The role of information technologies in ensuring banking security

M N Kondratyeva\textsuperscript{1,3}, D D Svirina\textsuperscript{1} and A I Tsvetkov\textsuperscript{2}

\textsuperscript{1} Russian Technological University — MIREA, Innovative Technologies and Public Administration Institute, Prospekt Vernadskogo, 78, Moscow, 119454, Russia
\textsuperscript{2} National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), 31 Kashirskoe shosse, Moscow, 115409, Russia
\textsuperscript{3} E-mail: kondrateva@mirea.ru

Abstract. In this paper, using practical examples, the author dwells on the possibilities of innovative technologies in banking. The necessity of implementing modern security systems to create a safe business space for banks is substantiated. The main trends and leading technologies in the area of information security are considered. The importance of tracking threats and risks associated with user information and resources in a fast and timely manner is emphasized. The article highlights modern information technologies and methods aimed at strengthening business processes, the implementation of which increases security of financial organizations and their ability to resist external threats. In the article, the technologies and methods described include Paperless Office technology, deactualization risks, social engineering, biometric identification, psychology of information security (from here on, IS-psychology), regulatory and supervisory technologies. The advantages and disadvantages of modern information approaches to solving problems of external threats discussed in the article are described. The objective of this research is to justify and reveal the importance of innovative technologies in maintaining the necessary level of security, as well as improving the protection and resilience of domestic banking systems in terms of external threats. General scientific methods are used as research methods: analysis and synthesis, generalization, interpretation of graphic information, as well as statistical analysis. The results of the study allow to claim that the development of innovative financial technologies and the digitalization of business processes in banking lead to systemic contradictions in the balance between the potential benefits of and damage to the system of financial relations. On the one hand, the emergence of modern innovative technologies provide the opportunity for the banking sector to improve and modernize the processes of its activities, and on the other hand, the very same advanced technologies can be used by scammers, which produces a detrimental effect on both banks and consumers. It appears to be so due to the fact that advanced technologies are relatively new and just being implemented into banking, which is characterized by the presence of both merits and downsides.

1. Introduction
The 21st century is referred to as the century of scientific and technological progress that has changed people's lives beyond recognition. The transition of the economy to a new qualitative state increased the importance of innovative activity, development of knowledge-intensive industries, which provided adequate conditions for economic development.
New technologies are rapidly evolving, and they are being implemented in the commercial sector. One of the most breakthrough and innovative sectors that contributes to modernizing of many processes of other industries is the IT (Information Technology) sector. It is information technology that helps to debug and protect production and business processes in enterprises, by ensuring competent and smooth operation. Through the active use of information technology, developed countries continue to improve their economic situation, while emerging and developing economies get the opportunity to approach the developed countries levels in terms of economic development.

The target of the research is the modern banking system, which faces many threats and attacks from the external environment. In this regard, there is an urgent need for ensuring security, both for banks and customers. The acknowledgment of this problem has become a key factor for the close cooperation and intertwining of two different but complementary structures — information security and banking [1]. One of the main tasks of the banking sector is to predict which technologies will become an ergonomic tool for solving existing problems in the banking sector.

The existence of a number of unsolved problems related to banking security add a special relevance to the implementation of new technological processes in their structure, which will, ultimately, lead to work organization optimization, positive financial results supported by the sustainable protection of resources, and client loyalty.

The Central Bank of the Russian Federation, as well as the non-profit organization “Fintech Association” deal with the information security model development and modernization of banking systems. “Fintech” was created at the initiative of the Central bank at the end of 2016 and it unites Russian banks that can develop financial technologies and test the work of digital services using its fintech-platform.

In her speeches, the Chairman of the Central Bank Elvira Nabiullina defines the sphere of financial technologies as the engine of progress for the entire banking system of the country, on which it is necessary to put emphasis, so that Russia would assume leading positions in this area.

