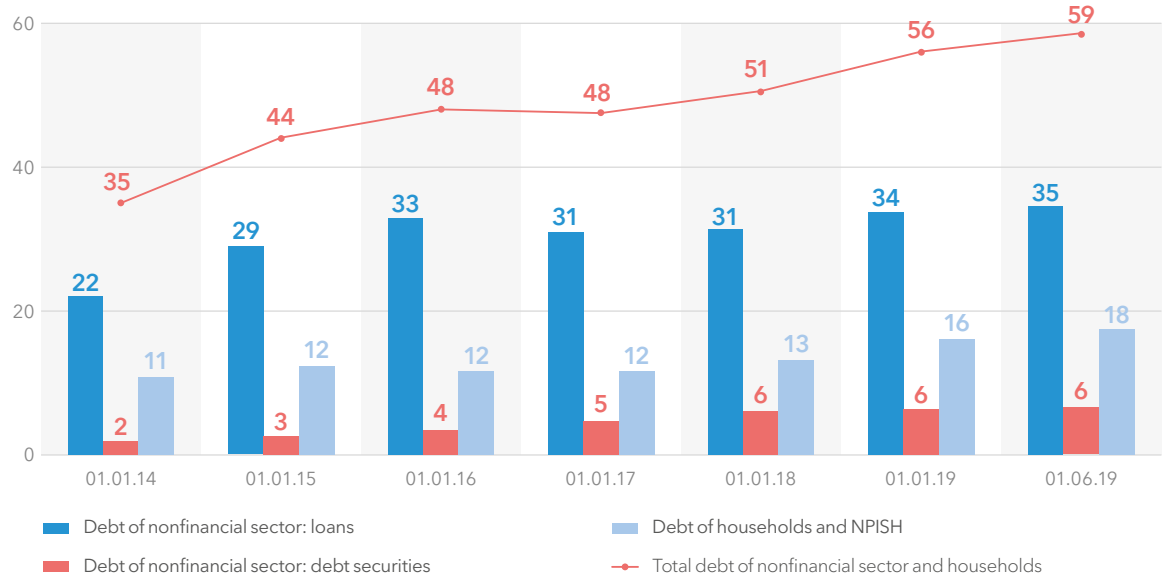
Calculation of DBI can solve only a part of the problems. In particular, it is still not clear whether the banks are eligible to collect and review data on income and liabilities of the borrower and his/her family. What is more, there is currently no database in the country with up-to-date and credible information on household incomes that could confirm the borrower's solvency.

A particular attention of the Regulator to the debt burden level covers not only the consumer lending segment. A special focus is currently placed on maintaining the balance between the measures to encourage economic growth and measures to support financial stability. Lowering the inflation to the close-to-target level of 4%, structural liquidity surplus, transition of the Russian economy to the revival and upswing phase and government benefits and interest rate subsidy schemes contribute to the downward trend in the interest rate development and increase in the bank loans and debt financing.

9,7%

– the growth rate of loans to households in Q1 and Q2 2019, according to the Bank of Russia

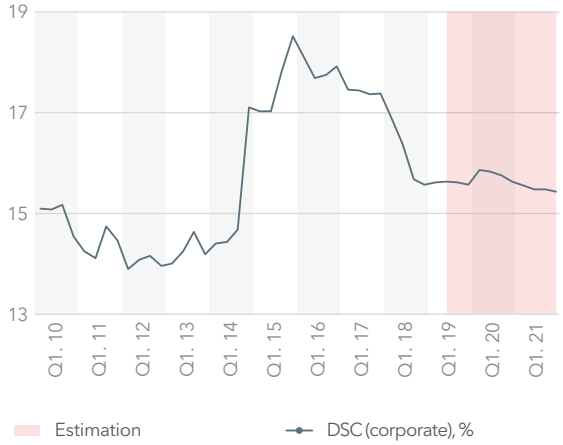
Aggregate debt of nonfinancial sector and households, trillion RUB



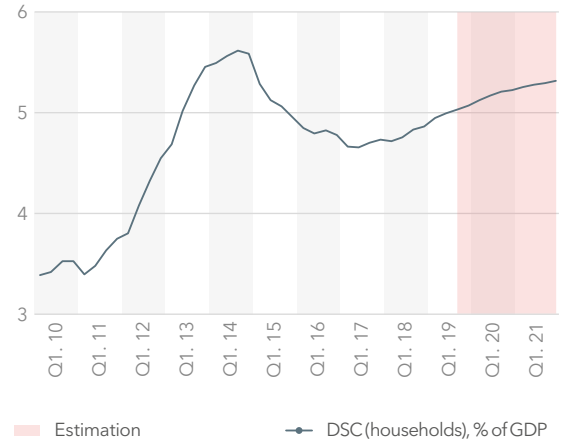
Source: calculated from the Bank of Russia's data

This results in a growth of debt burden that has certain critical limits. If such limits are exceeded, some banks begin to assume risks which they cannot absorb due to the scarcity of capital, thus putting themselves at risk of violating mandatory prudential standards and losing solvency. Excessive debt burden does not only jeopardise the banking sector acting disruptive to its financial stability. It also threatens long-term stagnation of the economy.

Debt burden on institutions (DSC), % of GDP

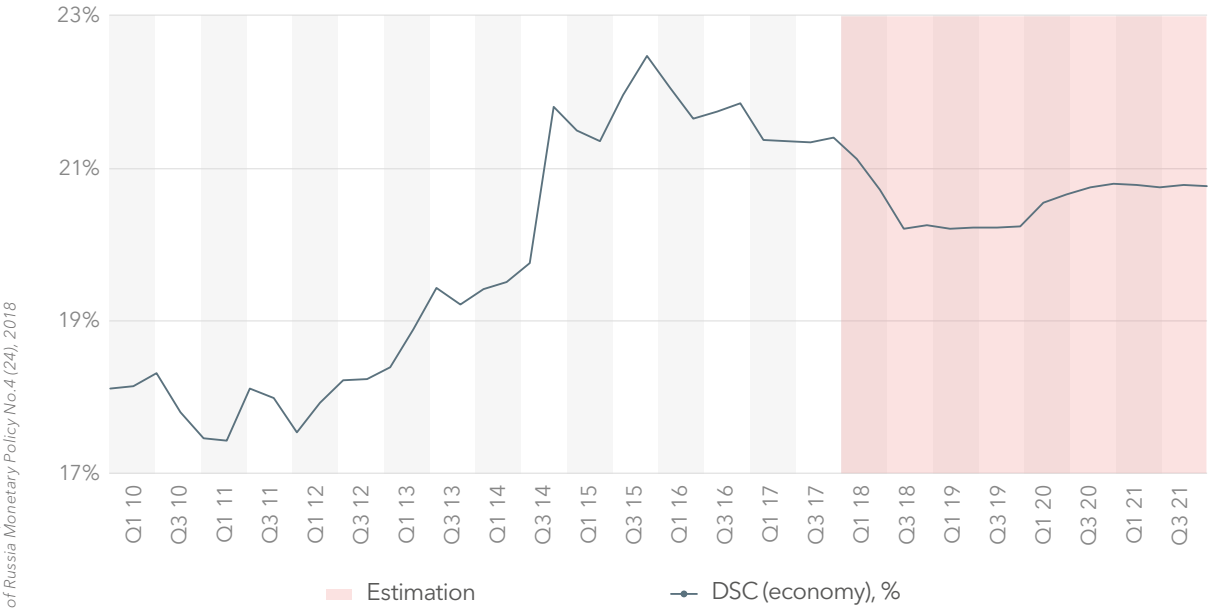


Debt burden on households (DSC), % of GDP



Source: Report on the Bank of Russia Monetary Policy No.1 (25), 2019

Debt service coverage in the russian economy, % of GDP



Source: Report on the Bank of Russia Monetary Policy No.4 (24), 2018

According to the Regulator's estimates, as of early 2019, the debt service coverage for the entire economy is approximately 20% of GDP. According to intercountry studies, the debt burden causing the risk of financial instability for the economy varies between 20 and 25%. It can therefore be concluded that the measures to limit the growth of debt burden are about to receive practical solutions. This can be confirmed by the Bank of Russia's focus on accounting for mutual influence between monetary and macroprudential policies that act as "connecting vessels". Easing of one can cause toughening of the other. This seamlessly blends with incentive based control that is mainly aimed at preventing accumulation of systemic risks, on the one hand, and abrupt credit squeeze, on the other.

3

Digitalization of society and a new framework of interaction between the real and financial sectors of economy

The fourth industrial revolution ("Industry 4.0.") is entering a critical phase, with half the global population connected to the Internet today. According to the estimate made by the McKinsey Global Institute, half of today's work activities could be automated in 20 years' time from now. The Internet of Things (IoT), Machine Learning and Artificial Intelligence systems are advancing at a furious pace. Digital technologies have penetrated all areas of life, and are transforming the world into a globally connected smart environment. The dominant position in the new structure is occupied by financial technologies, which pave the way for innovations in other spheres of the economy and the social sphere.

3.1. Financial technologies as drivers for digitalization of economy and social sphere

- *The financial sector ranks among the leaders in terms of the level and pace of digital developments.*
- *The digital transformation of financial industry in Russia is rapidly progressing, and showing the way to other sectors to follow its steps.*
- *Thanks to disruptive technologies, the financial sector is seen as one of the drivers for digitalization of the economy as a whole as well as the social sphere.*

The objective of financial technologies (or Fintech) is the development and implementation of innovative solutions in the banking industry and other segments of the financial sector. The use of publicly available application programming interfaces (Open API), other remote access techniques, Big Data Analytics, Blockchain, Robo-advising, Machine Learning and Artificial Intelligence is transforming the financial industry in Russia into one of the most innovative sectors of economy.

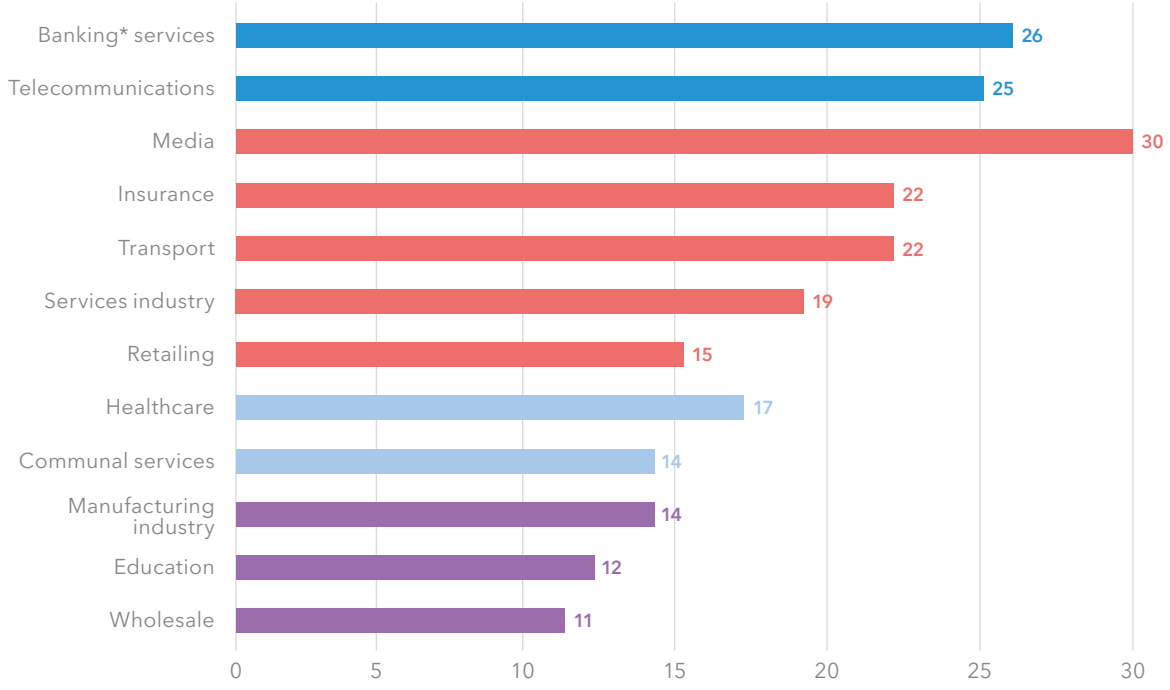
About 74 percent

of Russian suppliers of financial services are planning to pay priority attention to partnerships in fintech withing next three to five years

The World Bank report 'Competition in the digital age: strategic challenges for Russia' (September 2018) notes that the digital transformation of finance industry in Russia is moving forward at an exponential rate, setting an example for other industries. This places Russia among the top five global leaders in this sphere. According to the poll held by PricewaterhouseCoopers Russia in 2017, 74% of Russian financial service providers were planning at that time to focus on Fintech partnerships in the nearest three to five years, investing in Data Analytics (76%) and Mobile Services (60%). Today, the level of activity in the sphere of Fintech has grown even higher.

In terms of the level and pace of digital technologies advancement, the financial sector occupies a leading position. A study of a cross-sectoral group of leading IT directors in the industrial sector from more than 90 countries, carried out by Gartner, showed that the service industries, especially the financial and telecom sectors, are more disposed to deploy innovative technologies. Similar conclusions were made by McKinsey in their assessment of the digitalization level of the private sector in Europe. In terms of the digitalization index, a parameter that consists of a set of indicators to evaluate digital assets and the use of digital technologies and "digital" workers, the highest ranking belongs to the media, banking services and telecom sector.

Ranking of the business priorities of digital transformation by industries, % of polled people (ranked by industries 1–4)



Banking and investment services
Source: McKinsey Global Institute 2016, Digital Europe: Pushing the Frontier, Capturing the Benefits. McKinsey & Company, June, 2017

The advancement of Fintech initiatives brings fundamental changes to the landscape of not just the financial industry. Thanks to disruptive technologies, the financial sector is seen as one of the drivers for digitalization of the economy as a whole as well as the social sphere. This also means that, in a 'platform' economy, financial ecosystems in particular, as well as the financial sector as a whole, will occupy a central position.

3.2. Transformation of banking at the digital age

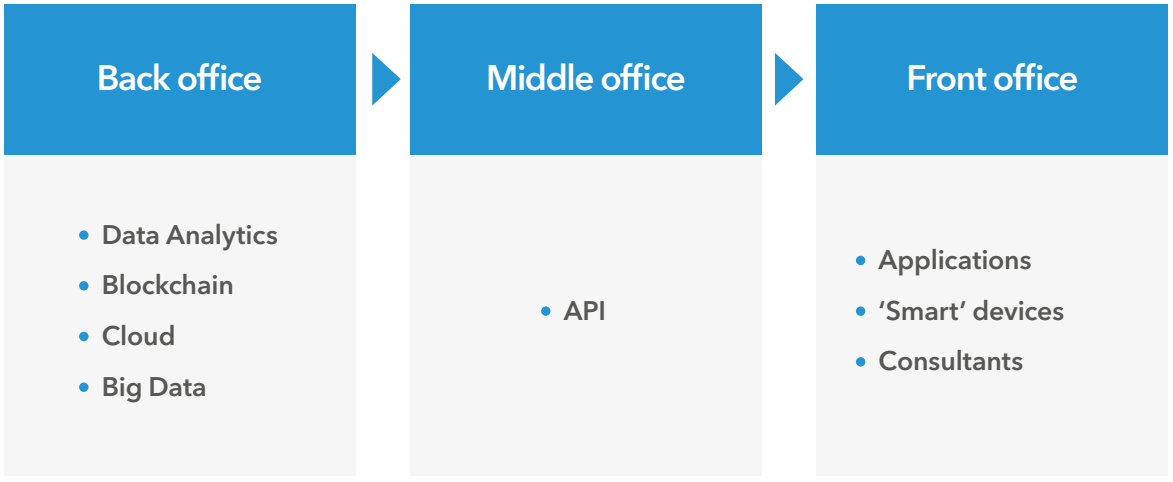
- *Transitioning to Open Source means a change in the paradigm of banking and its transformation into a brand new digital dimension. The 'open banking' model implies the use of mobile applications, remote-access digital technologies and analytics.*
- *The competitive edge of financial organizations is increasingly dependent on their ability to give up the monolithic, vertically integrated structure and move their focus to the use of open markets and all available information for business purposes.*
- *The traditional and digital banking are two opposite poles, between which there are many transitional models for providing financial services.*
- *Transforming traditional banking into digital banking will take a certain historical time. The duration of this period will depend on the preferences of customers and their digital literacy, the protection of financial assets and information against unauthorized access, the state of competition and the regulatory environment.*

In September 2015, the government agencies of Great Britain proposed a transition to the 'Open API' standards for banks allowing the provision of their data to other organizations. The initiative was developed by the Open Banking Working Group, comprised of representatives from banks, Fintech companies and professionals specializing in Open Data. From January 13, 2018, the use of the Open API principles became mandatory for 9 major banks in Great Britain, followed by a phased migration to this principle by other groups of credit and financial organizations.

