Using Cognitive Technologies to Ensure the Information Security of Banks in the Conditions of Digital Transformation and Development of Biometrical Identification

[1]BORIS M. FEDOROV, [1]SVETLANA V. FEDOROVA, [2]HUAMING ZHANG,
[1]NATALIA A. MAMEDOVA
[1]Basic Department of digital economy, Higher School of Cyber Technologies, Mathematics and Statistics, Plekhanov Russian University of Economics,
RUSSIA
[2]Deputy Dean, School of Economics, Shanxi University of Finance and Economics,
CHINA

Abstract: The digital transformation of the economy will affect all spheres of life of every citizen of the Russian Federation. This also applies to the financial sector, where in the near future the standard for providing services to customers will be the possibility of their remote receipt, which, among other things, will be facilitated by the use of biometric identification technology. However, this requires great effort in terms of information security. One of the directions in this area should be cognitive technologies, focused on human intellectual abilities. The article discusses the use of cognitive technologies to ensure data security when using biometric identification in the context of the development of this direction in the framework of the policy on digital development of the economy of the Russian Federation.

Key-words: digital transformation, financial companies, cognitive technologies, biometrics.

Received: July 22, 2022. Revised: November 25, 2022. Accepted: December 17, 2022. Published: January 26, 2023.

1 Introduction

The current stage of development of the world economy is characterized by a high level of scientific and technological progress, the introduction of new technologies into daily use, and an increase in the amount of information and data used in decision making, [1]. All these changes lead to the transition of existing economic formations to a new level - the economy of knowledge, one of the elements of which is the universal digital transformation. The basis of economic, social, and cultural relations is the use of digital information and communication technologies. The response to world processes was the adoption in the Russian Federation of the National Program "Digital Economy of the Russian Federation", approved by the government on July 31, 2017. The strategic objective of implementing the digital transformation of the Russian economy is a matter of global competitiveness and national security.

As part of the overall digitalization and transfer of the client base to the remote provision of its services, including through the use of biometrics technology, banks and other financial market participants in the Russian Federation need to ensure an adequate level of information security. Financial companies are responsible to customers regarding the execution of payments, as well as the obligation to ensure the confidentiality of transactions. For this reason, the use of advanced technologies in the field of security is a necessary task for business development and the ability to respond to your commitments.

18 December 2017: The Government Commission on the use of information technology to improve the quality of life and the business environment has approved an action plan for the direction of "Information Security" Program "Digital Economy of the Russian Federation " in 2018-2024 years. The approved program includes measures to develop and use new technologies to ensure the information security of personal data of citizens of the Russian Federation, as well as data that is a commercial or banking secret.

2 Role of Internet Technologies in Russian Banking System

In the conditions of transformation of the Russian economy and its transition from the traditional system level of the knowledge economy, a complex change occurs in its functions, values, development

vector and fundamentals of the reproduction process. Moreover, these are radical changes of the system-forming components, which lead to the formation of new relations based on innovations. This also applies to the relationship between organizations and customers.

A knowledge-based economy is an economy that creates, spreads, and uses knowledge to ensure its growth and competitiveness. This is an economy that not only uses knowledge in a diverse form, but also creates it in the form of scientific and high-tech products, highly qualified services, and education, [2].

The society is in the stage of technological singularity, which is stimulated by many factors: technological capabilities for analyzing large data arrays, increasing computing power and speed of information processing, improving artificial intelligence, and integrating real and virtual worlds when people and devices act as equal parties to communicate (Internet of things), [3].

One of the cardinal change, especially in the service sector, is the ability to render them remotely, using Internet technologies. The new paradigm of the information society is the ability to receive goods and services remotely, as quickly as possible and at the same time being in any part of the Earth. These processes are due to globalization trends, as well as new opportunities that have become available thanks to the achievements of scientific and technological progress. The primary relevance of this approach has been found in organizations engaged in the sale of certain goods to end users, but then the use of Internet technologies has become a general trend for service organizations, [4].

Nevertheless, there remained branches where the role of Internet technologies was not exclusive and was considered only in the concept of additions to the core business, which was carried out according to traditional schemes. One such industry is banking and other financial companies. First of all, this is due to the need to ensure a high level of information security, which is much simpler and easier to implement an “its” site: in bank branches, operational offices, ATMs. But market demands and high competition in the industry require banks to take active steps to expand the existing client base, which can be achieved primarily due to the high quality of services provided. At the same time, quality criteria in the first place mean the opportunity to receive the service as quickly as possible and with minimum requirements for its design. This requires the development of used technologies that contribute to the formation of a new, innovative business.