Chairman of the Board of PJSC “Sberbank” German Gref, actively supports the implementation and development of new financial technologies within “Sberbank”, which over the past five years has become the first bank to test innovations and conduct research internally [2]. Russian entrepreneur Oleg Tinkov — the founder of the neo-bank JSC “Tinkoff Bank” recognizes the need and fundamentality of information technologies, allocating budgets for recreating a completely new structure of banking architecture, making the bank completely digital. Also, this problem is subject to statistical analysis of such foreign companies as KPMG, Ernst&Young, which collect and systematize the obtained data.

The first major cyber-attack occurred in 1995. Russian mathematician Vladimir Levin, working from home, delivered an attack on the system of one of America's most significant banks. The mathematician succeeded in stealing about $12 million from the bank accounts, and then was detained by the FBI criminal intelligence agencies in the UK, where he came to withdraw the stolen funds. As we can see, cyber-attacks are not a new phenomenon; they have been gaining momentum every year. The possibilities of innovative technologies are rapidly expanding, and they can be applied in many ways, not only by banks, but also for fraud purposes. Nowadays, dealing with modern threats, experts are facing the fact that it is not enough to merely implement a new technology and customize it for each cyber-attack, as malicious software is able to bypass all standard protection methods. Modern attacks are large-scale and diverse, and they cause severe infrastructure and financial losses. According to statistical data, in 2019, the participants of financial relations suffered losses that increased by 300% compared to 2018 only from targeted attacks of systems [3]. Given these factors, it becomes clear that the banking sector needs a new model of information security, which will be able to prevent attacks on the structure evenly — it will have one management center for administration, monitoring and immediate response to emerging incidents.

Nowadays there is a shift from innovative business models to technological innovation. Technological innovations make it possible for the transactions to become faster and easier, but the same factors expose transactions to threats, and the issues of user protection are become harder to solve. In
In this regard, identity authentication and user security come first [4]. The competition between fintech companies and banks is also tangible.

Fintech (Financial Technology) means digital innovations that aim to improve and modify the internal infrastructure of banks, financial companies and business. Innovative financial technologies usually involve software, applications and transformed business processes. Fintech is a new technology industry of the economy, which is beginning to take precedence over traditional approaches to business relations between participants of the financial market [5].

According to one of the leaders of the global market for innovative technologies, “Accenture” company, in the first half of 2019 alone, the volume of global fintech investments amounted to $22 billion, and the penetration index of fintech services in Russian megacities amounted to 43%, which is 10% more compared to the index of use of similar services in other countries. Figure 1 shows Russia's place in the global market of innovation diffusion and use, which it shares with South Africa. Also, the levels of fintech technologies use in 27 countries in 2019 is given, where the average value among different countries is 64% — and it indicates that the sphere is a fast-growing and a fast-developing one (see figure 1). In 2019, Russia was among the top three countries in terms of fintech services market penetration, exceeding the average, which was 82%. India and China have a larger percentage. The diffusion level of financial high-tech services was 87% in the two countries [6]. In the United States, this index was 46%. The slow spread of information technology can be observed in France and Japan, where the average rate is 35% and 34% respectively, due to legislative restrictions in these countries.

Technical innovations are rapidly implemented in production and business structures, which helps fintech enterprises to reach new levels of technology rather quickly. The changes considered in this article, also lead to the emergence of new players in the industry [7]. For example, such players include
technology companies that used to do finance and have moved into the financial technology sector, promoting their own initiatives in the industry. However, IT giants such as Microsoft, Intel and Google are showing high interest in the fintech sector, supporting it with considerable investments [8]. This interest has led to the emergence of business incubators and technology parks that generate innovative solutions.

2. Research of technologies and methods
The field of financial technology is constantly evolving, which results in changes in the financial sector. It must expand its boundaries beyond familiar payments and credit, while modernizing not only its structure but also the structure of the entire financial sector of the economy. The payment and credit systems are the most favorable areas of financial technology. Investors are willing to finance and support enterprises engaged in developing such technologies, which results in start-ups of the industry having higher estimations. This contributes to the possibility to develop and implement innovative technologies in the banking sphere, that will ensure the security of information and financial transactions [9]. The following technologies and methods are currently being applied to ensure the security system of the banking sector. The comparative characteristics are presented in table 1.

