ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

THE ROLE OF ARTIFICIAL INTELLIGENCE IN THE CYBERSECURITY SYSTEM OF BANKING INSTITUTIONS IN THE CONDITIONS OF INSTABILITY

MAKSYM DUBYNA[1]*, ROMAN SHCHUR[2], OLENA SHYSHKINA[3], IRYNA SADCHYKOVA[4], OLENA PANCHENKO[5], OLENA BAZILINSKA[6]

[1] Department of Finance, Banking and Insurance,

Chernihiv Polytechnic National University, Chernihiv, Ukraine

[2] Department of Finance, Vasyl Stefanyk Precarpathian National University, Ivano-Frankivsk, Ukraine

[3] Department of Finance, Banking and Insurance,

Chernihiv Polytechnic National University, Chernihiv, Ukraine

[4] Department of Finance, Banking and Insurance,

Chernihiv Polytechnic National University, Chernihiv, Ukraine

[5] Department of Finance, Banking and Insurance,

Chernihiv Polytechnic National University, Chernihiv, Ukraine

[6] Department of Finance, National University "Kyiv-Mohyla Academy", Kyiv, Ukraine

E-mail: [1]maksim-32@ukr.net, [2]roman.shchur@pnu.edu.ua, [3]shyshkina.olena.v@gmail.com, [4]aspirant_chstu@ukr.net, [5]pan68@ukr.net, [6]olena.bazilinska@gmail.com

ID 55519 Submission	Editorial Screening	Conditional Acceptance	Final Revision Acceptance
08-09-2024	08-09-2024	01-10-2024	06-10-2024

ABSTRACT

The development of banking institutions in modern conditions is an important condition for the national economy development. The purpose of the article is to study the possibilities of using artificial intelligence technology to increase the efficiency of the functioning of banking institutions in conditions of instability of the external environment. The article substantiates that stability and favorable conditions for conducting business in the field of banking services are necessary to ensure stable economic development of the country. At the same time, effective functioning of the cybersecurity system of commercial banks plays an important role. The essence of such a system and the peculiarities of its formation and functioning are considered within the scope of the article. It was also established that digitalization of the financial services sector is an objective trend in the development of financial institutions. Accordingly, the use of digital technologies for banks today is extremely important to ensure their competitiveness. Artificial intelligence is one of the digital technologies that opens up new opportunities for banking institutions. At the same time, this technology can both contribute to and create risks for the development of commercial banks. Accordingly, such advantages and disadvantages of its use are considered in the article. Considerable attention is paid to the study of the role of artificial intelligence in ensuring stable functioning of the cybersecurity system of commercial banks. The article also substantiates the lack of a comprehensive understanding of the potential of the artificial intelligence technology for the development of banking among scientists and practitioners, and therefore the application of this technology will only expand to various areas of the operation of banking institutions, including the creation of new algorithms and information innovations to increase stability of the cybersecurity system of these institutions.

Keywords: *Banking Institution, Artificial Intelligence, Cybersecurity, Cyber Risks, Macroeconomic Instability, Information System, Analytical Information.*

1. INTRODUCTION

The development of banking institutions is an important condition for ensuring economic growth in the country. Accordingly, stable operation of commercial banks is a necessary condition for the formation of favorable conditions for the national economy functioning, ensuring its stability and the ability to counter external and internal risks. Banking institutions in the vast majority of developed countries play the role of the largest investors and creditors of national economies, which emphasizes an important role of these institutions in providing economic entities with financial resources, creating conditions for their development.

However, commercial banks in today's world also face a significant number of risks. By its nature, the banking activity is a high-risk business, and therefore making correct and balanced decisions in the activities of these institutions is an important condition for their development and effective functioning. Accordingly, managers and owners of commercial banks are constantly looking for the ways to ensure the rationality of managerial decisions, to improve the quality of information and data, based on the analysis of which such decisions are made. To do this, these institutions today actively use digital technologies, the use of which allows obtaining a significant number of advantages for the organization of the operational work of banking institutions, which ultimately has a positive effect on their overall efficiency.