In January 2016, the EU Payment Service Directive PSD2 came into force, which allowed bank customers to receive services associated with managing their finances from third parties. At the customer's discretion (and with the customer's permission), the bank provides access to the customer's payment and financial data for third parties whose services the customer is seeking, using the Open API (application programming interfaces) technology.

Those two milestones placed a watershed between the banking system of the past and the banking system of the future. Transitioning to Open Source means a change in the paradigm of banking and its transformation into a brand new digital dimension. The 'open banking' model implies the use of mobile applications, remote-access digital technologies and analytics; The point of this technique is to change from vertically integrated and tightly controlled structures to a market of automatically configured and customized services, implemented on special IT-platforms using machine learning and artificial intelligence.

A conceptual schematic of the 'bank of the future'



Source: Chris Skinner. Digital Human. M., Mann, Ivanov and Ferber Publishing House. 2019

With deployment of mobile and digital communication models, the traditional banking mindset does not assist the longings of the majority of customers anymore. Generally speaking, the most important things for the customer are now the simplicity, safety and speed of banking operations, their availability 24x7, and the opportunity to receive other services in addition to banking via a single interface. In general, the digital age makes it possible for any device with a micro-chip to make transactions in real time and practically free of charge.

In future, the lines of banking products will gradually become a thing of the past and will be replaced by components in the form of software applications. Each customer will arrange them in a way that suits their purposes. The mainstream trend of marketing strategies for banks in the digital age is the mass-scale customization of services on the basis of Big Data Analysis and the use of Artificial Intelligence.

> *The cornerstone of customer loyalty in this new reality will be the new format of customers' communications with the suppliers of financial services. In addition to the personalization of service, the omni-channel strategy of service becomes an important factor. This implies not only communication with the customer through many channels, but also the integration of those channels into a single system. This increases the informativity of the CRM system and allows using the received data for creating an even more personalized approach. With time, this will allow to move over from digital service chains to 'Digital Factories' for the provision of services.*

The change in behavioral patterns of customers, combined with growing competition from startups, is destroying traditional business models and provoking the development of new strategies. The competitive edge of financial organizations becomes increasingly dependent on their ability to give up the monolithic, vertically integrated structure and move their focus to micro-services and open markets. Accordingly, banks and other regulated financial 'mediators' are trying to capture new Fintech developments and change the format of their services as quickly as possible, depending on their financial capabilities.

Transforming traditional banking into digital banking will take a certain historical time. The duration of this period will depend on the preferences of the end users of financial services and their digital literacy, the level of protection of financial assets against unauthorized access and data leak, the state of competition and the regulatory environment. With time, the term 'bank' may go out of use, to be replaced by modernisms like 'financial ecosystem' or 'platform', although this will not change the economic nature of operations associated with the transformation of savings into investments. The requirements for the sufficiency of capital and other prudential norms will remain in force. Therefore banking will remain to be the 'eternal matter', changing its shape and transforming from one state to another.

The traditional and digital banking are two opposite poles between which there are many transitional models for providing financial services. In models based on traditional banking, the share of digital component is increasing. Any banking strategy now includes the use of digital technologies. Models based on digital banking are using, and in all probability will continue to use in future, the elements of traditional banking. A certain functionality related to consulting and operations will continue to be used for some categories of customers (e.g., those joining a bank for the first time or applying for their first loan, retirees, not-digitally-savvy people, private banking clients, etc.).

Digital banking will still be required to get a banking license or another form of approval from the regulator. The prudential norms will continue to exist, as well as the risk management procedures and internal audit / assurance procedures. In this sense, even 100% digital banks have not totally cut the 'umbilical cord' of traditional banking. This is due to the fact that the risks of traditional banking are well-known. They have been analyzed and regulated. The risks of digital banks are poorly known and practically unregulated. The national regulators and the Basel Committee are just starting to look for approaches to the solution of this problem. This means that it will take a certain amount of time to see in practice, on the one hand, what kind of financial intermediation models will survive, and on the other hand, in what direction the regulatory innovations will develop.

A classification system for digital bank models based on current practice was proposed in the IBM report 'Designing a sustainable digital bank', 2019). The analysis assumes that a digital bank provides the majority of its products and services in the digital format. In addition to that, its customers use digital channels in their everyday bank activities. The infrastructure of such a bank is optimized for digital interactions in real time, and its organizational culture is adapted to rapid changes in digital technologies. The report classifies digital banking into four models.

Model A – a 'digital bank' brand. Classic banks, with many of its business process going out of date, constantly try to be closer to the new 'advanced' customer, who would be happier using digital technologies. It often happens that, not wishing to scare away the existing customer base, such bank launch a new brand with unique proposals and products designed specifically for the younger generation – and more often than not using the existing banking infrastructure.

Model B – a bank with digital channels. Unlike the model described above, Model B banks build an organization designed to improve the user experience. Those banks usually utilize the back-office and the license of existing banks to re-sell their products via a more convenient user interface.

Model C – the digital branch of a bank. This model combines two approaches: digital user experiences and new business processes. Large banks may realize that the inertia of their systems is too great to launch a digital bank. Model C banks organize a separate structural unit – practically a new organization, with a more flexible modular soft- and hardware for providing the service (back-end), allowing to improve the customer's user experience.

Model D – a 100% digital bank. The Model D banks build their product range on the basis of digital technologies. They are not necessarily banks without any offices, but the customers mostly interact with the bank via digital channels.

Model	A – a 'digital bank' brand	B – a bank with digital channels	C – the digital branch of a bank	D – 100% digital bank
Products, sales, marketing	Bank's own	Bank's own	Bank's own	Bank's own
Channels	Often combined with the parent bank	Bank's own	Bank's own	Bank's own
Back office	Often combined with the parent bank	Often combined with the parent bank	Bank's own	Bank's own
Banking license	Using the license of parent bank	Using the license of parent bank	Using the license of parent bank	Bank's own

The need to move on to digital formats is explained not only by the desire to increase the efficiency of operations, although it is an important factor in the competition between banks. However, especially for major banks, the even more important factor is the growing competition from Fintech companies, from fintech-midgets (startups) to FinTech-giants (Big Techs such as, Apple, Amazon, Google, Facebook, Alibaba etc.), which are absorbing a portion of banking service functions. Primarily, this concerns payment transactions, and secondarily, loans and financial consulting.

In this situation, banks are facing the challenge of not only closing the 'digital gap', but, more importantly, taking the lead in digital developments. The solutions to this problem depend on a combination of factors, the most important of which are the size of capital and the scale of activity, the choice of business model, the main targeted sectors of the financial services market, and the willingness to develop and strengthen partnerships with Fintech companies.

This involvement with competencies being new to the banks may bring about new risks, but it also allows to increase profits not related to interest by receiving a share of the partners' profits. Besides, it expands the customer base due to the provision of payment and other banking services through controlled companies. For a successful transformation into a digital platform, however, it is necessary to have high multi-skilled professional competences, including risk management and cyber security, on the level of best practices.

Major Russian banks, mostly systemically important ones, are moving forward in their transformation into a digital organization offering a wide spectrum of financial products and services. They are investing significant funds into Fintech initiatives and launching innovative pilot projects. Following full-scale digital transformation, they will be able to offer their customers a wide spectrum of services using the framework of their own financial, and even non-financial, ecosystems. A number of such platforms are being developed now on the basis of major banks, giving such banks a serious competitive edge.

For the overwhelming majority of banks, the implementation of this type of projects is beyond their means. Big-scale investments into digital projects are extremely risky. The bank's resources and competencies may turn out to be insufficient, and the losses from a failed transformation may lead to bankruptcy. At the same time, it is increasingly more difficult for such banks to hold on to their already small shares of key market segments, while they keep using traditional technologies.

Their customers are likely to start moving to major banks offering a full-scale digital service. A portion of financial services will be provided mostly by major banks via the Telecom and IT companies having an extensive user content and digital service technologies.

Therefore, most banks will become players providing service to segments not covered by the ecosystems of major banks. Many of them will need to find a niche for themselves where they will have a competitive edge. It is not going to be easy, even for very specialized niches, without moving to digital service technologies.

The limited amount of funds for a digital transformation is partially offset by the creation of pan-national platforms with a set of high-technology services. The Bank of Russia includes the following main elements into the emerging financial infrastructure that will meet the digital age requirements: an express-payment platform, a financial marketplace, the Single Identification and Authentication System (ESIA) with incorporated biometrics, and a platform based on the distributed ledgers technique (Blockchain) that helps accelerate the document turnover between financial organizations. The connecting link of the new infrastructure will be the publicly available interface (Open API), providing the informational interaction between all participants of the financial market.

With the development of a pan-national financial infrastructure, the imbalance of competitive capabilities of different groups of banks will be partially leveled out, enabling a significant reduction in expenditures relating to business operations. This priority task of the currently ongoing effort is to create the digital profile (DP) of natural persons and legal entities, which will help minimize the turnover of paper documents. This technological solution offers, among other things, more opportunities to banks for online lending development and cost reduction.

The 'digital consent' service will be put into practice, allowing to store all consents given by the individual, as well as to submit and withdraw the digital consent, or forbid the transmission of certain data to one or several data recipients. The DP can also contain a system of digital documents, providing storage and update of the most sought-after and legally significant data.

Such data can be received by users directly from the DP, without a request to the State Information System, allowing to reduce the load on data exchange channels and to accelerate data exchange. The data will be stored in the ESIA, and their authenticity will be guaranteed by the sources from which they have been received.

According to the concept developed by PAO Rostelecom in cooperation with the Bank of Russia, an individual's DP is the aggregate of digital records about this individual, kept in the informational systems of governmental authorities and organizations. It contains primary data about the individual – passport data, the insurance number of individual ledger account (SNILS), the personal tax reference number (INN), references to the individual's data from other governmental systems, a register of personal data processing consents. The main principles of an individual's DP are as follows:

- *A natural person has the right to control access to their data kept in various governmental informational systems.*
- *Data from an individual's DP can only be used or transferred with prior approval of the individual. A natural person controls the process of giving or withdrawing their consent.*
- *To give a digital consent for access to data from their DP, the individual must undergo the identification /authentication procedure with the use of a regular or qualified electronic signature.*
- *The most sought-after data, such as copies of personal-storage documents, will be stored in the DP, although the rest of data will be kept in the informational systems in which they were originally created.*

The practical implementation of this task requires solutions to a range of legislative, technological, economic and even psychological problems. To solve this and other issues, the Government of the Russian Federation adopted the decision to initiate a pilot project (December 2019 – March 2020) with the participation of Russian banks.

Digital concordance will **facilitate** operations implying access to data of individuals and legal entities and will **increase control** over data circulation for their owners

The transition to extensive use of the distributed ledger technology offers a potential to enhance the competitive edge of banks, including small and medium-sized ones. The most common of those techniques is the Blockchain, a cryptographically secured, decentralized distributed ledger. The use of Blockchain and other distributed ledger techniques is especially effective in two areas: the maintenance of records and documentation (registration of new data, identification of users, smart contracts), and the performance of transactions (dynamic registration, i.e. the exchange of digital and physical assets on a digital platform, payment infrastructure, verifiable data). The distributed ledger technologies pave the way for brand new business solutions, which will be accessible (it is important to stress that!) to all groups of banks. Some Blockchain applications are already in use for trading various types of assets (including Crypto-assets), in payment systems, including B2B payment and P2P money transfer, stock exchanges and platforms for asset trading based on Blockchain.

The successful leveling-out of competitive capabilities will also depend on the ability of banks to interact with technological companies when jointly developing and rolling-out innovative solutions. Smaller credit organizations, which cannot afford upgrading their IT systems, can use the services of companies providing technological solutions in the outsourcing format, in a wide range from cloud storage and data processing to advanced analytics and big data analysis. This way, many credit and financial organizations, including small and medium-sized banks, will get a chance to create their own ecosystems.

The target vision of the banking sector in Russia (2030 foresight) is presented in the report 'Innovations in Russia: A sustainable source of growth', issued by the McKinsey Center of Innovation Development (July 2018). The study especially stresses the role of the banking sector as the engine and prime mover of new innovative solutions that promote digitalization in other sectors of economy. It needs to be noted that a special emphasis was made on the most important characteristics of business processes and customer profile.

Target vision of the banking sector in Russia (2030 foresight)

The banking sector of the future

Business	Customers
• Digitalization of banking processes allows to reduce banks' costs. • The use of Big Data allows to assess customers with maximum accuracy and reduces risks to a significant extent when giving loans. • A significant portion of banks' profits is derived from the sale of non-banking products.	• In the environment of well-developed ecosystems, customers receive, via a single window, not only banking services, but also telecom, retailing and other services. • With the introduction of new technologies (including Blockchain), banking operations can now be performed practically at lightning speed. • Customers receive only personalized proposals.

Industry as a whole

Banking sector	Non-banking players	Major banks	Other segments
The engine and prime mover of innovative solutions, and a provider of human resources to other industries	Telecom and IT companies: offer increasingly more services of traditional banking, and directly compete with banks.	Provide a wide spectrum of services to customers via their own ecosystems	Segments not covered by banking ecosystems are serviced by niche players

Source: Innovations in Russia: A sustainable source of growth. Center for Innovation Development McKinsey's Innovation Practice, July 2018

3.3. Ecosystems as a new format of interaction between the real and financial sectors of economy

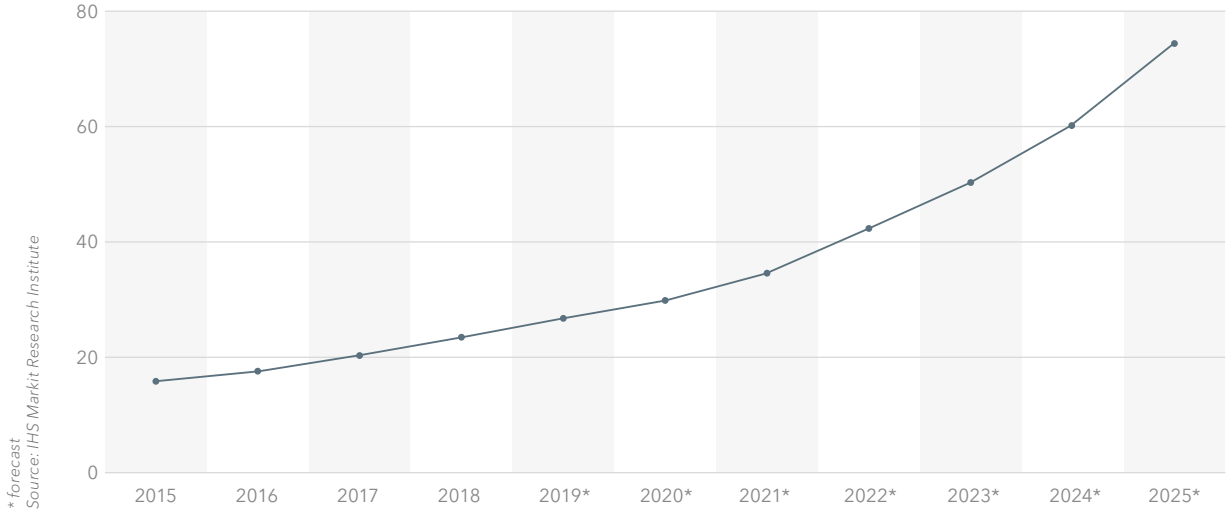
- *The world is entering the age of the Internet of Things (IoT), which has opened the transition to digital economy ecosystems.*
- *The main feature of the ecosystem is that the customer, via one of its participating companies, can gain access to all other organizations included in the system via the connected services.*
- *The creation of a financial ecosystem becomes an important factor for financial and credit organizations in the race for customers and, at the same time, a method of increasing the rate of return.*
- *As experience in the functioning of financial ecosystems is accumulated, and as standard software products appear on the market, there will be increasing opportunities for various groups of banks to create ecosystems.*
- *In the foreseeable future banks will compete not by their products, but by their ecosystems.*

The world is entering the age of the IoT. According to various estimates, 25–30 billion sensors and terminating units are already connected to the Internet, which has led to the creation of digital twins for billions of things. Digital twins are complete digital representations of individuals, objects, locations or processes, and may be used for modeling and forecasting the real behavior of people, as well as physical objects. Thus, billions of things equipped with artificial intelligence can now constantly connect to each other, transferring the necessary information at each contact. In the reality of market economy, a significant portion of this information is associated with financial transactions and cash flows.