| Table 1. Comparative characteristics of applied (implemented) technologies and methods. |
|---------------------------------------------------------------|
| **Technology/method**                   | **Advantages**                                                                 | **Disadvantages**                                                                 |
| 1) Paperless Office technology           | • cost reduction;                                                              | • high-speed, seamless internet connectivity is required;                       |
|                                         | • labor costs optimization;                                                    | • technology efficiency depends on software and hardware;                      |
|                                         | • operational risks minimization;                                              | • software failures result in failures of the paperless office;                |
|                                         | • The information is stored in one system in digital format;                   | • the possibility of unauthorized access to confidential records;              |
|                                         | • fast access to the information base;                                        | • consequences of commercial records leaks;                                   |
|                                         | • The ability to grant access rights to a group of users while tracking actions within the system; | • The process of digital records utilization is difficult due to the possibility of restoring files; |
|                                         | • saving on rent, as no paper document storage is required;                   | Note:                                                                         |
|                                         | • saving due to cutting down on paper usage;                                  | The process of digitizing of the available documentation is long and complex, but the degree of security and reliability of digital media compared to paper media proves the effectiveness of this measure [10]. |
| 2) Deactualization risks and social engineering | • availability of up-to-date personal data of clients;                      | • customers are reluctant to share personal information;                      |
|                                         | • prevention of embezzlement and theft of funds from customer accounts;       | • social engineering is also used for the purpose of obtaining unauthorized access; |
|                                         | • customer service work, explaining risks and mapping out of the ways to minimize money losses caused by fraud; | Note:                                                                         |
|                                         | • Social engineering is a tool that includes methods, techniques and technologies that achieve the desired result using psychology and sociology. However, it is impossible to apply it without developing it first, as, on the one |
hand, it gives the opportunity to work with distrustful and hostile bank clients, and on the other hand, it lets scammers obtain the financial statement details and PIN codes of gullible and careless users.

3) Biometric identification
   - resistance to forgery of information (inability to copy and transmit it to third parties);
   - singularity of identification information;
   - Multifactorial process of identification;
   - prevention and blocking of threats, targeted attacks;
   - expert support and assistance in the investigation of computer incidents;

This method was introduced into banking in mid-2018, but users have been familiar with this technology via the biometrics procedure when applying for the Schengen visa.

Biometric identification today is one of the most promising areas in the development of banking security.

4) IS-psychology
   - ensuring security within the company at the management level;
   - preventing data and classified information leaks.

So far, IS-psychology has not been given enough attention. The possibility and effectiveness of this method allows to test the processes of identification and timely response to suspicious files, calls and messages.

5) Regtech and suptech
   - Customer identification, information protection, transaction monitoring;
   - risk management, audit of internal systems, providing a report;
   - optimization of regulatory compliance processes, simplification of work at all stages;
   - participants of financial relations activity supervision;
   - collection, processing, analysis of the data obtained from the financial market participants;

Regulatory and supervisory technologies allow banks to meet state regulatory requirements faster, more efficiently, with minimal risks and costs.

After researching the comparative characteristics of technologies and methods, we are moving on to the analysis of each item separately.
2.1. Paperless Office technology

Paperless Office is the technology of electronic interaction between the bank and its client, based on the maximum reduction of paper flow between them by providing the client with a convenient and secure way to register operations. The implementation of this technology allows to reduce expenses, optimize labor costs and minimize operational risks when executing orders, and clients can obtain a more flexible, secure and fast method of receiving banking services [11]. The use of Paperless Office technology allows to convert and accumulate a large volume of documentation into a single digital system, making it possible to get quick access to the database of documentation: access rights can be granted to several employees (analyst groups, developers), with them working both from office and from home. The storage of digital files does not require large premises, compared to paper media, there is a reduction in the use of paper, which not only reduces enterprise costs, but also makes a company more socially oriented and environmentally open — the use of resources is reduced to the necessary minimum, there is no need to use toxic ink for printing. Such changes in the organization of office work are not revolutionary, they can be rather described as evolutionary, as they involve the transition to intellectual infrastructure.