An important condition for ensuring the reliability of a banking institution and stability of its functioning is the construction of an effective cybersecurity system, the presence of which allows preventing the loss of financial resources by these institutions and their clients, the stoppage of the activities of commercial banks due to unauthorized interference in their work. Active use of digital technologies in the work of these institutions also increases the risks of unauthorized access to the information system of a banking institution.

According to estimates, in 2020 cybercrime cost the economy slightly less a trillion USD, and the average the cost of hacking is 4.27 million USD.

Today, financial institutions all over the world spend a lot of money to fight fraud in the financial sector, the volume of which only grows every year. In Fig. 1, the data on losses due to card fraud worldwide are presented.

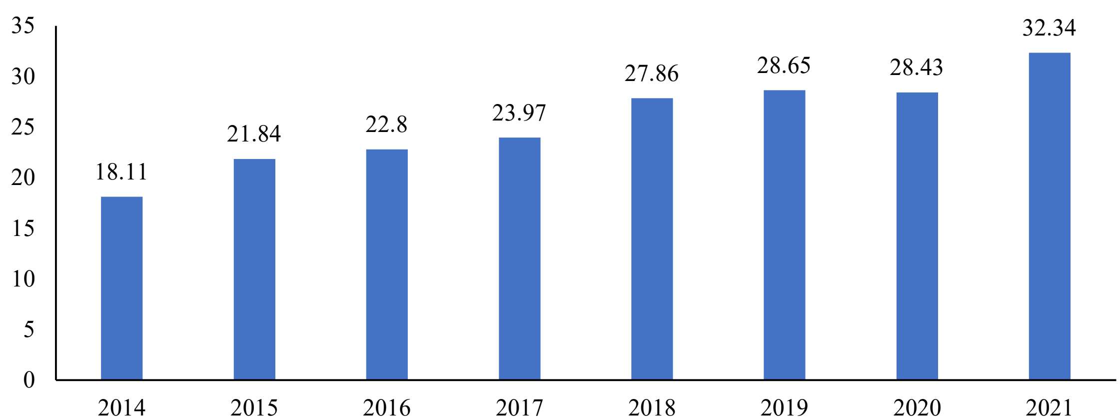


Figure 1: Card fraud losses across the board the world, billion USD

Source: https://www.statista.com

The forecasts of specialists in the field of financial services are quite pessimistic, since most are sure that the scale of fraud and cybercrime will only increase in the future around the world. Cybercrime has had an unprecedented impact on businesses across various industries, with a projected cost of 8 trillion USD in 2023 and 10.5 trillion USD by 2025 [1].

Accordingly, banking institutions actively involve digital technologies not only to improve the quality of providing financial services to their clients, but also to ensure reliable functioning of their own cybersecurity systems. One of the most important of these technologies is the artificial intelligence technology, which is gradually being used today by financial institutions to improve the efficiency of their own work and ensure the level of information security. The increase in demand for the use of this technology is also confirmed by the results of studying the opinions of experts and conducting analytical work. In particular, according to Statista, the global artificial intelligence market is expected

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

to experience tremendous growth over the next seven years, increasing from 200 billion USD in 2023 to 2 trillion USD in 2030. Already in 2023 in the USA accrued about 15,000 companies from artificial intelligence, and this it is expected that number will continue to grow

Today, the issue of using artificial intelligence technology specifically in the formation of reliable cybersecurity systems of banking institutions is insufficiently studied. It is quite clear that the potential of such technology is also significant in the field of information security. The market value of artificial intelligence in cyber security is expected to reach 46.3 billion USD in 2027 [1]. However, the possibilities of using artificial intelligence in the work of banking institutions, taking into account the nature of such technology, are really not yet fully studied and implemented by scientists and practitioners. Information protection is only one of the areas of the application of this technology; however, it is information security that forms the basis for stable operation of commercial banks, and this technology can play a key role in the construction of modern cybersecurity systems of these institutions.