This is especially true for medium and small banks. This is due primarily to the fact that the entire banking system in recent years has become closer to a complete monopoly on the part of state banks, which are at the same time the largest in terms of net assets. According to the Herfindahl-Hirschman index, which reflects the level of concentration of assets, in the Russian Federation it is 8.69 points, which indicates the oligopolistic nature of the market. For comparison, in the United States this figure is 16.85 points, in the UK - 24.27, and in Japan, on the contrary - 8.32, [5].

At the same time, one of the criteria for the high quality of the services provided is the safety of operations performed by customers. This part of the activity is not visible to the end user, but nevertheless it is critical, and its provision is the most important task of the bank.

Remote banking services have already become the norm, but not all organizations represented on the domestic market can offer a truly wide range of services or a unique and convenient service. Over the past five years, the share of users of such Internet banking services has grown by about 3-4 times in the total retail customers of Russian banks. According to a study assessing the effectiveness of Russian Internet banking services for individuals, conducted by Markswebb Rank & Report, 69.5%, or 37.4 million Russian Internet users aged 18 to 64, use Internet banking for individuals ,[6]. For comparison, in 2018, the number of Internet banking users increased by 32% compared with 2017.

3 The Use of Biometrics for Digital Identification of Remote Clients

Biometrics is a scientific discipline that studies ways of measuring and static analysis of people's physical and behavioral characteristics, to identify one person from many other people. Biometric technologies are being actively integrated into different areas around the world. Already, biometric identification technologies have become an integral component of the global information technology market and are becoming a convenient tool for solving a wide range of tasks. Currently, they are used and implemented in many areas or areas aimed at ensuring the protection of information, such as: online payment services, personal identification systems in various structures and in banking structures. Every year the number of biometric systems and their users increases.

Well-known examples of biometric data are characteristic patterns of the iris or papillary lines on the fingertips, [7]. However, it is worth noting that biometrics include not only physical, but also behavioral indicators, such as gait or individual features of typing on the keyboard, [8], [9], However, whatever type these data belong to, they are inherently inherent in a person and therefore can guarantee a very high reliability of identification - provided that the readers are difficult to deceive.

Identification using any type of biometric data consists of the following steps:

• Record - the system remembers the biometric data.

• Selection of a biometric sample - information is processed and converted into a mathematical code.

• Comparison — the stored biometric sample is compared with that presented during the identification.

• Getting the result - the algorithm gives the result of the coincidence of biometric samples.

The volume of the global market for biometric systems at the end of 2016, according to the international consulting company J'son & Partners, estimated at 14.45 billion US dollars. According to the forecast, for the next 6 years, the compound annual growth rate (CAGR) of the biometric technology market will be 18.6%, and the projected market volume by 2022 will grow to 40.2 billion US dollars, [10], [11]. (Fig. 1)

The largest segments of the world market for biometric systems are in the public sector, including the migration sector, as well as the travel segment. The third major market for biometric systems is the financial sector, whose share is estimated at 15%.

Banks around the world are launching pilot projects to test various biometric technologies, and many banks are already actively using them in business practice. For example, two major banks in Singapore (DBS and OCBC) use voice recognition systems in their call-centers. City Group also integrated voice biometrics into its processes in the Asian region (the bank plans to connect about 1 million customers to the service).

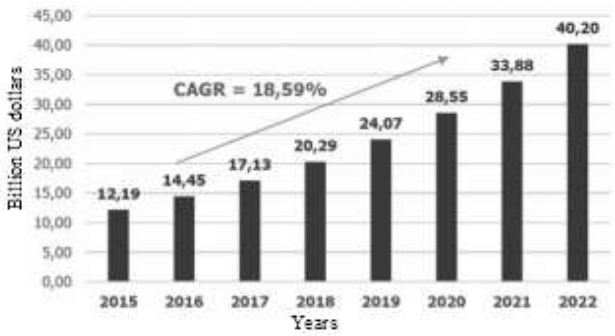

Fig. 1: Volume of the global market for biometric systems 2015–2022, [10], [11]

In recent years, multifactor authentication using biometric technologies has been developed at the highest rates in the financial sector, which is typically used in critical areas such as banking and insurance, as well as security.