PJSC “Sberbank”, which is one of the first banks to introduce a legally valid electronic document flow between the bank and the client, advances in implementing this technology while learning from the experience of leading foreign companies. According to PJSC “Sberbank”, the estimated amount of savings resulting from the use of the system amounted to 1.5 billion rubles per year, which confirms the many-fold return on development costs of Paperless Office technology. However, while considering the benefits of Paperless Office technology, a number of important factors should be taken into account — the efficiency of the paperless office depends entirely on the software and hardware used to store information [12]. Software failures and errors will result in paperless office failures, which makes it necessary for banks to facilitate a smooth system maintenance by technicians. The well-known problem of unauthorized access to confidential records by system hacking or by violations arising from non-compliance with security instructions on the part of staff causes risks of data modification and substitution [13]. The consequences of records leaks of a commercial nature (such as legal and medical) will be significant. Also, the procedure for utilizing digital records is particularly complicated, given the fact that the documents are located in a common network environment and files can be retrieved after having been deleted.

2.2. Deactualization risks and social engineering

The banking sector is expected to introduce a new standard — banks will oblige their clients to constantly update e-mail addresses. When it does not concern money transfer, most people do not understand the need to update personal information for banks. It is because of this misunderstanding that attackers, using the information they collected about the clients, can use social engineering techniques, which can ultimately result in the client's account losing money funds [14]. This requirement is needed because customers' obsolete email addresses make them vulnerable to spam, phishing, malicious software mail-out, and identity theft. Banks collect and analyze information about technical means the customer uses for electronic banking. Legislation and regulations require banks to collect such information to assess the customer's profile to determine if the transaction is performed by a legal account holder rather than a cyber-crook [15].

Social engineering plays a key role when attempting to gain unauthorized access to information and technology systems. The reasons of social engineering popularity in cyber-attacks is its cheapness and time-effectiveness. In 2019, using a set of social engineering methods, scammers stole 1.4 billion rubles from users' bank cards, which is 44% more than in 2018. The spread of such fraud is connected with the development of banking technologies and remote banking, so the Central Bank obliges commercial banks to work with their clients, explaining the risks of money transfer and information protection measures that can be undertaken. The figure below shows the life cycle of social engineering (see figure 2).
2.3. Biometric identification

Every year, biometric identification functions in banking keep expanding and are getting more complicated due to the comprehensive approach based on analysis and action recognition. Biometric identification has gained its spread and increasing popularity due to high resistance to forgery of such information — the inability to copy and transmit it to third parties, as biometric technologies are based on the identification of unique human parameters, which include fingerprints, face and its heat chart, iris, hand geometry, vein pattern, DNA, voice, handwritten and keyboard handwriting [16]. All this data helps biometric readers, sensors, scanners, and controllers improve the identification process, develop and apply a set of solutions against targeted attacks and complex threats:

- continuous monitoring at the network and workplace level;
- blocking threats and reducing the risk of targeted attacks;
- detection of outliers in the behavior of information infrastructure objects;
- expert support and assistance in the investigation of computer incidents;
- assessment of potential risks within the current infrastructure information security.

Today, Kaspersky Lab successfully copes with such tasks by using the platform that combats targeted attacks — “Anti Targeted Attack Platform”.

Biometric technologies have spread in the public sector; they protect electronic documents and national security system programs. The banking structure is also beginning to implement identification systems to improve the security of internal structures, data and client funds [17].

PJSC “Sberbank” became one of the first banks to implement biometric identification into its system. Today, biometric identification consists of several stages:

- Pulling and memorizing the data provided by the system;
- Identification of biometric samples, obtained information is converted into a unique mathematical code;
- Comparison of the obtained biometric sample with the image that was previously submitted;
- The algorithm confirms if the biometric samples are a match, the identification process is finished.

Figure 3 shows the forecast of biometric data usage by banks and government authorities in the framework of digital technologies up to 2022 (see figure 3).
2.4. IS-psychology

Information security is constantly developing, and it is never stagnant. IS-psychology can be used yet as another tool to combat security incidents. Today it is in demand in three areas:

- anti-hacking, preventing and investigating incidents;
- ensuring information security of client services.