Thus, the main goal of the article is to research the possibilities of using artificial intelligence technology to increase the efficiency of the functioning of banking institutions in conditions of instability of the external environment.

To achieve the set goal, the following tasks were performed: analyze the prerequisites for the formation of a cyber security system in the functioning of banking institutions; to investigate the essence and structure of the banking institution's cyber security system; justify the peculiarities of the use of artificial intelligence technology in the activities of banking institutions; describe the potential of using artificial intelligence technology in the work of commercial banks; determine the risks associated with the use of this technology; determine the advantages of using artificial intelligence to increase the effectiveness of the banking institution's cyber security system and describe the main digital technologies that should be used to ensure the effectiveness of such a system.

2. LITERATURE REVIEW

Scientific works of many researchers are devoted to the study of the use of artificial intelligence technologies in the activities of banking institutions and their role in ensuring cybersecurity in the conditions of modern challenges and threats. Articles [2-11] are devoted to various aspects of ensuring cybersecurity in banking institutions.

In the scientific paper [2], the authors note that the importance of cybersecurity in several areas of national security and the global trade system is of concern to many countries around the world. The authors of the study investigated the peculiarities of ensuring cybersecurity in Jordanian banks.

Scientists [3, 12] believe that cyber-attacks are more appropriately classified as a critical risk due to the increased use of the technology and new developments in digital transformation that dominate service sectors such as the banking one. According to scientists, it is necessary to provide clear control in the cybersecurity management mechanisms of banks to ensure an acceptable level of risk in the process of carrying out financial transactions. The authors also considered the trends of the Eurozone and the prospects for the use of the digital currency of central banks within the framework of the implementation of the European Green Agreement.

The basis of article [4] is the development of methodical and practical recommendations for the elimination of the payment system oversight threats, stabilization of the protection of participants and users of the payment portfolio of banking institutions against misinformation and fraud. The authors proposed a synergistic cybersecurity model, which takes into account securitization of the payment portfolio of banking institutions in the financial market and is aimed at preventing threats and meeting the needs of participants and users of banking services.

The study [5, 13] found that one of the biggest threats facing the banking sector worldwide is credit card fraud. The authors proposed a completely new deep learning algorithm for use in cybersecurity applications to detect theft in the banking industry. The authors analyzed the development of the credit market of Ukraine in the conditions of macroeconomic instability.

Studies [6-7, 14] argue that by providing a comprehensive and accurate approach to assessing the business costs of security attacks, big data analytics can help banks reduce operational risks and improve their cybersecurity. The importance of making optimal strategic decisions in such a complex environment has also been proven. Scientists have modeled financial influence of political-oligarchic interests of state-sponsored enterprises on the formation and implementation of the financial policy in the state in the context of modern challenges and instability.

The practical value of the study [8-9] is to focus on understanding cybersecurity threats and defense approaches that should be used to protect against

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

threats from financial institutions. The authors proposed a model of cyber risk management and control, based on the identification of the most complete assessment methods, qualitatively and quantitatively, which can better describe possible effects of its manifestation on the bank's activities.

The authors [10-11] are convinced that the more information technology is used, the greater the gaps in security incidents and the potential for cybercrimes, so cybersecurity becomes an important factor in minimizing this problem. Scientists analyze in detail the cybersecurity of Internet banking in three developing countries, and then propose a new model for reducing cybersecurity risk to bridge the gap between banks and customers.

Let's consider the existing research in the direction of the peculiarities of the use of artificial intelligence technologies in the activities of banking institutions. Interesting from the applied side is the study [15], within which it was studied how the consequences of the Covid-19 pandemic mitigate the impact of artificial intelligence on effective application of cyber management in Islamic banks. As a result, the significant influence of artificial intelligence on the effective application of cyber management in Islamic banks has been proven.