Of all the multifactor authentication models, the most common (and traditional) is two-factor authentication (for example, pin code or one-time password plus biometric technology), which is used in online banking, ATMs, and access to bank cells. Three-factor and more authentication solutions are applied when it is necessary to provide exclusive access or for operations requiring increased confidentiality. Having considered the best practices, we concluded that for most online operations, when providing banking services, a two-factor model will suffice, provided it is highly reliable, or both factors are directly related to biometrics.

In the Russian Federation, biometric identification in banks is widely used. Large banks use voice technologies in call centers, face recognition technologies when a client re-applies to a bank for a loan, fingerprint scanning to enter a mobile application and access bank cells.

The remote identification mechanism in the Russian Federation allows you to open deposits, accounts, and receive many other services online. To do this, the client only needs to come to the bank with the documents once and go through the primary identification - to record voice and video. The bank sends this data to the Unified biometric system. Then a person can remotely receive the services of any bank, having passed a double confirmation of identity: through the Unified State Identification and Authentication System and through the Unified Biometric System. The whole procedure will take several minutes. At the same time, the Ministry of Digital Development, Communications and Mass Communications has developed criteria for biometric samples - face

images and voice recordings that will be used to identify citizens in a single biometric system.

On December 25, 2017, "Otkritie Bank" officially announced the launch in their mobile application of money transfer services by customer photo. "Otkritie Bank" became the first bank in the world with such a service. The service is implemented using a unique technology - the neural network facial recognition system, which allows you to identify a client with his biometric data with a high degree of accuracy. To use the service, you need to download the application "Opening. Translations" (available for iOS and Android systems), in the main menu, select the type of translation - "translation by photo"- and take a picture of the recipient on the smartphone's camera or select a photo of it from the gallery. Next, the image will be sent to the banking system of face recognition, which will determine the recipient and will display in the application the masked number of his bank card, to which the transfer will be made. One of the main problems encountered during the creation of the service was the correct identification of the user and the ability of the mechanism to estimate that the camera reads to a real person and not his photo.

It is important to note that biometric data is particularly sensitive information, the compromise of which leads to serious consequences. In this regard, when using biometric data for identification purposes, uniform requirements for their transfer, storage, processing, and protection of data should be applied.

4 Modern Technologies to Ensure the Safety of Banking

The increase in the number of transactions carried out by customers of banks through remote services leads to the need to develop mechanisms and means to ensure their high level of security. First of all, it concerns the detection of "suspicious" and fraudulent transactions. An example is the work of the international payment system MasterCard, which unites more than 22 thousand financial institutions around the world, [12]. Millions of payments pass through the payment system every day, some of which are potentially fraudulent. And for their detection, analytical systems are used, which according to the developed algorithms correlate transactions according to certain criteria and, if they coincide, block a bank card. Such algorithms are simultaneously used more.

1 million, which in a matter of seconds can relate a transaction to an unreliable one. For example, a person making a trip from Moscow to Brazil with a transfer in Portugal, made purchases at three airports, risks that his card will be blocked due to transactions in three countries distant from each other during the day. The bank card will be blocked due to an algorithm based on machine learning technology.

But similar technologies are implemented with the active influence of a person as an expert, creating the necessary models for analyzing incoming data and developing the necessary solutions. However, only about 20% of this data is structured, that is 80% of it is not visible for computer systems created by classical technologies. To solve this problem, cognitive calculations are used, which allow to partially replicate the characteristics of the brain in terms of processing and analyzing incoming information, as well as opportunities for self-learning, [13]. For example, a client's profile can be enriched from various sources, from the transaction history — how a person spends money in relation to how much he receives. It is also possible to find data on how he behaves in social networks, how he moves around the city, in which places he spends more time. And this data is used in the subsequent determination of the attribution of transactions for fraud.