Let us take a closer look at the corporate needs of banks. Psychology plays a significant role in ensuring corporate information security. It is important to address “weaknesses” that arise in the process of working within the bank: vulnerability analysis, annual updating and supplementing information security instructions, providing staff with knowledge of the personal characteristics of each employee and the team as a whole. All these measures will help to build a system that can prevent data and classified information leaks.

The psychological motivation of information security specialists is of considerable importance, namely their legal awareness, ethical principles, responsibility and motivation to work. Information security managers need to monitor and supervise specialists who have access to data and technical equipment relevant to the bank, because, despite all measures taken, the most vulnerable link in the protected system is the human factor. This claim applies to both employees and customers equally. Very effective measures in the field of IS-psychology include the distribution of confidential information among employees, special records for storing data of special importance, mandatory signing of NDA (non-disclosure-agreement) for all new and outside experts, as well as disposal of documentation and various records that have not become part of the work process. The scheme illustrating the human factor in the banking information security system is presented below (see figure 4).
2.5. Regtech and suptech regulatory and supervision technologies

2.5.1 RegTech (Regulatory Technology) was developed to simplify regulatory requirements by financial organizations. It is used when customer identification, information protection, transaction monitoring, corporate governance, risk management, internal systems auditing, and reporting are required. RegTech’s is used to optimize regulatory compliance processes, as well as to simplify all stages of the processes.

2.5.2. SupTech (Supervisory Technology) is similar to the previous technology, but the difference is that it aims to improve regulation and supervision effectiveness, concerning the activities conducted by the participants of the financial relations. In terms of its current activities, SupTech responsibilities can be divided into two areas: data collection and processing of received information, as well as analysis of the obtained data of financial market participants [18]. The use of this technology involves automation, simplification of administrative procedures, transition to electronic document flow and improvement of the quality and structure of reporting documents.

Having learnt about RegTech and SupTech, one might ask: why were these technologies developed if there had already been regulators controlling the banks before then? After the crisis in the US in 2007, it became apparent to experts that the existing regulators are not enough and to prevent such a situation a new approach to regulating and supervising financial organizations is required [19]. That is why RegTech and SupTech technologies were first used in the United States, and then gained their popularity in other countries due to their functional qualities. But despite all the positive aspects of the two technologies, there are risks associated with their implementation in the structure of organizations:

- Cyber risks — the number of targeted attacks on banking systems with the implementation of technologies has increased by 1.8 times compared to 2018.
- Error Risks in Algorithms — Transactions from Client Accounts without using authentication tools.
- Risks associated with the interdependence of participants of the financial relations — confidential information might spread as a result of the cooperation with third-party external counterparts, as it happened with Alfa-Bank JSC, which had confidential information of 400,000 clients of the bank leaked.
- Risks of shadow (unfair) practices — such as running an advertising campaign that aims to mislead consumers, or charging illegal fees to customers etc.

Thus, the transition from traditional business models to technological innovations, reflected in the trends of effective application of fintech technologies in the banking sector, faces serious contradictions.
A paradox to be considered is that, on the one hand, information technologies allow to optimize the work of organizations, supported by internal resources protection, with positive financial results, and on the other hand, the same advanced technologies are used by hackers and scam sites, which results in negative consequences for both banks and the customers [20]. Given the negative dynamics of damage to participants of the financial relations, investments and activities of IT specialists should be focused on the development and implementation of new technologies, in order to ensure the security of banking activities and to prevent attacks on the banking sector.

Despite this contradiction, the authors emphasize the importance and the necessity to develop innovations in banking [21]. It seems to us that, first and foremost, we should pay special attention to the preparatory process — we need to employ a satisfactory number of developers, to increase the time for testing and pilot production, which will enable us to take into consideration all the scenarios for the technology implementation in banking, thus providing a system of financial security for all the participants of the process.