"We are entering the age of the 4th generation Internet. It is the 'Internet of things', and it will begin in earnest only in 2020s. It is possible to build a microchip into any device – and it will become 'smart'… The next ten years of Internet growth will see many innovative developments put into practice, and we will start to create a semantic web, Web 5.0."

/ C. Skinner. Digital Human, M., Mann, Ivanov and Ferber Publishing House. 2019, p. 53–54/

Number of operating IOT devices, global market, billion units



** forecast*
Source: IHS Markit Research Institute

It is expected that by 2025 ca. two thirds of the global population (which by that time will number ca. 8 billion people) will use several devices, and that 80 billion of sensors connected to the Internet will be exchanging data. For the first time in human history, material values are transforming into a network-based digital format, becoming timeless, global and interconnected, with access to them being practically free of charge. The development of informational technologies has reached a level allowing organizations to collect, process, store and provide a great number of data about the manufacturers as well as consumers of products and services, building effective communications via all available channels.

IoT opened the transition to digital economy ecosystems, which are inter-dependent groups of subjects (production plants, people and things) participating in the 'value chain' and jointly using standardized digital platforms for mutually profitable purposes[1]. The main feature of the ecosystem is that the customer, via one of its participating companies, can gain access to all other organizations included in the system via the connected services, possibly even on special (privileged) conditions, existing only within its boundaries. According to expert assessments, by 2025 ecosystems will account for ca. 30% of global revenues of organizations and over 40% of their combined profit.

The base that unites organizations and companies is the single technological platform (marketplace) with access open to all participants. It allows to generate proposals matching to the fullest extent the customers' needs in various areas (education, healthcare, retailing, business, finance, etc.), taking into account customers' preferences. The technical capabilities that the planned ecosystem will provide to its participants include a customer identification system, rapid data exchange, common software interfaces and other services.

The ecosystems, being multilateral marketplaces, may be internal, being a part of the production process or supply chain (providing coordination between customers and suppliers), or external (industry-wide), where the leader of the platform brings together the external capabilities of participating companies. The digital platforms of ecosystems offer a range of seamlessly integrated products and services, covering a wide spectrum of customer needs in a number of sectors. The leaders in this area are the American (Facebook, Google, Apple, Amazon) and Chinese (Alibaba, Tencent) companies. They are operating on the global market and seen as the giants of the world of conglomerates (Big techs).

[1] *In Russia, the term 'digital economy ecosystem' was first introduced at the legislative level in 2017 as a 'partnership of organizations, ensuring constant interaction of their technological platforms, applied internet-services, analytical systems, informational systems of the Russian Federation government authorities, organizations and individuals'.*

Big techs	Market capitalization,*$ billion
Apple	956.9
Amazon	954.8
Google	838.5
Facebook	549.5
Tencent	456.2
Alibaba	421.7

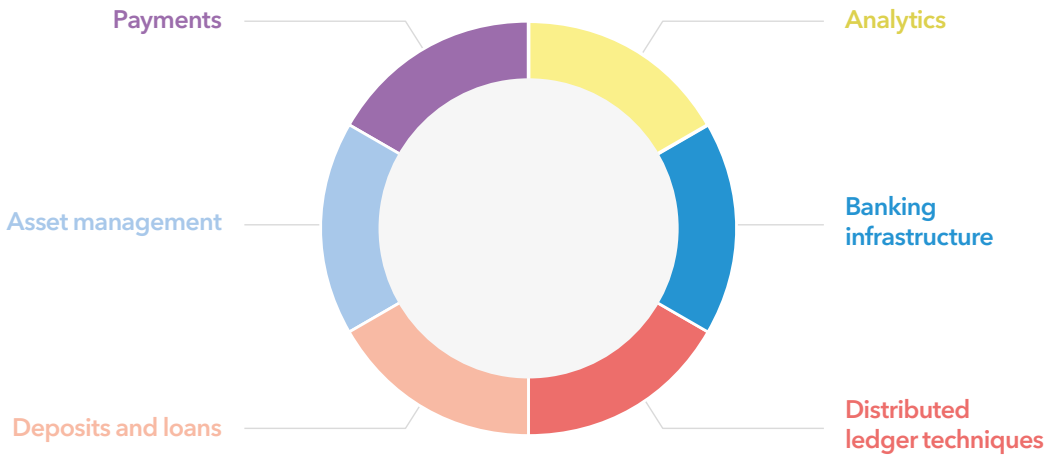
* as of August 2, 2019

Digital ecosystems are created in various sectors and spheres, but they have a number of common features, including payments and money transfers between participants, placement of deposits, provision of loans, and attraction of investments. This function has been historically dealt with by the banking sector, which had its boundaries and was governed by its regulatory and legal framework. The industry consisted of banks which carried out some or all functions and operations. The largest 'universal' banks used the concept of a 'financial supermarket' as their main business model.

In the implementation of this model, the main accent was made on the creation of vertically integrated structures, including by mergers and acquisitions. Major banks increasingly resembled factories manufacturing standard lines of services, which had built a colossal number of branches and additional offices around themselves. The emergence of financial technologies started the process of disintermediation and disintegration of the financial industry as a whole and the banking system in particular. The 'financial supermarket' business model, based on the provision of a wide spectrum of products and services to customers, started falling apart like a house of cards. The transition to public interfaces completes this process.

The market place is intended to improve availability of financial products for general population

The taxonomy of banking sector shaped by transition to Fintech models



Metaphorically speaking, the banking activities are no longer deployed vertically, but horizontally. Payment service, asset management, and, to some extent, deposits and loans have stopped to be the monopoly of banks or other financial mediators. Fintech allows using various configurations of business models, adapted to the needs and requirements of targeted customer groups. The establishment of electronic platforms (marketplaces) for the provision of remote financial services is changing the nature of relations between financial service providers and their customers. Competition between brands is being replaced by competition of the consumer properties of products and services. The expansion of customer base and emergence of a competitive edge due to the uniqueness of the product creates opportunities to increase the effectiveness of operations. Vertically integrated structures are being replaced by combinations of financial and other services that can be provided via a digital platform. This is, in effect, a financial ecosystem.

Using the principle of financial supermarket as a basis, the ecosystem significantly expands its boundaries and capabilities. The financial ecosystem today provides a number of advantages to its users (customers), which include, among other things, the fact that the service is extremely simple, clear and convenient, and that the customer can receive any service that they may need, both offline and online, via a platform available round the clock. Another factor that contributes to this situation is the change of concept in the relations between the bank and its customers: a transition from 'multi-channel' to 'omni-channel' – the integration of various communication channels into a single system to support the seamless uninterrupted communication of the organization with the customer and the creation of a single communication environment.

The creation of a financial ecosystem is an important factor in the fight for customers among the financial and credit organizations and, at the same time, a method to increase the rate of return. The growth of technologies allows combining all financial products, services and experiences into a single smart environment. Some organizations put together customized sets of services to make their customers fully satisfied in a certain area. The main factor for the customer is that they can, via one of the ecosystem's companies, gain access to all other connected services included in the system via the connected services, possibly even on privileged conditions, existing only within this ecosystem.

In the modern world, there are two main scenarios for creating a financial ecosystem. The first scenario is to build a comprehensive ecosystem (the so called 'lifestyle banking'), where the ultimate purpose is to fully cover the existing and potential day-to-day needs of the customer in one application. During the creation of an ecosystem, its cornerstone is the 'open code' concept, allowing to engage various partners within the system, which can use the bank's open data and codes.

The second scenario is to build a 'niche' ecosystem that will cover the customers' needs in one or several limited areas (housing purchase, education, healthcare, etc.). In this case, banks can create ecosystems around products that have a high development potential, incorporate significant expert knowledge and are supported by all necessary infrastructure.

At the present time, to create a financial ecosystem, it is necessary, firstly, to have a high-potential and well-adapted technological solution, as from the technical viewpoint the system represents an aggregate of interconnected IT solutions, web and mobile applications and customer relationship management (CRM) initiatives. A big role is played by the presence of a single standard for user interface. The difficulty is that for the time being there are no off-the-shelf IT solutions on the market that could be purchased and launched into operation as a ready-made platform for the implementation of an ecosystem. Significant investments need to be made in the development of technological solutions, such as, cloud techniques, Big Data and Analytics, machine learning algorithms and artificial intelligence, electronic accounting systems, cyber security, etc. Secondly, it is necessary to have an extensive base of customers who trust the bank and are interested in receiving various services and experiences from its partners. Thirdly, it is necessary for the bank management to be creative and willing to give up the traditional banking methods.

About 67 percent of respondents *

already have and are developing their own ecosystems or are planning to switch to a similar business model

* *Results of the questionnaire survey conducted by the Association of Russian Banks (page 86).*

"Brand new models are emerging on the financial market, in which value is created by collecting, processing and providing information: platforms, aggregators and mediators between financial organizations and customers. Those models are built on the assumption of exponential development of components that are the basis of competitive edge – the creation of a unique product, increase in operational efficiency, improvement of customer relations"

/ Competition in the financial market. Analytical report. M., Central Bank of the Russian Federation, 2018, p. 30-31/

As experience in the functioning of financial ecosystems is accumulated, and as standard software products appear on the market, there will be increasing opportunities for various groups of banks to create ecosystems. Technically speaking, any bank can build an ecosystem. The challenge is in its economic efficiency. The costs of the ecosystem might not pay off if it provides services to a comparatively small number of clients. The bank will have problems attracting partners to this ecosystem due to, again, the small number of customers.

However, a whole range of niche banks are quite capable of creating services that will allow them to act as a service operator for local "value chains" that will include local businesses, healthcare, education, trading and services. Besides, it is not impossible that comparatively small specialized banks will join their forces to create a common ecosystem, complementing the products of each other and, among other things, selling services through agency agreements.

Thus, infrastructure accessible through standardized interfaces is transformed into one of the main factors in achieving a competitive edge. That is the reason why qualitative changes are taking place in the architecture of financial sector. The transition to open informational space motivates the creation of alliances between credit organizations and innovative 'digital' companies. Thanks to the above, banks get an opportunity to incorporate innovative services from other industries, including not only the traditional financial ones but also many others, even the provision of domestic services to customers within the same ecosystem.

Irrespective of their size, banks that will be able to form effective partnerships with the most advanced Fintech players and companies having innovative competencies in Big Data Analysis, will be able not only to keep their position on the market, but to significantly improve it. In the foreseeable future, it is expected that there will be several major ecosystems on the financial market, targeting various audiences with an extremely wide spectrum of proposals, as well as a number of comparatively small specialized ecosystems. Banks will increasingly compete not by their products but by their ecosystems.

4

Cyber threats and information security: problems and solutions

Cybercrime is a global problem in today's world. The Global Risks Report 2019 of the Word Economic Forum lists cybercrime among major threats that may disrupt the world. Cybercrime not only causes financial losses, but also restrains the potential of practical solutions in the field of digital technology. This is especially true for the spheres where relations are based primarily on trust. The finance industry is at the top of the list of such spheres.

4.1. The scale of cybercrime in economy sectors and spheres

- *The scale of cybercrime has reached a dangerous level. The actions of criminals are a threat not only to the global economy as a whole, but also to each individual country, business unit or person.*
- *The most frequent targets of cyber-attacks are governmental entities, healthcare facilities and financial organizations.*
- *Cyber-attacks on financial organizations are motivated by financial gain, and also by access to information on payment cards and credentials for personal accounts of card holders.*
- *Increasingly more frequent targets of cyber-attacks are manufacturing companies, especially major ones. Big business is getting more and more involved with the Digital Environment and the Internet-of-Things. This means that the threat of cyber-attacks becomes higher.*

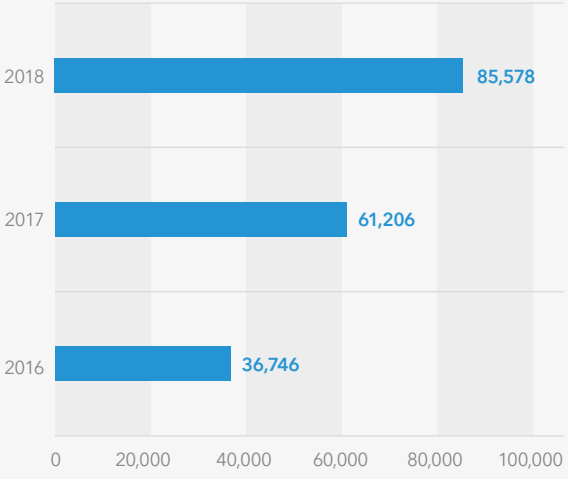
The scale of cybercrime in the world can only be assessed very roughly in quantitative terms. Firstly, there is no single centralized database. The figures shown here are mostly calculations made by organizations that are in charge of information security, whose data are limited to the areas of their professional interest. Secondly, for a number of reasons not all legal entities and individuals disclose their losses after cybercriminal networks attacked them, which is another reason why the records on actual total losses from cybercrime may be inaccurate. Nevertheless, the results of expert reviews clearly point to the fact that cybercrime has reached dangerous levels and has become a serious problem for the global economy as well as individual countries, business units and individuals.

> *Based on WEF assessments, cyber-attacks rank at the fifth place amongst the top ten risks. According to the data provided by BI.ZONE, total losses of the global economy caused by cybercrime in 2018 amounted to $1.5 trillion, and in 2019 they may increase to $2.5 trillion. According to the calculations of Accenture, an international consulting company, cyber-attacks cost an average company $13 million in 2018, or 12% more than in 2017.*

Digitization of social interactions is a highly dynamic process, the boundaries of which are blurred, and this provokes new forms and types of cyber threats. For a number of reasons, they can only be identified and neutralized with a certain time lag. According to the forecast of the company Cyber-Security Ventures, annual losses caused by cybercrime can reach $6 trillion by 2021.

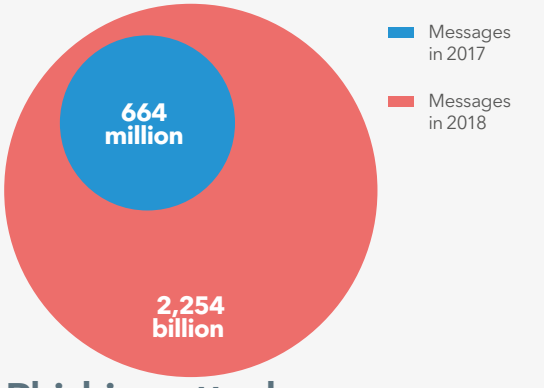
The examples that confirm the growing activity of hackers are the DDoS attacks and phishing, seen now as the most common and wide-spread forms of cybercrime. The number of DDoS attacks has increased more than twice in the past two years. The year 2018 saw the two biggest DDoS attacks in history, reaching 1.35 and 1.7 terabits per second, with hackers using memcached servers for their strike. No less impressive are the data on increasing phishing attacks, whose average number in 2018 reached 2.2 billion messages.

Global dynamics of DDoS attacks



Source: Qrator Lab's data

Average monthly phishing attacks around the world



Phishing attacks growth rate **350%**

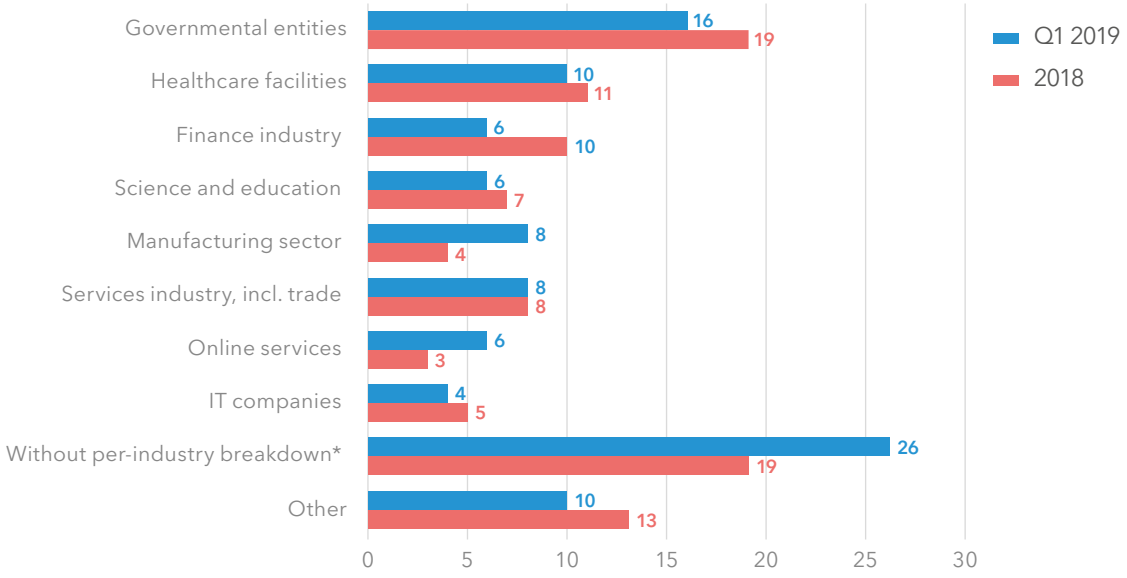
Source: Microsoft's data

Especially worrying is the growing scale of personal data leaks. In 2018, ca. 4800 websites unintentionally disclosed personal data of their users due to cyber-attacks, with 563 million credentials compromised as a result of the publicized three major leaks.