The field of cognitive technologies is one of the most promising in terms of the development of human intellectual abilities. In addition, artificial intelligence can use many different parameters to identify behavioral abnormalities and minimize the risks associated with the human factor, eliminating subjectivity in making decisions. With a high degree of accuracy, it is possible to identify certain segments of the IT infrastructure that may be subject to network attacks or external intrusions, [14], [15], [16]. The consequences of cyber attacks are predicted based on machine learning and natural language processing methods. One of the implemented solutions is the use of a semantic model of security descriptors in order to automate the low-level modeling of threat scenarios based on the description of computer attack patterns. This model simplifies informing about the consequences of an attack and reduces the cognitive burden on researchers by automatically predicting the consequences in case of new attacks, [17], [18]

With the help of cognitive technologies, it is also possible to identify possible cases of fraud, including actions by bank employees. With the standard work of an analyst in the detection of fraud, there is a high degree of probability that some

things will be overlooked. The use of systems based on cognitive technologies is able, for example, to detect anomalies in the behavior of traders in making transactions, analyzing several sources of information at the same time, including telephone conversations, assessing intonation, and comparing the speech to keywords. According to a study of the US banking market, only 16% of the surveyed banks were able to detect fraud cases in real time, [12].

Approved systems have the ability to self-learn, which increases their effectiveness in the accumulation of a larger number of analyzed events. The creation of "anti -fraud" models and the possibility of their distribution among the participants will increase the level of protection in general for the financial market.

Cognitive calculations are particularly effective in processing and evaluating unstructured data — information that is difficult to structure in rows or columns. In cognitive technologies, such as natural language processing, semantic computing, and handwriting and image recognition, advanced algorithms are used to analyze data to identify valuable information and determine the tone of the text. According to a study conducted by the International Data Group in 2015, almost 90% of the data collected today are unstructured. Thus, the use of cognitive computing can help companies to become a leader in their industry, [18].

For our part, we consider it imperative to use cognitive technologies to ensure information security in the context of the transition to remote customer identification, considering the use of biometrics, [19]. According to a study of the international market for the use of biometric technologies, more than 70% of all biometric information is unstructured, [20]. For this reason, the application of cognitive technologies nowadays looks like the most promising direction for ensuring the protection of information. The existing examples of solving individual elements of biometric identification, already implemented by Russian banks, have proven the high efficiency of using cognitive technologies (based on neural networks, genetic algorithms, and data mining).

Biometrics has already established itself in other areas, such as border control, where increased requirements for correctness and correctness of decisions are also applied. Moreover, these decisions are made in real time, which is especially important for identifying adverse financial transactions when using biometric data, [21], [22], [23].

The development of areas of digital biometric verification, cognitive technologies and the use of artificial intelligence should be as closely integrated with the national Digital Economy program in information security. Ensuring the safe use of biometric identification will be provided through the federal supervisory authority in this area, as well as the creation of working groups between all participants in a pilot project to develop a single biometric system.

The remote identification mechanism is universal and can later be extended to other areas of the financial market, in particular insurance, microfinance, as well as to the sphere of the state and other services. Also, information security solutions that will be implemented for financial companies will find application in these industries, which will significantly reduce costs for future implementations.

5 Conclusion

The need for changes, the transfer of most services to remote services, caused by customer needs will contribute to more active technological changes in banks. The massive use of biometrics will increasingly contribute to this trend. Along with these financial companies, it is necessary to approach with great responsibility the implementation of the information security policy of the operations, as well as the storage and transmission of customer data. The use of cognitive technologies in the near future looks like one of the most promising areas. And despite the high costs of implementation, it can bring tangible results, including financial results, as well as improve business transparency and reduce the negative consequences of various risks. Positive effect will be achieved through the active participation of the state in the development of technologies and regulatory standards within the framework of the Digital Economy of Russian Federation. It is also necessary for financial companies to create partnerships in the development of cognitive technologies in the field of biometric identification and information security. In the near future, it is expected that Russian companies will be able to offer comprehensive solutions, taking into account adaptation to the conditions of the functioning of the modern financial market.

References:

[1] V. Tikhomirov, N. Tikhomirova, *Russia on the way to a smart society: a monograph*, NP Center for the Development of Modern Educational Technologies, Moscow 28-42 (2012)

[2] A. Urintsov, *Knowledge management. Theory and practice*. Yurayt, Moscow (2015)

[3] Tjeu Blommaert, Stephan Van den Broek: *Management in Singularity: From linear to exponential management*, Vakmedianet (2017)

[4] T. Dubovich, *Modern problems of management in the conditions of the information society*. Unity-Dana, Moscow (2012)

[5] W. Toke S Aidt, Facundo Albornoz, Esther Hauk, *Foreign in influence and domestic policy: a survey*, Cambridge Working Papers in Economics: 1928, 14 March 2019.