3. Results
The article revealed contradictions in terms of information financial technologies usage within the banking system — on the one hand, the appearance of modern innovative technologies provides the opportunity for the banking sector to improve and modernize the processes of its activities, and on the other hand — advanced technologies are just beginning to evolve and their implementation in banking is relatively new. That leads to the presence of weaknesses which are subject to external cyber-attacks that damage both banks and customers. Given the fact that the aforementioned problem is a new area of the scientific study, the authors of the article do not provide a sufficient number of research literature references and emphasize the paramount importance of further work on analyzing the role of innovative technologies in banking.

4. Conclusion
Despite the fact that the banking sector is performing a herculean task of modernizing and protecting its system to preserve user resources, confidentiality of information, and to generate new digital products, the authors focus on the fact that it is not possible to solve the problem of cyber-attacks on bank accounts yet. In this regard, it is necessary to continue working in the same direction, to interact with employees and clients.

References
[1] Zveryakov M, Kovalenko V, Sheludko S and Sharah E 2019 Fintech sector and banking business: competition or symbiosis Economic Annals-XXI 1-2 53-7
[2] Eskindarov M A, Maslennikov V V, Maslennikov O V 2019 Risks and chances of the digital economy in Russia Finance: theory and practice 5(113) 6-17
[3] Sherstuk V P 2020 Review of the book «International information security: theory and practice» Cybersecurity issues 1(35) 87-8
[4] Zveryakov M, Kovalenko V, Sheludko S and Sharah E 2019 Fintech sector and banking business Economic Annals-XXI 175(1-2) 53-7
[5] Kotliarov I D 2018 Fintech: nature and models of implementation ECO Journal 12(534) 23-39
[6] Usoskin V, Belousova V and Kozyr I 2017 Financial intermediation in a new technology environment Money and credit 5 14-21
[7] Kotliarov D 2020 Digital transformation of the financial industry: the substance and trends Manager 3(11) 72-81
[8] Podkolzina I M and Gliwa D I 2019 Trends in the development of the financial market of Russia Colloquium-journal 1 92-6
[9] Vengerovsky E L 2018 Innovations of internet banking as a factor of competitive performance of credit institutions on the modern bank service market Banking law 1 47-52
[10] Kiyutsevskaya A M 2019 Fintech: current trends and challenges for monetary policy Voprosy
[11] Bank of Russia (Central Bank of the Russian Federation) data 2018 Main Areas of Financial Technologies Development for the Period of 2018-2020 7 https://cbr.ru/StaticHtml/File/36231/ON_FinTex_2017.pdf) last accessed: 2020/04/10

[12] Zaitsev O A and Pastukhov P S 2019 Formation of a new strategy for crime investigation in the era of digital transformation Bulletin of Perm university. Legal science 46 752-77

[13] Borsuk N A, Deryugina E O and Minina A D 2019 Questions of increasing the efficiency of document circulation at the enterprise Electromagnetic waves and electronic systems 7(24) 56-61

[14] Kisliutsyn D V 2020 Financial literacy training programs and financial behaviours: why people do not become «financial literate»? Voprosy Economiki 9 80-93

[15] Belianin A 2017 Economic of lies: causes, determinants and experimental measurements Voprosy Economiki 21(2) 201-23

[16] Bank of Russia (Central Bank of the Russian Federation) data 2018 Market Overview of Biometric Technologies and their Application in the Financial Sector 4 https://cbr.ru/Content/Document/File/36012/rev_bio.pdf

[17] Dobryanskiy V 2019 Blockchain based authentication in cyber-physical systems Current problems of infotelecommunications in science and education (Apino 2019) 1 414-8

[18] Bank of Russia (Central Bank of the Russian Federation) data 2018 Issues and Directions of Regulatory and Supervisory Technologies in the Financial Market in Russia p 5 https://cbr.ru/Content/Document/File/48604/Consultation_Paper_181016.pdf

[19] Povetkina N A and Ledneva Yu V 2018 Fintekh and redtekh: boundaries of legal regulation Law. Journal of the higher school of economics 2 46-67

[20] Lauts E 2017 New banking technologies and anti-crisis regulation of banking market Banking Law 4 36-44

[21] Belousova V, Karminsky A and Kozyr I 2018 The macroeconomic and institutional determinants of the profit efficiency frontier Russian banks Applied econometrics 1(49) 91-114