According to the cyber security threats monitoring carried out by the company Positive Technologies, the top cyber-attack targets include governmental entities, healthcare facilities and financial organizations. The percentage of each target may vary depending on the reliability of the information security system and on whether the target is willing to disclose the fact of the cyber-attack. Very common in the recent years have been "mass attacks' that have affected companies in different spheres. Mass attacks account for ca. 20-25% of all hacks, according to Positive Technologies.

The most frequent target of hacking attempts is government agencies. The criminals are mostly motivated by corrupt intent and are interested in confidential information. Stealing data remains their main motive. At the same time, hackers often use the websites of government agencies to attract public attention to certain ideas or aspects of public life. About one fourth of all IT incidents fall into the "hacktivism" category, or the use of computer networks to promote a political agenda or the freedom of information. The hackers usually target the infrastructure of government agencies, and infect their computers with spyware and remote administration malware.

Cyber-attacks distribution by economy sectors and spheres, %



The cyber-attack was a mass campaign and affected companies in different spheres

Sources: Current cybersecurity threatscape: 2018; Cybersecurity threatscape: Q1 2019, Positive Technologies

Healthcare institutions continue to be at the center of attention from hackers. In some cases, the hackers attack healthcare institutions to steal personal data (medical records, healthcare insurance policies or medical certificates). In other cases, they invade the infrastructure of healthcare companies and encrypt their data, demanding a ransom in exchange for restored access to the affected system. That is why cyber criminals can force these companies to pay up is due to the nature of healthcare operations, where patient lives and health are at stake.

> *Positive Technologies cyber-attack statistics show that the healthcare sector was most highly targeted in 2018. Healthcare institutions were hit by more attacks than the financial sector. According to experts, attackers got hold of the personal data and medical information of more than 6 million people.*

Credit and financial institutions continue to remain a frequent target of cyber-attacks, despite their higher security level. Due to higher security level, the attempts to penetrate the informational and telecom networks of banking and finance organizations are usually made not by individual hackers, but by well-organized criminal groups.

> *The challenge that the financial sector faces in dealing with cyber-attacks is their transnational borderless nature. Fraud is frequently committed through servers located in foreign jurisdictions. According to FinCERT's data of the Bank of Russia, more than 540 web resources that distributed malware, or were the malware's management servers, were identified in 2018. It is worth mentioning that more than 500 of those resources were registered outside of Russia.*

The main objective of hackers in the banking and financial sectors remains the theft of funds. But alongside with that, we see a growing number of IT incidents targeting sensitive information on payment cards, personal data and credentials for access to the users' personal accounts. Criminals use this information to steal money from the client accounts, or sell it on the Darkweb.

Increasingly more frequent targets of cyber-attacks are manufacturing companies, especially major ones. The average damages per IT incident in Russia, according to the estimate by Kaspersky Laboratory, are 14.3 million rubles. Big business is getting more and more involved with the "digital environment" and the "internet of things". The business environment is expanding to include cloud services and mobile devices, which are changing the perception of the "perimeter security" of a company. This means that the threat of cyber-attacks becomes higher.

The above considerations not only concern major manufacturing companies. Small and medium businesses are also not immune to cyber-attacks, especially companies which use digital profiles on a regular basis. The most affected sectors are the trade and the services sectors. The companies most exposed to these risks are online shops and other online services practicing online payments. It is also worth mentioning an important implication for this sector, namely, that it suffers from a shortage of financial resources and qualified personnel required for putting in place a proper information security system.

4.2. Information security threats in the digital space: current situation review

- *Protecting information against unauthorized access and preventing the use of confidential data for criminal purposes is a necessary condition for confidence and security in digital economy.*
- *Data theft and direct financial gain remain to be the main motives of cyber criminals. It is likely that the increase in cyber-attacks will remain a dangerous trend in future. Criminals will continue their attacks, targeting the less protected web resources to steal personal, medical and payment data.*
- *A dangerous trend is the increase in incidents caused by lowered cybercrime entry threshold, which is due to the growing number of cyber-attack tools and instructions being available on the Darkweb.*
- *In the foreseeable future, it is likely that social engineering combined with malware will be the main weapon of cybercrime.*
- *The most common method to implant the malware on the computers of users continues to be the phishing messaging. There is also an increase in cyber-attacks aimed at compromising credentials in cloud services.*

Information is the most important asset in the digital space. Protecting it against unauthorized access and preventing the use of confidential data for criminal purposes is a necessary condition for creating an environment of confidence and security, without which the potential of breakthrough technologies will not be experienced in full.

Cyber criminals use a broad variety of increasingly sophisticated tools, from spam to attacks on software and even hardware. Crimes that now happen on a mass scale include money theft, stealing of clients' personal data and information containing commercial secrets, interruption of operations of mobile services and applications, hacker attacks in the form of sending out malware and trojans, DDoS attacks, ATM disabling, blackmailing the owners of stolen credentials and personal data.

A dangerous trend is the increase in incidents caused by lowered cybercrime entry threshold, which is due to the growing number of cyber-attack tools and instructions being available on the Darkweb. A common type of cyber interference is hacking, or making changes (usually malicious ones) to the software for purposes different from the ones, for which the software was initially intended.

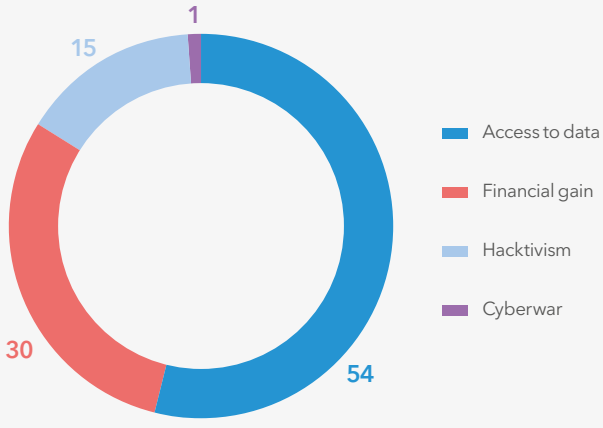
According to Positive Technologies[1], boundaries between cybercrime and other criminal activity are rapidly blurring. A large part of incidents is related not to direct money theft, but to stealing confidential information, when cracking the computer systems is the initial step, followed by fraud schemes and transactions causing financial, economic and even political damage.

[1] *See Cybersecurity threatscape 2018 // Analytical Report // Positive Technologies. – 2018; Cybersecurity threatscape – Q1 2019 // Analytical Report // Positive Technologies. – 2019.*

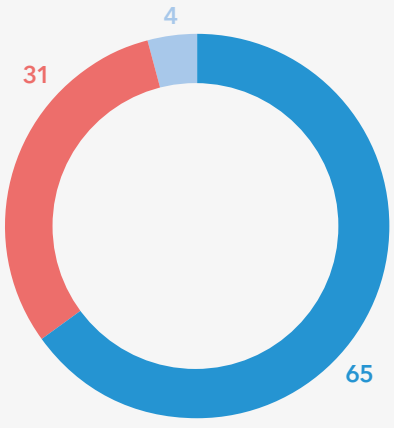
The main motive of cyber criminals in the bank and finance sector remains the direct financial gain (65% of incidents). However, the percentage of data theft has been growing at a higher rate. This is attributed to the fact that attacks aimed at data theft in most cases are also driven by financial motives: the stolen data are used afterwards to steal funds.

The main targeted system continues to be the processing of payment cards. Hackers try to get to the interface of the card processing control system, irrespective of its type, or to the database server, and to secretly increase the balances and limits of already issued cards that are in the hands of their accomplices. Then all funds accessible from those cards are withdrawn from ATMs. Data theft from financial organizations has now evolved into a multifaceted criminal business. Approximately 80% of all information sold on the Darkweb is represented by passwords and logins for various credentials, and the details of payment cards.

Motives of cyber criminals in the economic and social sphere, %, Q1 2019



Motives of cyber-attacks in the banking and finance sector, %, Q1 2019



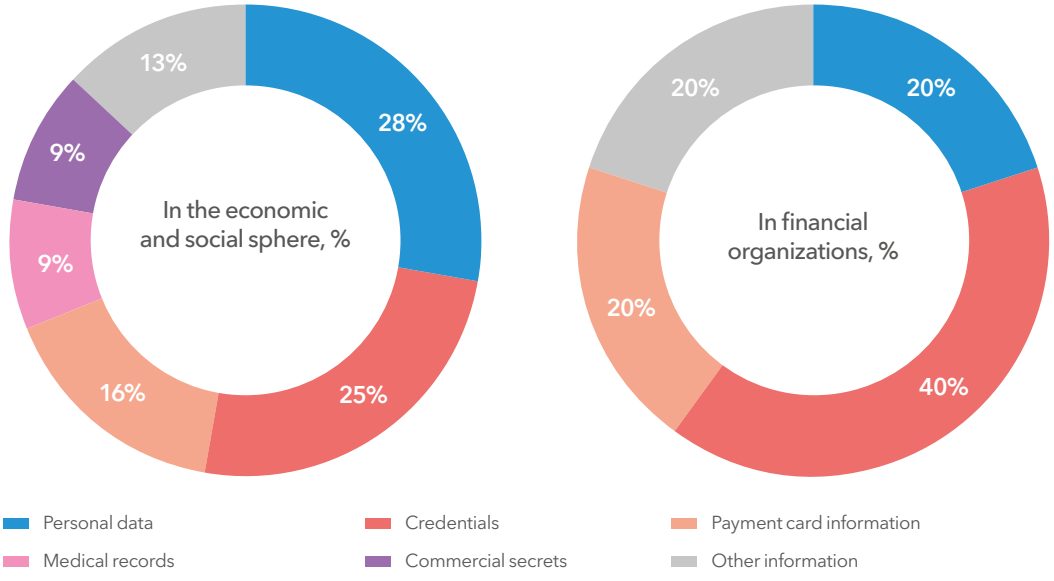
Source: Positive Technologies's data

Criminals are interested in all kinds of data - from personal correspondence to commercial secrets. In the economic and social sphere, the most attractive targets for cyber criminals generally are personal data and credentials. The statistically significant percentage of the theft of medical data and information containing commercial secrets has also been noticed by analysts. The dominating type of attacks in the banking and finance sector is the theft of payment card details.

Statistics demonstrate that data theft is, for all economy sectors and spheres taken as a whole, the main motivation of cybercrimes. Data theft accounts for 54% of all IT incidents, while the direct financial gain and hacktivism are responsible for 30% and 15% respectively.

The trend for increase in attacks aimed at data theft is likely to continue. Criminals will continue their attacks on the less protected web resources to steal personal, medical and payment data. Companies whose level of cyber security is not very high at the moment, such as, in the spheres of services, education, healthcare and retail trade, are in the high-risk zone.

Types of stolen data, %, Q1 2019

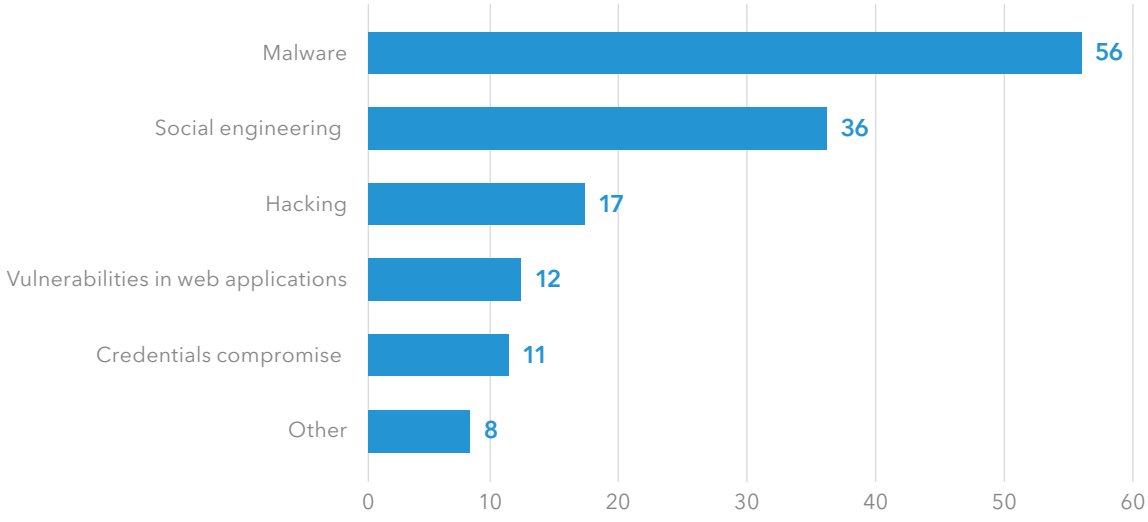


Источник: данные Positive Technologies

Cyber-attack methods do not remain unchanged. To break and bypass the information security system, cyber criminals use new malware or modifications of traditional viruses. They increasingly more often use complex multi-phase techniques, such as hacking the infrastructure of the partners, or infecting the resources of known software manufacturers, or a combination of several methods in the same attack.

A serious danger, especially for major companies and integrated production plants, is posed by attempts to infect not only the software, but also the hardware equipment. Malware is now used in 56% of cyber-attacks in the economic and social sphere. The percentage of its use in the banking and finance sector is even higher (65%).

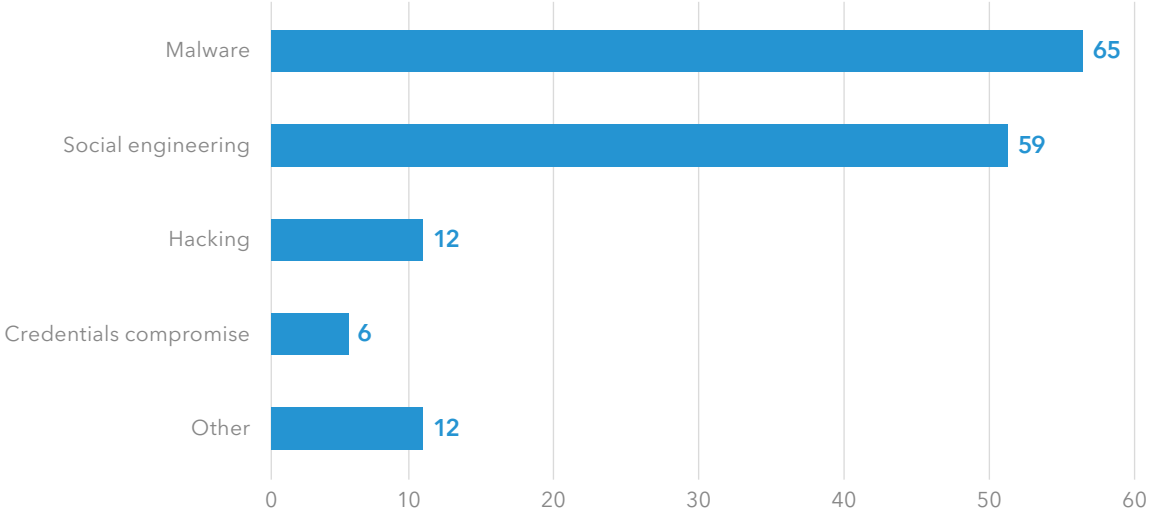
Cyber-attack methods in Q1 2019, %



Source: Positive Technologies's data

Hackers not only attempt to bypass the safeguards, but also cheat the users. The role of social engineering in attacks on organizations as well as individuals has significantly increased. Criminals use all kinds of communication channels – e-mail, messengers, telephone calls, SMS messaging and even the regular post service.

Cyber-attack methods in Q1 2019, %



Source: Positive Technologies's data

> *Social engineering is becoming one of the main methods for remote money theft from individuals. According to the estimate of BI.ZONE, 80% attacks on bank clients in Russia are performed with the help of social engineering. In most cases, the victims themselves transfer their funds to cyber criminals, usually lured by false sale advertisements.*

The most common method to implant malware on the computers of users continues to be the phishing messaging. The results of monitoring carried out by BI.ZONE show that 27-30% of the employees of Russian companies open e-mails with malicious attachments, allegedly sent by partners or colleagues. However, e-mail is not the only way to distribute malware. For example, users actively download files from torrent trackers, causing the risk of getting infected by a virus to increase many times. There is a notable increase in the cases where users were targeted by encryptors. This type of cybercrime is often used in combination with phishing.