[6] Markswebb Rank & Report. Internet Banking Rank 2018, https://markswebb.ru/report/internet-banking-rank-2018/

[7] Zhong Dexing, Shao Huikai, Du Xuefeng, *A Hand-Based Multi-Biometrics via Deep Hashing Network and Biometric Graph Matching*, IEEE Transactions on information forensics and security, Volume: 14, Issue: 12, 2019, pp. 3140-3150

[8] Oliver Buckley, Jason R. C. Nurse, *The language of biometrics: Analyzing public perceptions*, Journal of information security and applications, Volume: 47, 2019 pp. 112-119

[9] Md. Khayrul Bashar, *Integrated Biometrics for Human Identification Integrated Biometrics*, 2nd International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS), Graduate Univ, Okinawa Inst Sci & Technol, Okinawa, Japan, 2017, pp. 24-26

[10] J'son & Partners Consulting. World market of biometric systems, 2015-2022. January 2017, http://json.tv/en/ict_telecom_analytics_view

[11] Allied Market Research, *Biometric Technology Market by Type (Face recognition, Iris recognition, Fingerprint recognition, Hand geometry recognition, Signature recognition, Voice recognition and Middleware recognition) and End User (Public sector, Banking & financial sector, Healthcare, IT & telecommunication, and Others)*, Global Opportunity Analysis and Industry Forecast, 2015 – 2022, 2016

[12] IBM Research. Foiling financial fraud (2018), https://www.ibm.com/think/fintech/mastercard-and-ibm-partner-to-make-big-data-work-for-smaller-businesses/

[13] Cognitive computing with using IBM Watson (2017) https://www.ibm.com/systems/ru/power/solutions/cognitive-computing.html

[14] Philip J. Smith, Robert R. Hoffman, *Cognitive Systems Engineering: The Future for a Changing World (Expertise: Research and Applications Series)*, CRC Press; 1 edition, 2017

[15] Krylov, SM, *Formal technology and cognitive processes*. Volume: 24, Issue: 3, 1996, pp. 233-243

[16] Min Chen, Francisco Herrera, Kai Hwang, *Cognitive Computing: Architecture, Technologies, and Intelligent Applications*, IEEE ACCESS Volume: 6, 2018, pp. 19774-19783

[17] Dem'Yanovich Y., Bich L.T.N., *Discrete and continuous wavelet expansions*, WSEAS Transactions on mathematics, Volume 21, 2022, pp. 58-67

[18] Romanchik T., Kitchenko O., Cherkashina M., Shapoval O., Heliarovska O., *Security management of innovation activity of an enterprise based on a multiple-factor approach*, WSEAS Transactions on business and economics, Volume 17, 2020, pp. 664-675

[19] Deloitte risk analysis review. Why cognitive computing has become a turning point in risk management 2019, https://www2.deloitte.com/ru/ru/pages/risk/articles/cognitive-computing.html

[20] *Review of the international biometric technologies market and their application in the financial sector*, Central Bank of the Russian Federation. January 2018. Moscow.

[21] Ella Kolkowska, Annica Jk Kristofferson, *Privacy by Design Principles in Design of New Generation Cognitive Assistive Technologies*, 31st IFIP TC 11 International Conference International Conference on ICT Systems Security and Privacy Protection (SEC), Gent, Belgium, 2016

[22] Marek R. Ogiela, Lidia Ogiela, *Cognitive and Biometric Approaches to Secure Service Management in Cloud-Based Technologies*, IEEE cloud computing, Volume: 5, Issue: 4, 2018, pp.70-76

[23] Doyel Pal, Praveenkumar Khethavath, Tingting Chen, *Mobile payments in global markets using biometrics and cloud*, International journal of communication systems Volume: 24, Issue: 3, 2017 №: e3293.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare that are relevant to the content of this article.

Creative Commons Attribution License 4.0 (Attribution 4.0 International, CC BY 4.0)

This article is published under the terms of the Creative Commons Attribution License 4.0
https://creativecommons.org/licenses/by/4.0/deed.en_US