One of the sources of income for hackers is the sale of credentials on the Darkweb. The more logins and passwords the hacker steals, the higher is his income, which explains why attacks involving password compromise have a mass character. It is alarming that there is an increase in cyber-attacks aimed at credentials compromise in cloud services (particularly, Office 365 and G Suite).

In the foreseeable future, it is likely that social engineering combined with malware will be the main weapon of cybercrime. Alongside with that, due to growing awareness of users about the fraudulent techniques, hackers will continue to develop new and more sophisticated schemes. In this situation, there is a clear demand for the improvement of computer literacy and digital culture of both people and businesses.

4.3. Biometric identification and the practical aspects of its use

- *The development of a unified biometric system in Russia began in 2017. During the initial stage, biometric templates can be registered only in bank offices.*
- *At the moment, the use of a biometric template is possible only for remote acceptance of a client by a bank.*
- *To reduce bank costs for launching this process into operation, it is possible to use cloud solutions for ensuring information security when working with the biometric data of citizens.*
- *It remains a challenge to determine the ways to inform the citizens of the Russian Federation about the benefits and functionalities of biometric identification.*

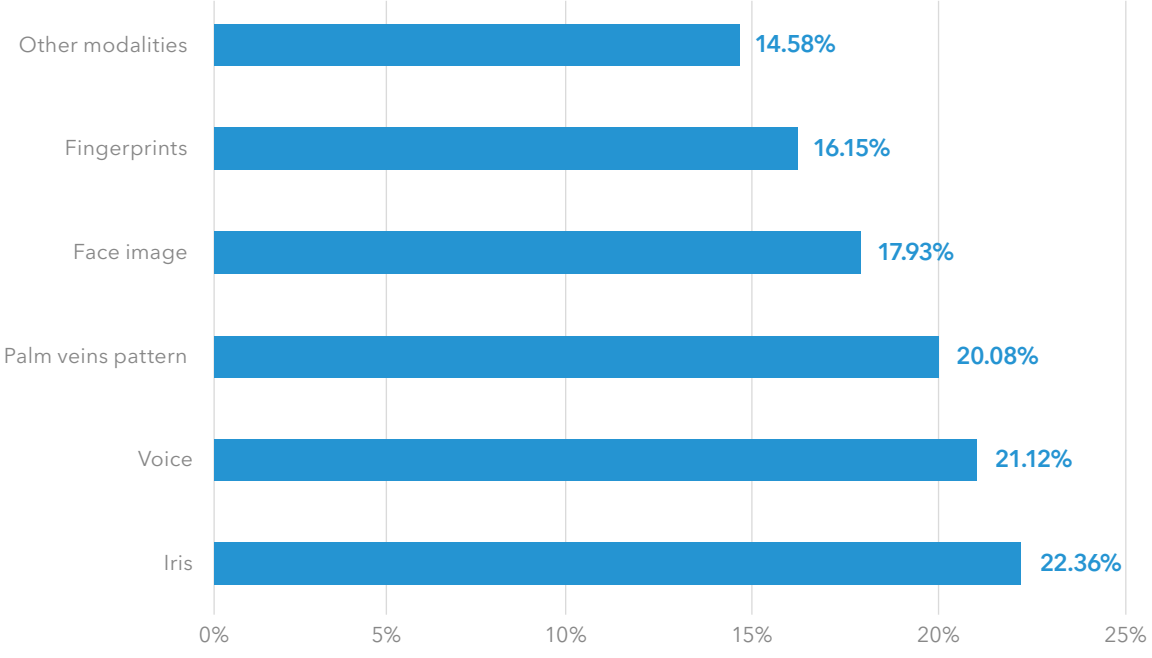
Biometric identification is an important part in digital technologies, banking services, and also provides access to services for people in remote regions (while maintaining their financial affordability). The global use of biometrics is actively growing both in the finance industry and in other sectors of economy. The growth rate of the biometric technologies market is high. There are grounds to believe that even in mid-term perspective most of the countries in the world will have remote banking services linked to a biometric database.

According to Sberbank Cybersecurity, global practices show that the probability of confusing one person's biometric data with those of another person varies depending on the type of biometric data, namely, for the face, veins, retina/iris and DNA this criteria is less than 0.1%, for fingerprints - 0.15%.

In any case, biometric data offer a much higher level of cyber security than the customary passwords. At the same time, the risk of non-coincidence with own data when using new biometry types (veins, retina and fingerprints) is less than 1%.

According to experts, it is expected that by 2022 the most widely used types of biometric data will be the iris (by 22.36%), the voice (by 21.12%) and the veins on the palm of the hand (by 20.08%). Please note that the fingerprints identification practice will grow at a rate lower than the rest of the biometric systems market until 2022. This is accounted for by the "high base" effect, as the share of this modality on the global market already exceeds 50%.

Forecast of the average annual growth rate of the biometric systems market with a breakdown by modalities until 2022



Source: Review of the global market of biometric technologies and their use in the finance industry // Central Bank of the Russian Federation. – 2018

On June 30, 2018, the Russian Federation introduced changes to a number of laws, allowing governmental entities, banks and other organizations, in cases envisaged by the law, to carry out remote identification of individuals on the basis of their biometric data[2]. At this stage, banks need to establish internal structural units, which will register biometric templates, by the end of 2019. Banks have been working to arrange the acquisition of clients' biometric data in their offices, and also to build processes which will allow registering an individual as a new client by using remote identification through remote service channels.

The experience that bank offices have accumulated in registering biometric templates allows identifying the following factors which impact not only the quality of those templates but also the overall process of registering such templates and the involvement of personnel:

- *qualifications of bank personnel involved in client services;*
- *awareness of clients about the benefits and functionalities of the unified biometric system and its difference from internal databases of biometric templates;*
- *creating a comfortable environment for clients during the collection of biometric templates;*
- *easily reachable bank offices authorized to collect biometric templates.*

Many clients, who come to the bank offices for consultation about the principles of the Unified Biometric System (UBS), had their misgivings about the transfer of their biometric template through a commercial bank. In this connection, it seems that it would be more acceptable if the biometric template service was provided through the MFC - Multi-Functional Centers for governmental services. This step would allow significantly accelerate the expansion of the UBS database, and to collect biometric templates not only for those individuals who come to bank offices.

In addition, banks are facing the need to provide constant training for personnel in their offices with a high attrition rate, and in "satellite" offices – small offices with 1 or 2 employees, which are additional to the main office in that locality. The constant turnover of personnel impacts the competence level of the bank's employees in charge of the collection of biometric templates. In particular, this has an impact on the ability of personnel to explain as clearly as possible the functionality and benefits of biometric identification, as well as on the speediness of template collection. To avoid this problem, a number of banks are establishing separate "anchor" offices with a comfortable waiting area and stable personnel, to which clients wanting a biometric template are routed from "satellite" offices.

A bill has been sent to the State Duma on postponement of imposing the obligation on banks with the basic license to collect biometric personal data from late 2019 to January 1, 2021

[2] *Federal Law dated 31.12.2017 No. 482-FZ "On Making Changes to Certain Legal Acts of the Russian Federation".*

The collection of biometric data and remote services based on the UBS require a change to the banking infrastructure, including IT modifications, in terms of information security. To arrange the process of remote identification and ensure the security of personal data, it is necessary to deploy additional material and financial resources. For that reason, this process goes more successfully in the large banks. It needs to be noted, however, that for most banks the cost of this process (especially the initial investment) is extremely high. Besides, most banks do not have enough qualified specialists on their staff to launch the process of biometric identification.

The mechanism of remote identification rests on a number of key concepts:

- *The establishment of the Unified Biometric System (UBS) and its integration with the unified identification and authentication system. There are four definitive features to the UBS: Universalism, Remoteness, Uniqueness, and Convenience.*
- *The technology is in conformity with the legal framework.*
- *A multi-vendor model is used to identify a fraud.*
- *The system detects that the biometrics is coming from a living human being (liveness).*
- *Separate storage of biometric data and personal data is provided.*
- *Biometric samples are stored in the protected part of the system.*
- *Protected data transmission channels are provided.*
- *The giving of biometrics is completely voluntary.*

Despite significant advantages of the biometric technology, experts foresee a number of problems in the process of its implementation. Firstly, there will be an excessive amount of profiles in the system. The more profiles are registered in the system, the harder it is to distinguish one person from another, which increases the risk of errors. Secondly, if for some reason the scanner is not able to distinguish a copy from a real person, it will be necessary to change the compromised credentials. Thirdly, before the biometric identification begins, it is necessary to ascertain that there is indeed a human being in front of the scanner rather than an attempt to present a copy of the person's biometric data.

To address the above-mentioned problems and threats, the regulatory authorities developed a program of activities to ensure the security of biometric data. When a person's biometric data are entered into the UBS, they are run through the anomaly module, which develops the profile of the user and the device, maintains the record of all operations and actions involving the user, assesses any anomalous behavior, responds to actions or operations, accumulates the machine learning and exploits external data sources.

The mechanism of remote identification implemented by the banking sector is universal and will be expanded in future to other spheres of finance market, such as the insurance sector, pension scheme providers, and the sphere of governmental and other services.

By the end of 2019, after necessary approvals received from regulatory authority, the cloud-based biometrics encryption method developed by Rostelekom will be deployed (for the face and voice) in the process when biometric data are transferred from banks to the UBS.

The idea of this technology is that the encryption key is stored on the cloud, so the biometric data from the bank are transferred to the cloud and from there to the UBS.

This cloud technique will be especially beneficial to the medium and small-sized banks, as they will not have to purchase the expensive equipment. They will be able to rent a space on the server, and the cost of server connection and support will be significantly lower than the cost of the bank's own solution for information security.

As it will take a certain time to deploy the processes involved in the collection and use of biometric data, a draft law has been presented to the State Duma of the Russian Federation, which delays the deadline after which the banks with a basic (restricted) license will be obligated to collect biometric data, from the end of 2019 to January 1, 2021.

4.4. The main challenges of cyber security

- *Governmental and business entities see the assurance of cyber security as one of their primary challenges. Data protection technologies become increasingly more advanced. At the same time, the methods used by cyber criminals are also getting more and more sophisticated.*
- *With the digitization of social communications, it is especially important to promptly disclose information on cyber-attacks and data leaks, so that appropriate actions could be taken to neutralize them.*
- *The complete disclosure of IT incidents can only be achieved if the government and businesses work together. The key to the solution of this problem is the improvement of the legal and regulatory framework governing the issues of cyber safety.*
- *An important challenge facing the cyber security industry is the shortage of qualified personnel and the increasingly high requirements for professional training on this subject.*
- *Outsourcing of cyber security scopes is becoming a visible trend both for organizations and for service providers.*

In recent years, there has been a notable progress in the sphere of cyber security in general and in safeguarding digital data in particular. Governmental and business entities see the assurance of cyber security as one of their primary challenges. Data protection technologies are becoming increasingly more advanced, the legal framework is developing and the level of digital literacy is growing.

However, life does not stop. New data transmission technologies are emerging, the boundaries of cyber-trade and cyber-finance are expanding, and the internet of things is invading our lives. At the same time, methods used by cyber criminals are also getting more and more sophisticated; the scale of cyber-attacks is increasing. According to the information (as of early 2018) of the anti-virus developer G DATA SOFTWARE, a new file with a malicious code emerges on the Web every 4 seconds.

Recognizing the necessity for consolidation in matters of information security, the Association of the Banks of Russia has rolled out a data exchange platform.

This platform allows the participants to receive verified and relevant information automatically in the online format. The benefits of this platform include the aggregation of more than 26 data sources about threats (FinCERT of the Bank of Russia, telecom operators, BI.ZONE), the downloading of only the useful information to protect the bank, and the automation of the process of using this information. The functionality of the platform can be used not only by large-scale businesses, but also by small-sized organizations which do not have advanced security systems or highly-qualified personnel.

As a result of pilot operation of this platform in 2018, the loss of at least 3 billion rubles was prevented. From 2019 the platform has been in commercial operation, and its basic version is free of charge for the Association members. More than 60 organization are connected to this platform already as of today. With the help of this platform, more than 55% of the bank system assets are reliably protected against threats, with banks in 22 regions of the country participating. According to the participants of the exchange, every week the security facilities of those banks register 3 or 4 attempts of attack on the average, based on the indicators downloaded from the platform.

The platform participated in the Cyber Polygon online training, where it demonstrated its high efficiency. After the platform had been deployed, the efficiency of the competition participants increased by more than 7 times.

The platform was demonstrated at the display of the International Cyber Security Congress - 2019, causing much interest among the participants, including those from oversees. Possibilities for information exchange have been discussed with representatives of the Association of the Banks of Italy, members of the International Banking Council, the Bank of Mozambique, some banks of Belarus and others.

With the digitization of social communications, it is especially important to promptly disclose information on cyber-attacks and data leaks, so that appropriate actions could be taken to neutralize them. The existing practice is that, due to the risk of losing their reputation and market capitalization, many companies hush up the incidents, and only disclose the facts after an investigation and remedial actions have been completed. Leaks might not be disclosed for weeks or months after they have been detected. In reality the losses caused by hackers are much bigger.

The task of full disclosure of information about IT incidents can be successfully solved only within the framework of effective interaction between the state and business

The goal of complete disclosure of IT incidents can only be met if the government and businesses work together. The key factor in the implementation of necessary actions is the improvement of the legal and regulatory framework governing the issues of cyber safety. In this regard, it is necessary to mention the importance of the European Union's General Data Protection Regulation 2016/679 (GDPR). Starting from May 2018, all companies working with personal data of the European Union residents are obligated to comply with standards when collecting and processing information about the users. A company is now obligated to report any data leak within 72 hours after the incident has been detected.

GDPR expanded the coverage of the European legislation, detailed the rights of the subjects of personal data and tightened the requirements for operators involved in the processing and protection of data, taking into account new technologies. The requirement for compliance with GDPR applies not only to companies operating in the 28 EU countries, but also to any companies irrespective of their location. Any individual on the EU territory is automatically entitled to having their personal data protected in accordance with GDPR, regardless of their citizenship. GDPR does not require any national laws to be put in place, and applies to the operators directly.

GDPR makes the web industries significantly more transparent. The new regulation obligates companies to report problems immediately, or pay a penalty amounting to 20 million Euros or 4% of revenue, whichever is higher. This practice is already in actual use. For example, in January 2019 the French government charged Google the sum of 50 million Euros for non-compliance with the GDPR. Just in the first few months after the new regulation had been put in place, the relevant watchdogs in the EU received almost 60,000 reports of data leaks. It is important to note that the GDPR also defines the cases of personal data processing, with respect to which the operator, when planning such activities, must carry out a Data Protection Impact Assessment (DPIA). If the DPIA results show that the data processing is associated with a high level of risk for the subjects, the operator must consult with the regulatory authorities prior to the start of data processing.

A number of laws and regulations have been put in place in Russia in recent years, showing the intention of the government to set forth unified standards of cyber security in the key sectors. In 2018, the Federal Law dated 26.07.2017 No.187-FZ 'On the security of the critical information infrastructure of the Russian Federation' came into force. This law determined which governmental entities and companies should regard their networks as critical and how they should protect them. The law obligates the responsible organizations to report incidents to the authorized governmental agency and to undergo a security assessment.

In May 2018 the Bank of Russia made amendments to its Regulation No.382-P, dated June 9, 2012, 'On the requirements to protect information related to funds transfers and on the procedures for the Bank of Russia to control the compliance with the requirements to protect information related to funds transfers', in which the regulator set forth the cyber security requirements for all financial organizations. In particular, banks must use only certified software for their transactions, must carry out a security review every year and must inform the Bank of Russia about incidents. The specific feature of this law is that it protects organizations against attacks motivated purely by financial gain. In January 2019 the Bank of Russia Regulation No. 672-P, dated 9 January 2019, 'On requirements for data protection in the Bank of Russia payment system' came into force.

In 2018, the Bank of Russia enacted its Standard 'Safety of Financial/Banking Operations. Managing Information Security Incidents' which defines the forms and time lines of the Bank of Russia's engagement with the participants of information exchange to identify incidents involving violation of information security requirements. Compliance with this Standard is monitored by the Financial Sector Computer Emergency Response Team of the Information Security Department of the Bank of Russia (FinCERT) created in June 2015 for the purpose of ensuring information security during financial operations.

In this regard, one of the Team's main lines of activities is to support the information exchange between the participants of the financial market, which include banks and other credit institutions, system integrators, anti-virus laboratories, telecom providers, telecom operators, law-enforcement agencies, incident response groups, etc. In 2018 the total number of information exchange participants included 718 organizations, more than 70% of which were banks[3].

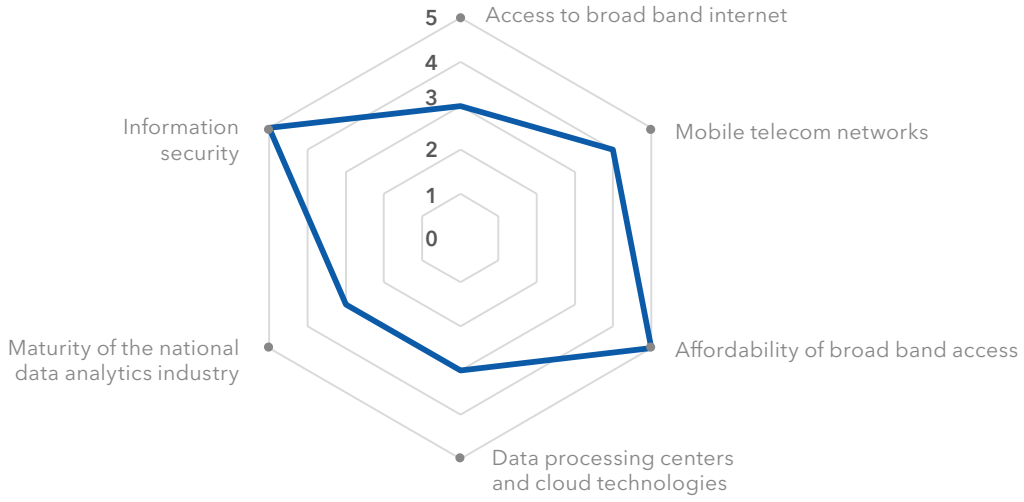
FinCERT collects and processes information received from the exchange participants regarding the attacks that had taken place or had been averted, details of the manner and method of attack, persons who had been accessory to the attack, and data on the victims - legal entities and individuals. Afterwards this information is analyzed by the Team, and the participants are promptly informed of the cyber threats. The summarized data on the main types of cyber-attacks in the banking and finance sector are published in open press[4].

[3] *Report of the Financial Sector Computer Emergency Response Team of the Information Security Department of the Bank of Russia. // Central Bank of the Russian Federation. – 2018. P. 4.*

[4] *Review of the main types of cyber-attacks in the banking and finance sector in 2018. FinCERT, Bank of Russia, 2019.*

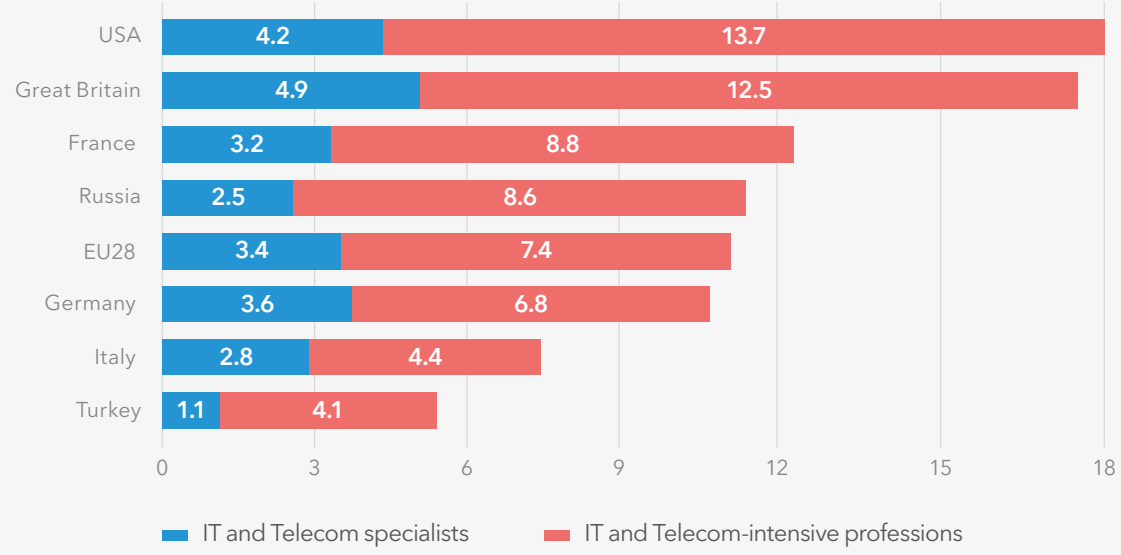
The report of the World Bank on the digital economy development in Russia 'Competition in the digital age: strategic challenges for Russia' (September 2018) presented an assessment of the readiness of digital infrastructure for the digital economy. For two of proposed criteria – information security and the affordability of broad band internet – Russia received the highest grades. The objectivity of this assessment is confirmed by the fact that Russia is on 10th place in the Global Cyber Security Index of the International Telecommunication Union. The implementation of the governmental program 'Digital Economy' will help strengthen and improve Russia's position in this ranking.

Assessment of Russia's readiness for digital economy: digital infrastructure



Source: "Competition in the digital age: strategic challenges for Russia", by World Bank, September 2018, p.7

Percentage of workers employed in digital economy professions in 2018, %



Sources: Institute for Statistical Studies and Economics of Knowledge of the National Research University and the Higher School of Economics

In comparison with the OECD countries, Russia looks comparative good in terms of the employment rate for digital economy professions. According to the OECD methodology, such professions include not only IT and Telecom specialists, but also others whose job responsibilities imply the use of computer technologies, including work on the internet. The number of workers employed in professions involving active use of information and telecommunication technologies (IT and Telecom) in Russia in 2018 exceeded 8 million, or 11.1% of the total number of employed people. At the same time, IT and Telecom specialists constitute only 22.1% of all people employed in 'digital' professions, or less than 1.8 million people. In this criterion, Russia is behind most of the OECD countries.

Another important challenge facing the cyber security industry is the shortage of qualified personnel and the increasingly high requirements for professional training on this subject. According to Ernst & Young, a consulting company, by 2023 the shortage of cyber security specialists will reach 1.8 million persons. Countering this shortage will require the establishment of an integrated system for training and re-training of personnel.

With the shortage of personnel and limited amount of financial resources, the solution to the problem of information security can be improved by outsourcing, which is becoming a noticeable trend in cyber security both for organizations and for service providers. To be able to provide adequate protection and response to the threats, companies need qualified professionals and significant investments. The specialists, on the other hand, need to be constantly on the guard for new malicious software and the vectors of cyber-attacks, which is impossible without a stable flow of incidents.

Medium-to-small-sized companies, as a rule, are not hit by attacks too often, and do not have the financial resources to keep the required professionals on their payroll. Such companies would benefit from hiring firms specializing in cyber security. As for major companies, they face a different problem, i.e., shortage of personnel. So, even for big business outsourcing becomes a necessity.

The tightening requirements for cyber security compliance and audit also encourage businesses to turn to external experts. New legislative initiatives are designed to strengthen the supervision over compliance with the cyber security requirements. This means that organizations will increasingly need professionals in this specialty.

According to Ernst & Young consulting company, the shortage of cyber security specialists will reach

1.8 million by 2023

5

Development of regulatory environment for the banking activities in transition to digital technologies

Pursuant to Federal Law No. 86-FZ On the Central Bank of the Russian Federation (Bank of Russia) dated 10.07.2002, banking regulation and oversight are mainly aimed at maintaining stability of the RF banking system and protecting the interests of depositors and lenders. The incentive-based regulation of the banking business[1] is established to assist in addressing two inter-related tasks, namely, boosting of the economic growth and assurance of financial stability. Depending on which task takes priority, changes in the regulatory environment take place developing a system of incentives and disincentives which reflects specifics of the present. The regulatory burden should in turn account for specific features of various lenders' groups according to the amount of capital, scale of business and assumed risks. At the same time, current development of the regulatory environment is meant to contribute to a phase-by-phase transition of the banking industry to the digital dimension.

5.1. Current tasks faced by the incentive-based regulation

- *A decision was made by the Bank of Russia to limit financing by banks of merger and acquisition transactions for reasons of being discouraging of the economic growth.*
- *The Bank of Russia is currently changing to a new standardized approach to credit exposure assessment. An 'alternative' option of transition to a new credit exposure assessment standard chosen by the Bank of Russia has however stirred a dispute with the Russia's Ministry of Finance.*
- *The Bank of Russia's Board of Directors[2] were vested with new powers, permitting them to establish buffers to risk ratios for the purpose of macroprudential control. A capability for exerting a prompt impact on the financial system granted to the banks has aggravated the need for expansion and improvement of sharing of data between the banks and information systems, primarily state-run.*
- *A Working Group is established in the Bank of Russia whose function will be to consider possibility for cancellation of outdated and excessive requirements contained in the Bank of Russia's regulations. This will put in action some sort of a 'regulatory guillotine'.*

[1] *This was for the first time defined in the Report by the Bank of Russia entitled «Incentive-Based Banking Regulation» in 2018, although some elements were earlier implemented in several regulatory instruments and federal laws.*

[2] *In accordance with Federal Law No. 53-FZ On Amendments to Certain Statutes of the Russian Federation dated 07.03.2018 and Instruction by the Bank of Russia No. 4892-u On the Types of Assets and Characteristics of the Types of Assets that are Subject to Setting Buffers to Risk Ratios and Methodology for Application of Buffers to Such Asset Types to Allow Calculation of the Capital Adequacy Ratio by Lenders dated 25.09.2018 issued in pursuance thereof.*

The Bank of Russia's innovations of 2019 focus on maximizing the role of incentive-based banking regulation that, as the world practice shows, aims at encouraging the well-balanced economic growth through the use of the 'checks and balances' driver.

The prudential regulation and supervision of reserve creation continues to diversify the approaches to reflect specifics of certain customer segments. Specifically, concerning loans to the real-estate developers who use escrow accounts to receive funds from equity construction investors, the approach used deviates[3] from the standard one focused on the assessment of the borrower's solvency and debt servicing shifting to the assessment of the project to be pursued. For implementing the Bank of Russia's Roadmap to develop financing of small and medium-scale entrepreneurs. A new approach to creation of provisions for small loans and small & medium scale entrepreneurs' commitments has been developed and is currently pending the approval thereunder banks can create provisions based on the bank in-house solvency assessment models, e.g. transactional models, without the need to use any official reports from such small and medium-scale entrepreneurs. The above diversification and the statistically confirmed low default rates existing in the market determine the projected changes in the minimum rate of provisions for small (up to RUB10 mln) guarantees to government contract bidders.

In June, the Bank of Russia published a draft regulation whereby from October 1, 2019 and on, any loans granted for merger and acquisition (M&A) transactions will be automatically classified as the third quality category, i.e. doubtful loans. Such loans will require creation of provisions of 21% to 50%. The reserve can be reduced if the funds are invested into the companies' capital under Federal Target Programmes or the capital of strategic industrial enterprises and where secured or guaranteed by the Russian Federation. Loans can be reclassified as the second quality category if the borrower's operational performance proves that the principal debt and interest payments will be made on time and in full. However, even in this case, the amount of reserve should be at least 5%.

The Bank of Russia also plans to introduce restrictions on investments by banks into nonfinancial sector's equity securities. The Regulatory Authority intends to increase risk ratios from 150% to 400% for unlisted equity securities and up to 250% for listed securities. The Bank of Russia plans to increase such ratios step by step beginning in 2020.

[3] *Instruction by the Bank of Russia No. 5043-U On Amendments to the Bank of Russia Regulation No. 590-P dated June 28, 2017 «On Procedure for Creating Reserves for Potential Loss on Loans, Loan and Equivalent Debts by Lenders» dated 26.12.2018.*

At the same time, the Bank of Russia has already introduced the incentive-based measures into the investment financing. The instruction by the Bank of Russia No. 5137-U On Amendments to the Bank of Russia Instruction No. 180-I dated June 28, 2017 "On Regulatory Ratios for Banks" dated 06.05.2019 in particular reduces risk ratios from 100% to 20% for loans in roubles under VEB.RF guarantees. This is done to attract more banks to participate in the programmes run by the "VEB.RF Project Financing Factory" and other large projects, including through the use of the syndicated lending potential as part of the public private partnership. The anticipated benefit of such regulatory innovations is in providing the economy with long-term money from the funds released as a result of the loan restrictions introduced in respect of M&A transactions.

Experts predict a potentially limited effect from the decision by the Bank of Russia on discouragement of financing by banks of investments into the company capital where this brings no economic growth. Such loans account for no more than 10-15% of total loans over the entire banking system. They are mainly concentrated in the largest banks, more specifically, banks partially owned by the government. This innovation will not bring an instantaneous growth of as the intent is to apply it to new loans that will be granted after October 1, 2019.

The increased provisions for loans for M&A transactions will at best force banks to turn down high-risk transactions but will never turn the banks away from the transactions with large and reliable borrowers. Loans to such borrowers constitute only an insignificant share that will not affect the capital adequacy performance. It should also be noted that loans to industrial businesses and M&A transactions seek to achieve different purposes. The thus released funds will not necessarily be allocated to finance nonfinancial economy.

There are some concerns currently that more stringent prudential requirements to banks in respect of financing of M&A processes can complicate economically justified transactions which, among other ways, are funded by issuing market bonds. Such requirements can also have restraining effect on financial ecosystems whose growth is largely supported by such transactions and on alliances between fintech companies and the banks.

As the simplified standardized approach of the Basel Committee on Banking Supervision pursued by the RF banking regulation suggests, the Supervisory Authority's capabilities for use of incentives in determining the risk ratios for calculation of capital adequacy ratios are currently limited and therefore the tools used by the incentive-based regulation consist mostly of disincentives, that is, higher risk ratios. The simplified approach means that the minimum risk ratio for loan debts of legal entities that do not pertain to portfolio loans granted to small and medium-scale entrepreneurs is established at 100%[4]. A lower ratio may be applicable in respect of the public debt in roubles supported by the state guarantee.

[4] *Consequently, according to international financial organisations and the Bank of Russia, the RF banking system shows the maximum (over 90%) ratio of risk-weighted assets to assets. The countries with the economies comparable in sustainability demonstrate lower ratios, compare 72% in Greece, 59% in Portugal, 49% in Italy, an average of 57% in BRICS (less Russia) and 33% in Germany and the United Kingdom.*

In developing the banking regulation to encourage credit support of the economy, since 2019 the Bank of Russia has been carrying out a phase by phase change of the procedure for calculation of a bank capital adequacy ratio, turning away from the simplified standardized approach and implementing a new standardized approach to the loan rick assessment.

During the first phase of transition completed in this June, the Bank of Russia issued an Instruction No.5137-U dated 06.05.2019 whereby the risks of sovereign borrowers are now assessed based on external long-term solvency ratings rather than OECD's country ratings.

In June 2019, the Bank of Russia started to proceed with the second phase having posted on its web site a draft instruction entitled "On Regulatory Ratios and Buffers to Capital Adequacy Ratios for Banks with General Licenses" that will have to substitute two effective instructions at the same time, that is, "On Regulatory Ratios for Banks" and "On Regulatory Ratios of Lenders Issuing Mortgage-Secured Bonds". This Instruction changes the approach to assessment of the borrowers' loan risks based on the Basel Committee's recommendations, widening the capabilities for application of low risk ratios to RWA (risk-weighted assets) calculations, but at the same time, tightening the liability of banks for incorrect assessment of their solvency, thus in fact introducing penalties.

The Bank of Russia's draft instruction "On Regulatory Ratios and Buffers to Capital Adequacy Ratios for Banks with General Licenses" addresses a wide range of issues, including assessment of corporate borrowers' risks and risks on speculative investments. It also reduces risk ratios for small and medium-scale businesses and project financing. The Instruction covers calculation of the regulatory limit for a minimum mortgage pool ratio and the issue of mortgage-backed bonds. In the meantime, the Instruction cancels the limit for an aggregate risk for bank's insiders and adjusts the calculation of liquidity ratios. It introduces lower risk ratios for asset classes which will make it possible to grant more loans without increasing the capital. A coefficient of 0.65 is introduced for large corporate borrowers and 0.85 for non-portfolio loans to small and medium-scale businesses. A class of non-financial guarantees (e.g. contract/agreement performance bonds and guarantees in favour of customs (tax) authorities) with the loan conversion coefficient of 0.5 (instead of 1) is distinguished.

[5] *Subject to compliance with two conditions at the same time, one relating to the loan quality category (Quality Categories I or II in accordance with the Bank of Russia's Regulation No.590-P dated 28.06.2017 «On Procedure for Creating Reserves for Potential Loss on Loans, Loan and Equivalent Debts by Lenders») and the other relating to inclusion of securities into the quotation list made by tender organizers.*

The Draft Instruction also establishes a number of more stringent conditions. Specifically, it establishes a loan conversion coefficient of 0.1 (instead of 0) for loan-related contingent liabilities. Where a payment for an unsecured loan for which a reserve of lower than 20% is made (Quality Group I) becomes overdue for longer than 90 days, such loan becomes subject to application of a risk ratio of 150%. The currently applicable risk ratio for such loans is 100%. This in fact means that the Bank of Russia intends to fine a bank for any incorrect assessment of the borrower's solvency irrespective of whether this is a mistake or the bank intentionally underestimates the created reserves.

One of the factors hindering the use of the solvency rating-based methodology as the principal approach is the lack of any ratings in overwhelming majority of Russian borrowers. Only a few hundreds of corporate borrowers were assigned ratings. These mainly include issuers of securities that are traded in the market. Meanwhile, tens of thousands of companies will have to be rated which as of today exceeds the capacity of existing agencies (there are currently only two accredited rating agencies in Russia). Another hindrance reported by some analysts is that these agencies have no accumulated valid default statistics, and hence no official correlation scale between national and international ratings. Besides, when it comes to comparing Russian and international agencies' ratings, even the best Russian borrowers would bump into the country ceiling (now BBB on S&P scale).

Application of this new approach is estimated to allow banks to release some share of their capital and grant affordable loans to the borrowers. Experts believe that these new requirements may cause the loan portfolio to grow by 10% without increasing the burden on the capital. The 'alternative' option of change to the new loan risk assessment standard chosen by the Bank of Russia (based on the criteria that include the requirement for marketability in accordance with paragraph 42 of the Basel Committee on Banking Supervision's document) was however challenged by the RF Ministry of Finance who deems it necessary to use the arrangement that relies on the assessment of the borrowers by rating agencies rather than by banks.

This means that bearing in mind that the rated companies whose securities are traded in the market are roughly the same circle of companies, options from the Bank of Russia and the RF Ministry of Finance in respect of the change to a new standardized approach to the loan risk assessment apply to the same group of borrowers.

At the same time, the potential for national agency ratings to be applied for the purpose of prudential control and the amount of capital to be potentially released depend on the certainty of rating scale mapping and the ability to ignore the country ceiling. This requires a fundamental decision falling outside of the Bank of Russia's powers.

Alongside with that, an internal rating-based approach to the assessment of loan risks is becoming more and more common. Such approach is believed to be more advanced, yet only two banks, PJSC Sberbank and JSC Raiffeisenbank, are currently using it. Similar methodologies have been developed and applied by other systemic lenders to make reports for the Bank of Russia. They are however used only for information purposes. An authorisation from the Bank of Russia has to be obtained for use of internal ratings in the bank business. For this, the subject bank has to present to the Regulatory Authority the internal rating calculation methodology and defend it. Development and implementation of internal rating-based models are extremely labour consuming. The major costs are incurred when preparing data, adjusting and validating the internal rating-based model. However, a number of large Russian banks are expected to be using this approach to assess loan risks in the foreseeable future which will make it possible for them to reduce the burden on capital and release funds for lending to the economy.

For calculation of capital adequacy ratios, the two types of risks, credit and systemic, were distinguished in the banking regulation in 2018. Federal Law No. 53-FZ vests the Bank of Russia's Board of Directors with powers for determining the amount of buffers to risk ratios as a measure aimed at reducing the threat to financial stability of the Russian Federation (an amendment to the regulation was required earlier). The description and types of the assets that are subject to application of a buffer are defined in the Bank of Russia's Instructions No.4892-U[6] dated 31.08.2018 and No.5072-U[7] dated 12.02.2019 In general, the buffers are applicable to consumer and home loans to individuals, real estate building and purchase loans to legal entities, foreign currency loans and liabilities and the buffer matrix takes account of the loan issue date, claimed currency and the ranges of the debt burden performance, true interest cost and LTV.

Thus, the main tool used by the Bank of Russia for macroprudential regulation is the sectorial buffers to risk ratios to ensure stability of the banks through establishing additional allowances to cover any loss incurred due to occurrence of internal or external risks (another tool, countercyclical buffer, is not currently used due to the low growth rate demonstrated by corporate lending) and as such buffers may have only positive values (or be equal to zero), the available tools are limited with disincentives.

The fact that the vast majority of Russian borrowers have no ratings is the major setback to using the approach based on credit scoring

[6] *On the Types of Assets and Characteristics of the Types of Assets that are Subject to Setting Buffers to Risk Ratios and Methodology for Application of Buffers to Such Asset Types to Allow Calculation of the Capital Adequacy Ratio by Lenders.*

[7] *On Specifics of Application of Buffers to Risk Ratios for Certain Types of Assets by Lenders that Assumed Obligation to Apply Bank Risk Management Methodologies and Quantitative Risk Assessment Models for Calculation of Regulatory Ratios.*

Another significant change relating to the exercise of powers in respect of incentive-based regulation to reduce the household debt is charging banks with the responsibility for calculating debt burden performance to determine macroprudential buffers to the liabilities of individuals. From October 1, 2019, lenders will have to calculate the debt burden performance on new loans in accordance with the requirements in Instruction by the Bank of Russia No.4892-U and, subject to the buffer matrix set by the Bank of Russia's Board of Directors, weigh requirements to individuals.

On the one hand, the earlier dependence of a risk-weight solely on the true interest cost, being not a comprehensive measure of risk but rather a measure of the loan cost, that is, the metric that aggregates funding, insurance and other costs, raised criticism from active household lenders which made transition to the use of debt burden performance in the banking regulation welcome.

On the other hand, the approaches to estimation of personal incomes established in the Instruction by the Bank of Russia No.4892-U that differ from more advanced models established in the market used by lenders fail to take account of 'non-official' incomes. A robust automation of business processes requires well-adjusted interaction with the Russian Pension Fund and Federal Tax Service. Currently, the RF Tax Service does not provide any information on personal incomes to lenders despite that the Annex to Russian Federation Government Decree No. 1471-r[8] dated 15.08.2012 (as amended on 03.10.2017) lists information from the personal income statement (2-NDFL) and personal income tax return (3-NDFL) as the information to be provided to applicants via IEIS (Interdepartmental Electronic Interaction System). Sharing of information with the Russian Pension Fund for estimation of personal incomes is currently available only to a limited number of banks. The respective mechanism is imperfect and low-tech and the information on insurance contributions is less helpful for estimation of incomes than tax data.

Improvement prospects are associated with the execution of the Digital Profile project and cooperation between governmental bodies and certain financial market players as part of the pilot project defined in the RF Government Decree No. 710 dated 03.06.2019[9]. At the same time, the list of data to be shared under this pilot project contains only the status of the personal pension account of the insured from the Russian Pension Fund but not the personal income data from tax authorities.

From October 1, 2019, Credit organizations must calculate the Debt Burder Indicator (DBI) to apply to new loans and, depending on the surcharge matrix, weight requirements for individuals

[8] *On Approval of a List of Documents (Information) Shared Using a Unified Interdepartmental Electronic Interaction System.*

[9] *On Experiment to Improve the Quality and Connectivity of Data Contained on Governmental Information Resources (together with the Regulation on Experiment to Improve the Quality and Connectivity of Data Contained in Governmental Information Resources).*

Besides, for calculation of the debt burden numerator to estimate an average monthly payment amount of a borrower for all loans, efforts should be undertaken to improve interaction of the banks with the Credit History Bureau system, including streamlining of the information already contained in various bureaus. It is expected that this will bring significant changes in the loan history legislation. A Bank of Russia's Roadmap to improve the debt burden performance and ensure oversight of financial institution activities in respect of the use of individual borrower's debt burden performance assumes that comprehensive upgrade of the existing credit history system will end up in Quarter IV 2020 and will be followed up by several other actions.

Therefore, in the coming year the infrastructure set from 01.10.2019 to assist lenders in calculating the debt burden performance imposed on them cannot be considered as adequate, so all further efforts to update formats and services by information providers will force banks to continuously update their own IT systems in response.

It should be noted that a Working Group is established in the Bank of Russia whose function will be to consider possibility for cancellation of outdated and excessive requirements contained in the Bank of Russia's regulations. It is expected that the above review will cover the outdated standards overlapping in the control system, replicating each other and raising arbitration. This will put in action some sort of a 'regulatory guillotine'.

5.2. Regulatory and oversight technologies under digitalization of the financial sector

- *The Basel Committee on Banking Supervision, Financial Stability Board and national oversight bodies act cautiously when working out regulatory requirements for bank operations involving the use of financial technologies.*
- *Certain experience gained to date makes it possible to roughly outline a regulatory paradigm to be adhered to under digitisation of financial services. It is more and more confirmed that oversight bodies take the "same activity, same regulation" principle as their guide.*
- *In response to swift changes in the pattern of banking operations and nature of regulatory requirements, new control and oversight formats known as RegTech (Regulatory Technologies) and SupTech (Supervisory Technologies) have been developed.*
- *Application of these technologies is still under pilot testing in various countries. As such, bank control and oversight bodies are more than interested to receive some feedback from the professional community.*
- *In October 2018, the Bank of Russia published an advisory report entitled "Issues and Ways Forward for Development of Regulatory and Supervisory Technologies (RegTech and SupTech) in the Russian Financial Market". Requested by its members, the Association 'Russia' conducted a survey and discussion of this document at a joint session of dedicated committees.*

The growing use of innovative technologies in financial sector challenged regulatory authorities to work out new approaches for exercise of their oversight powers. This primarily involves banking industry where the activities are licensed and the supervision is prudential. The Basel Committee on Banking Supervision (BCBS), Financial Stability Board (FSB) and national oversight bodies act cautiously when working out regulatory requirements for bank operations involving the use of financial technologies.

In 2017, the Basel Committee on Banking Supervision (BCBS) published an advisory report entitled "Sound practices: Implications of fintech developments for banks and bank supervisors". The Report considers various future potential scenarios, with their specific risks and opportunities. In addition to the banking industry scenarios, three case studies focus on technology developments (big data, distributed ledger technology and cloud computing) and three on fintech business models (innovative payment services, lending platforms and neo-banks). It is noted in the Report that banking standards and supervisory expectations should absorb innovations while adhering to relevant prudential standards. Against this backdrop, BCBS identified key observations and presented recommendations for consideration by banks and bank supervisors.

Such approach is fairly well warranted for the first digitisation phases of the banking business. Premature actions of supervisors may double the negative effects. They can slow down the development of forward-looking banking service technologies and stimulate creation of alternative methods for banking operations outside of the supervisors' field of supervision. This is why in many countries, including Russia, supervisors choose to pursue the creation of regulatory platforms, known as regulatory sandboxes. A special legal regime is established for such sandboxes that allow the institutions to conduct experiments in a limited environment, introducing new products and services based on financial technologies without the risk of violating any effective laws. And for innovative solutions, it is allowable not to have any or be only partially covered by bylaws.

Using RegTech and SupTechtech technologies is still in the testing mode is some countries. One can expect a consultation documentto be drawn up in the years to come by the Basel Committee on BankingSupervision or Financial Stability Board to synthesize the best world practice

The first regulatory platform in the financial industry was de facto established in the United Kingdom in 2016. During the first streams of experiments, a total of 146 applications from candidates were received of which 50 were approved by the supervisory body. Forty one applications have successfully passed the testing. The distributed ledger technology (DLT) was the most common of all the tested technologies. Such platforms have to date been established in many countries. In April 2018, the Bank of Russia announced the launch a regulatory platform and later, in February 2019 with the first results in hand, shared information on the projects pursued by the supervisor.

Such regulatory platforms are in use not only in the financial industry. Specifically, Russia has developed a draft federal law entitled "On Experimental Legal Regimes for Digital Innovations in the Russian Federation and Amendments to Certain Statutes of the Russian Federation". This draft law covers organisations and areas that implement special methods of regulatory controls for industrial production, business and other types of activities to promote digital innovations. This will allow the companies and some executive & local government bodies related to digital innovations to use such innovations in practice during a certain period of time and test their usefulness in an environment free from any restrictions established by regulatory requirements, without the risk of violating them. This will help fintech companies set the rules for the development of new technologies in order to be able to place such new solutions on the market more efficiently.

Certain experience gained to date makes it possible to roughly outline a regulatory paradigm to be adhered to under digitalization of financial services. It is more and more confirmed that oversight bodies take the "same activity, same regulation" principle as their guide. The same principle applies not only to global Big Techs. Data collected by the Bank for International Settlements prove that many countries introduce compulsory licensing for organisations pursuing different fintech lending models (P2P, B2B, B2P and others), fundraising and providing other banking services.

The approach to the bank licensing institute is also changing. What is new about it is that so-called "fintech licenses" are issued to the types of banking services rather than legal entities, and that for digital payment systems, non-banking licenses are issued. Several countries followed the same route (Switzerland, Hong Kong and others). However, one should not overestimate this initiative. For example, in Germany, the well-known Mobile Bank No.26 that was acting under conventional banking licenses was issued a dedicated banking license when so requested by the supervisor. Nevertheless, the Bank of Russia expressed its willingness to discuss whether it is appropriate to issue "fintech licenses".

Development of new standards for anti-money laundering and combating the financing of terrorism (AML/CFT) is becoming one of key regulatory trends. A new revision of the money-laundering directive (5MLD) will be enacted in January 2020 that will introduce more stringent requirements to examining ultimate beneficiaries of the companies and high-risk country clients. This 5MLD will also focus on the platforms trading crypto-assets and online services of cryptocurrency wallets. Besides, mobile banking dealing with pre-paid payment cards should take into account that the 5MLD envisages more serious examinations and new restrictions for such payment tools. This new revision of the directive sets a limit of 150 Euros on the balance available on the card and 50 Euros on online transactions. In contrast to conventional banks, it is harder for digital financial intermediaries to achieve proper balance between mobility of their operations and more stringent AML/CFT requirements. They are restrained by the budgets and the lack of competent personnel. What is equally important is that to the large extent the compliance is not about the reliability of technologies but rather about the corporate culture.

The emergence of fintech has resulted in complication of the operations and growth of processed data volumes. It gave rise to new nonconventional financial services which brought further tightening of regulatory requirements and added new statements to the report package. This caused an increase in the expenses by lenders and finance institutions to enforce these requirements. In response to swift changes in the pattern of banking operations and nature of regulatory requirements, new regulation and oversight formats known as RegTech (Regulatory Technologies) and SupTech (Supervisory Technologies) have been developed.

RegTech refers to the use of innovative technologies by financial institutions to improve efficiency of regulatory compliance and risk management and facilitate adherence to regulatory requirements by financial institutions. RegTech technologies are able to make it possible for financial institutions to optimize compliance with the supervisor's requirements, including preparation of necessary reports, accelerate and enhance reliability of the client identification processes, improve the quality of transaction analyses and ensure control of the level of risks and combat of cyberthreats.

According to the world practice, most common applications of RegTech include:

- *checking that supervisor's requirements are met, or compliance control;*
- *identification of customers and monitoring of transactions;*
- *protection of information, audit of systems;*
- *management of risks and corporate management;*
- *submission of reports.*

SupTech are the technologies used by supervisors to improve efficiency of control and oversight of activities of financial market players. SupTech technologies are used by a financial oversight body to automate and simplify administrative procedures, convert the data and the tools intended for interaction with financial market players into digital format, enhance credibility and quality of the reported information and improve the decision-making support system. Two SupTech major application domains are globally identified:

- *collection of data – periodic collection and processing of information obtained from supervised institutions;*
- *analysis of data – analysis of obtained data sets to assess whether the activities of supervised institutions comply with regulatory requirements.*

Application of these technologies is still under pilot testing in various countries. It is likely that a BCBS or FSB-based advisory report summarising the world best practice will be developed in the near future. As such, bank supervision authorities are more than interested in receiving some feedback from the professional community.

In October 2018, the Bank of Russia published an advisory report entitled "Issues and Ways Forward for Development of Regulatory and Supervisory Technologies (RegTech and SupTech) in the Russian Financial Market" for open discussion. Requested by its members, the Association 'Russia' conducted a survey and discussion of this document at a joint session of dedicated committees.

The survey has immediately revealed a problem of the volume of reporting required to be submitted to the supervisor that needs to be reduced which remains on the agenda for many years. Large credit institutions noted that the software systems used by the Bank of Russia to accumulate the above reporting have already become outdated and are now hardly compatible with the existing automation process. Frequent changes in the reporting forms necessitate engagement of additional staff as filling of the forms by staffers is more economical than automation of the report collection process. For banks with basic licenses, this work stream has become almost the key activity. Specifically, during 2018[10] the amount of expenses incurred to support the activities of lenders have grown for banking sector and most lender groups by 12% in general, reaching 2.0 trillion roubles (accounting for 63% of income reduction sources in the relevant breakdown). Around 50% of such expenses are the employment costs which grew by 14% during that year. The largest share of such expenses in the breakdown of income reduction sources is held by the banks with basic licenses (95%) and other banks (72%).

[10] *Report on Development of the Banking Sector and Banking Supervision in 2018. Bank of Russia.*

In its Report, the Bank of Russia provides international examples for applications of RegTech & SupTech. Such desire to algorithmize interaction with the lenders shown by the supervisor is hailed by the bank community. However, as to initiatives and projects, they primarily cover SupTech technologies, as being aimed at the improvement of oversight efficiency and therefore of prime interest to the supervisor. At the same time, RegTech are of no less importance for those banks who seek to improve operational efficiency and cut the costs. It was therefore recommended by the Association to the Bank of Russia to:

1. Complete creation of the register of mortgages and pledges for the supervisor and financial market players within a short timeframe. This will ensure transparency of reporting on transactions dealing with mortgage execution and pledge issue, speed up decision-making on necessary deals (scoring) by lenders and help the Bank of Russia (along with the State Deposit Insurance Agency as part of the lenders' winding-up procedure) exercise control of these transactions without contacting the lenders. The Association "Russia" takes part in this project and hopes it will be a success.

2. Tie up the transition to the calculation of ratios (KLIKO software) specified as one of RegTech potential applications with the introduction of changes into the Bank of Russia's regulatory instruments which will make it possible to build a form-filling algorithm and make such calculation transparent, thus reducing regulatory risks for the banks. Of note in this respect is an alternative scenario aimed at the development of KLIKO software towards Open-API based technologies. This will help mitigate the impact of the software's user interface on filling, validation and data transfer processes.

3. Develop a buffer base of source data required for the Bank of Russia's oversight function which will be filled in by the credit institutions following uniform principles and standards. Such base will provide the Bank of Russia with online information which the regulator could use to create the required reporting. The Bank of Russia's Report refers to a similar system deployed in Austria where seven largest banking groups have established an AuRep platform that served a framework for creation of a shared data model and a common information system for building both managerial and regulatory reports.

4. Stimulate efforts for digitisation of regulatory requirements (computer-readable control). This initiative seems to be of paramount importance as will help enhance the transparency of oversight and mitigate the risk of conflicts in interpretation of the Bank of Russia's regulations. Besides, this step is prerequisite to successful implementation of, in fact, any SupTech initiative.

5. Complete the work on the project entitled "Collection and Analysis of Detailed Data from the Bank's Operating Day" launched in 2018. All banks are expected to change to a regulatory daily submission of transaction information from the operating day in end 2019. Bearing in mind however the composition of the operating day's data, we are not expecting a predicted change in the workload at this phase as the operating day's data are not sufficient to build most reporting forms. As such, the implementation of data-centric approach to building banks' reporting continues to be one of priority tasks.

5.3. Practical issues of competition in banking sector under digitalization

- *The competition between lenders is more and more shifting to a competition between platforms, services and consumer characteristics of a wide range of services provided in a digital format.*
- *One of the most important tasks faced by the protection of competition in banking services is to prevent monopolization of the cyber-finance space.*
- *Efforts undertaken by the Bank of Russia and the RF Government to create digital infrastructure for the financial market as part of the nationwide economy and social sphere digitalization mission are conducive to the solution of this task.*
- *The existing nationwide digital infrastructure alongside some individual solutions will, on the one hand, contribute to the development of fair competition in price and non-price parameters and, on the other hand, will shield the cyber-space against monopolization.*

The strategic document by the Bank of Russia entitled "Major Ways Forward for the Financial Market in the Russian Federation for the Period Between 2019 and 2021" puts the support of competition amongst the prime targets of the financial market development. One of the most important conditions of the task in hand is accounting for the growing influence of digital technologies on the state of competitive environment, the reason being that the competition between lenders is more and more shifting to a competition between platforms, services and consumer characteristics of a wide range of services provided in a digital format.

An important task is not to allow of the cyber financial space monopolization, to put into practice a system of measures to ensure non-discriminatory access of credit organizations to information and open interfaces

Then, here are the disruptive technologies that help combine banking services with financial technologies. Thus, the banks can offer a variety of products and services required to their clientele on a single platform. The infrastructure accessible via standardized interfaces is one of the key drivers of development of the competitive market in the financial sector. At the same time, the emergence of fintech in the financial sector serves a strong driver for a wave of M&A. This will be conducive to enhancing the economies of scale and diversification of services, which will have positive effect on the operational efficiency of market players. Concurrently with it, a trend to establishing conglomerate-type financial ecosystems will be increasing, bringing about creation of a rigid infrastructure oligopoly for a narrow group of banks.

Digitalization is conducive to the increase in competitive abilities of many lenders. Thanks to the FinTech, not only the size but also the skillful positioning in the digital space in various segments of the financial sector help now maintains the competitiveness. However, for an overwhelming majority of banks, the costs related to adoption and maintenance of digital access technologies is extremely high, in fact unaffordable. In competition for market shares, only large banks now have adequate capabilities for creating their own technological services. Provision of financial services via their platforms allows not only earning the profit but also meeting the growing demand of financial service consumers. Meanwhile, this is accompanied by further concentration of the market power in large banks.

As such, a particular attention of the supervisors represented by the Bank of Russia and the Federal Antimonopoly Service (FAS) to accounting for the development of a competitive environment in transition to digital technologies is fairly well-warranted. One of the most important tasks faced by the protection of competition in banking services is to prevent monopolization of the cyber-finance space and implement a system of measures to ensure non-discriminatory access of lenders to the information and open interfaces.

Efforts undertaken by the Bank of Russia and the RF Government to create digital infrastructure for the financial market, including an express payment system, marketplaces, digital profile and biometric identification system, as part of the nationwide economy and social sphere digitalization mission are conducive to the solution of this task. What this is about is therefore the creation a 'public good' providing customers with the freedom of choice and financial service providers with equal opportunities for promotion of their products. This however does not prevent large banks from establishing their own technological platforms and digital infrastructure.

The existing nationwide digital infrastructure alongside some individual solutions will, on the one hand, contribute to the development of fair competition in price and non-price parameters and, on the other hand, will shield the cyber-space against monopolization. The global experience to date shows that corporate interests and competition protection measures will be getting to a consensus if both the administering and "uncopiable" benefits are not overindulged with.

One of the main functions of competition is the provision of consumers with the freedom of choice. This will be accomplished by providing lenders with equal access to government-run information systems and public non-budgetary funds; and providing citizens with the right to choose specific banks to transfer their salaries to and receive payments from state budget and public non-budgetary funds. Transition to digital technologies opens up opportunities for gradual liberation from the 'salary slavery'.

Implementation of state-of-the-art technologies in any sphere is a labour and cost consuming process that requires relevant competencies. And it is good luck for the financial sector as the supervisor, the Bank of Russia, is itself an active player. Being one of the FinTech Association founders, the Bank of Russia is engaged in development and implementation of new technological solutions for the sake of development of the Russia's financial market. As a means of supporting the competition and restricting market power, an express payment system has already been put in operation.

An Express Payment System (EPS) is the most important nationwide infrastructure project aimed at encouraging the competition, improving the quality of payment services, expanding financial accessibility and reducing the cost of payments for households. EPS makes it possible for individuals to instantaneously transfer money (24/7) using the mobile phone number to their own and other individual's accounts irrespective of which banks the payer's and payee's accounts are opened with. The system is accessible via mobile applications of the banks linked to the EPS both from smartphones/tablets and from computers.

For an instantaneous payment, one should select 'payment via EPS' in the bank's mobile application menu, enter the account to be debited, recipient's mobile phone number and the sum to be transferred. Funds are transferred and become available to the recipient within several seconds after the payer confirms the operation. The only need is for banks to be connected to the EPS. A total of 16 lenders are connected to this system as of August 12.

The next step will be the launch of an e-commerce platform (a marketplace for financial services and registration of financial transactions); and the work is currently underway to populate the Uniform Biometric System. It makes possible for the banks who are not capable of creating own platforms to promote their products based on digital technologies. Simultaneously it increases the degree of consumers' freedom in selection of financial services by volume, quality and cost factors.

5.4. Fostering an trust environment as the driver of banking digitalization

- *With the transition to digital communications and financial services customization, the level of trust in banks becomes one of the main competitive advantages in the eyes of consumers.*
- *To promote and support better behavioral standards, many banks have adopted Codes of Business Conduct. The Bank of Russia published the document "Main principles of good conduct (Code of Good Conduct)".*
- *The Association "Russia" developed and, after a discussion, approved the "Principles of professional ethics for members of the Russian Banking Association", and also adopted the "Service provision standard for credit institutions – members of the Association "Russia", acting as representatives of non-credit financial organizations".*

Transition to digital technologies moves the focus of attention to the fostering of an environment of trust in the financial sector. The digitalization of banking industry cannot be successful without effective partnerships between Fintech companies and financial organizations, as well as coordinated efforts to ensure cyber security and protection of confidential information. Trust and confidence in banks in the situation of emerging 'augmented reality' and service customization becomes one of the main competitive advantages in the eyes of customers. Speaking of financial market as a whole, the problem of trust is now viewed in a much broader context than the confidence of customers in their banks. It implies the confidence of banks and other financial organizations in each other, and the trust of banks in the regulator. It also implies confidence in the competence and business reputation of the management and owners of financial organizations.

The platform for advancing business ethics (good conduct) standards is the document developed by the Bank of Russia "Main principles of good conduct (Code of Good Conduct)". A poll held by the Association "Russia" showed that in general the banks approve of the Code and see no problems in implementing it into a practice. This is not surprising, as most of the principles that are included in the Code have been reflected in the banking legislation and normal business practices. Many credit and financial organizations have either adopted their own business ethics principles and standards, or joined the relevant codes of other entities. All of such codes are conceptually the same. This means that the level of actual implementation of the ethics principles into practice is quite high: 85% of banks consider their actions targeting good conduct of credit organizations to be sufficient. More than 60% of banks assured that they were ready to join the Code proposed by the Bank of Russia. More than 30% said they would consider this matter in the near future. Practically all polled banks (90%) expressed an opinion that it was not necessary to develop recommendations for banks aimed at implementing this Code.

On the request of participating banks, the Association "Russia" developed and, following a discussion with its members, approved the "Principles of professional ethics for members of the Russian Banking Association" (hereinafter the 'Ethics Principles"), and also adopted the "Regulation on the Ethics Committee of the Russian Banking Association".

The requirements of the Ethics Principles apply to all members of the Association "Russia", irrespective of their type of activity. To identify violations of the Ethics Principles, the Association "Russia" established an Ethics Committee operating in a voluntary capacity. A violation of the Ethics Principles can only be reported to the Ethics Committee of the Association "Russia" by a member of the Association "Russia". Decisions made following the review of statements on violation of the Ethics Principles are not published, unless the Council of the Association "Russia" (Presidium of the Council of the Association "Russia") makes the decision to make the investigation results public. This concept of the Ethics Principles was developed for the purpose to increase the level of responsibility and self-discipline of the Association members, and also to establish unified criteria for assessing their business reputation.

To strengthen the environment of trust, the Association "Russia" also adopted the "Service provision standard for credit organizations – members of the Association "Russia", acting as representatives of non-credit financial organizations", which is designed to counteract the so-called mis-selling - an unfair practice of selling financial services to customers on the basis of misleading advice.

The Standard is voluntary to join for all credit organizations that are members of the Association and provide their financial services (products) as representatives of non-credit financial organizations, if they had made a decision to comply with the requirements established by the Standard. The main objective of the Standard is to regulate the procedure of communicating information to consumers of financial services (products).

The "Service provision standard for credit organizations – members of the Association Russia acting as representatives of non-credit financial organizations" was developed on the basis of the requirements of the existing legislation of the Russian Federation, the Strategy of state policy of the Russian Federation in the area of consumer protection for the period until 2030 (approved by the Government of the Russian Federation dated August 28, 2017 No. 1837-r), the Charter of the Russian Banking Association, and also taking into account the provisions of international documents on consumer protection, aimed against unfair practices of selling financial products and rendering financial services, including the Directive 2014/65/EU of the European Parliament and of the Council dated May 15, 2014 on markets in financial instruments and amending Directive 2002/92/EC, the Directive 2008/48/EC dated April 23, 2008 on credit agreements for consumers and repealing Council Directive EC 87/102/ЕЭС.

This document, which most of the members of the Association have joined, is an important step in increasing the level of trust between credit organizations and financial service consumers. Given that banks need some time to make amendments to their internal regulations for compliance with the Standard, a change was made to the Standard stating that legal consequences for violation of the Standard will occur following the expiry of three months after the organization joined the Standard.

In June 2019 the Bank of Russia published an informational letter with a recommendation for non-credit financial organizations to avoid entering into contracts with banks that had declines to join the Standard aimed at counteracting mis-selling practices.

During the poll held by the Association "Russia" in June 2019, most banks (over 92%) to some extent agreed that the absence of a systemic approach to the development of corporate culture is one of the key reasons for low trust in financial organizations. At the same time, 77% had a negative opinion on the proposal to apply stringent sanctions for systematic violations of consumer protection requirements or for unfair practices. However, global experience shows that, in addition to the change in personnel motivation, only large penalties and compensations can help improve the situation with mis-selling.

The MiFID (the Markets in Financial Instruments Directive), regulating investments in financial instruments, was developed in 2004 and put into effect in 2007. Its main objective is to protect the interests of customers of financial sector companies and investment companies (including Forex brokers, dealing centers, etc.), as well as to ensure effective and safe financial operations on the common European market of financial instruments and services.

The key norms and requirements of the MiFID 2007:

- *Providing maximum of information to customers about the company's services and market risks.*
- *Classifying all customers into categories with differing levels of information awareness: a private customer, a professional customer, a partner.*
- *Strengthening the control over the financial recommendations of broker companies and the disclosure of information about offered investment products.*
- *Tight requirements for the implementation of the customers' orders.*
- *Tight requirements for the minimum charter capital of the broker and the qualifications of its personnel, including its senior management.*

In October 2011, the European Commission adopted the decision to make changes and amendments to the Directive, tightening the market control. New requirements in the MiFID 2 have strengthened the customer protection requirements on the EU financial market. The existing rules were updated (including from the viewpoint of new financial technologies), covering practically all aspects of trade within the European Union, including the colossal over-the-counter (OTC) markets of derivatives and bonds and the financial service industry as a whole, from banks to institutional investors, stock exchanges, brokers, hedge funds and HFT (high-frequency traders).

In January 2018 the updated version of MiFID 2 came into effect, which set forth new standards for the reporting of financial organizations (including broker companies in the retail and Forex sectors) submitted to the regulators, aiming to increase the transparency of financial markets and to strengthen the customer protection requirements in financial services.

An effective tool for implementing the Ethics Principles is the motivation of personnel. The approach to this aspect needs to be changed. The fees should not create a conflict of interest. The aspect of fees was not reflected in the Code of Good Conduct proposed by the Bank of Russia. Presumably, the aspect of fees requires a dedicated document that will obligate the managers of financial organizations to act in the customers' interests.

This requirement is fundamental and features in the European directives regulating the sphere of financial markets. In particular, in accordance with the requirements of MiFID the institute of independent investment advisers was established. They (along with trustees) are not allowed to receive commission fees from the provider of financial service.

The topic of trust has raised the issue of 'reasoned judgment', the main aspect of which is the trust of market participants in the regulator, its procedures and personnel, on the one hand, and the trust of the regulator in the supervised organizations, on the other hand. The prerequisite condition for transparency and trust in this situation is that the bank should have the opportunity to present a reasoned objection to the regulator.

The procedure for use of professional judgment is not clearly regulated by the law. The Russian Banking Association developed the draft Concept for the use of reasoned judgment by the Bank, which proposes a mechanism of checks and balances. We believe that this mechanism should:

- *be based on the transparent interaction procedure,*
- *include the mandatory possibility for the bank to present a reasoned objection and to have this objection reviewed in an unbiased manner,*
- *guarantee the professionalism and responsibility of the person making the reasoned judgment, and the possibility to use an independent expert.*

ASSOCIATION
OF BANKS
OF RUSSIA

location (address for correspondence):
113180, Moscow,
Bolshaya Yakimanka, 23

tel.:
+7-495-785-2990

e-mail:
asros@asros.ru

web site:
asros.ru