Research [16-18] is aimed at studying artificial intelligence marketing, and is also aimed at improving the level of customer experience of banks with the help of artificial intelligence and creating long-term relationships with customers. The authors also researched the applied aspects of artificial intelligence in the context of assessing the safe development of business.

Within the scope of article [19], the authors check the possibility of artificial intelligence to decipher the messages of the European Central Bank. It is noted that the author's indicator based on artificial intelligence repeats quite similar indicators based on human expert judgment, but at a much higher speed and with lower costs.

The relevance of research [20-24] is the study of banks on investments in new technologies, such as artificial intelligence, blockchain, since their main goal has become customer loyalty and satisfaction thanks to digital transformation. The research focuses on studying the impact of artificial intelligence techniques through the CAMELS approach for cross-sectional analysis of the bank financial performance.

Considering the relevance and timeliness of research conducted by scientists from different countries of the world, we would like to draw attention to the fact that the issue of researching the role of artificial intelligence in ensuring the cybersecurity system of banking institutions in the conditions of instability requires further study and analysis of challenges and threats in this direction.

3. METHODOLOGY

The article uses a range of scientific methods to substantiate the possibilities of using the artificial intelligence technology in ensuring reliable functioning of the cybersecurity system of banking institutions.

In particular, a systematic approach was used to justify the essence and features of the construction of the cybersecurity system of the banking institution. This was implemented through the use of the content analysis method to study the essence of the concepts of "cybersecurity", "artificial intelligence" and the method of historical analysis to specify the prerequisites and reasons for the formation of the cybersecurity system in banking institutions. The system approach is used from the position of describing the essence of the system according to the scheme.

$$\begin{cases} S^t \to S^{t+1} \\ S = \{C; R\} \\ C = \{c_1, c_2, c_3 \ldots c_n\} \\ R = \{r_1, r_2, r_3 \ldots r_n\} \\ S = \{f; p; p_r; r_s\} \\ Exf \to S^t \leftarrow Enf \end{cases} \tag{1}$$

where *St* – the system at time t;
C – a set of components (c) of the system;
R – a set of interconnections (r) of the system;
f – system functions;
p – properties of the system;
p_r – principles of the system;
r_s – system resources;
Exf – external factors;
Enf - internal factors.

The article also uses methods of comparative analysis, statistical methods to present data on modern trends in the development of the artificial intelligence technology, current trends in its use in the field of cybersecurity and information security of commercial banks.

The application of methods of comparison, abstraction and systematization made it possible to specify the possibilities of using artificial intelligence technology for the development of

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

banking institutions, to determine the risks of using such technology. Also, the use of the outlined methods made it possible to substantiate the features, advantages and disadvantages of using artificial intelligence technology in ensuring the effective functioning of the banking institution's cybersecurity system.

4. RESULTS

The importance of ensuring the development of cybersecurity systems in the modern world is a crucial element in creating conditions for stable functioning of all economic entities without exception. Already today, it is quite clear that cyberattacks are objectively an integral part of the development of economic systems, since they are carried out constantly, their nature changes in accordance with the new possibilities of modern information and communication technologies. In Fig. 2, individual statistical data on the current state of cyberattacks in the world are presented.

From the data of Fig. 2, we can conclude that in 2023, 18.2% of all cyberattacks occurred in the field of financial services, which indicates the presence of significant threats to the functioning of banking and non-banking financial institutions. At the same time, if in 2018 55.1% of economic entities faced cyberattacks, then in 2023 – 72.7%. This only emphasizes the urgency of building effective cybersecurity systems for them. In turn, in 2023, 64% of financial institutions were affected by cyberattacks that affected their stable functioning. Analytical data also show that in most cases, among the reasons for carrying out cyberattacks, financial gain is the primary reason for fraudsters. This is confirmed again by the data of Fig. 2. In 2022, 73.9% of cyberattacks were carried out with the aim of embezzling financial resources.

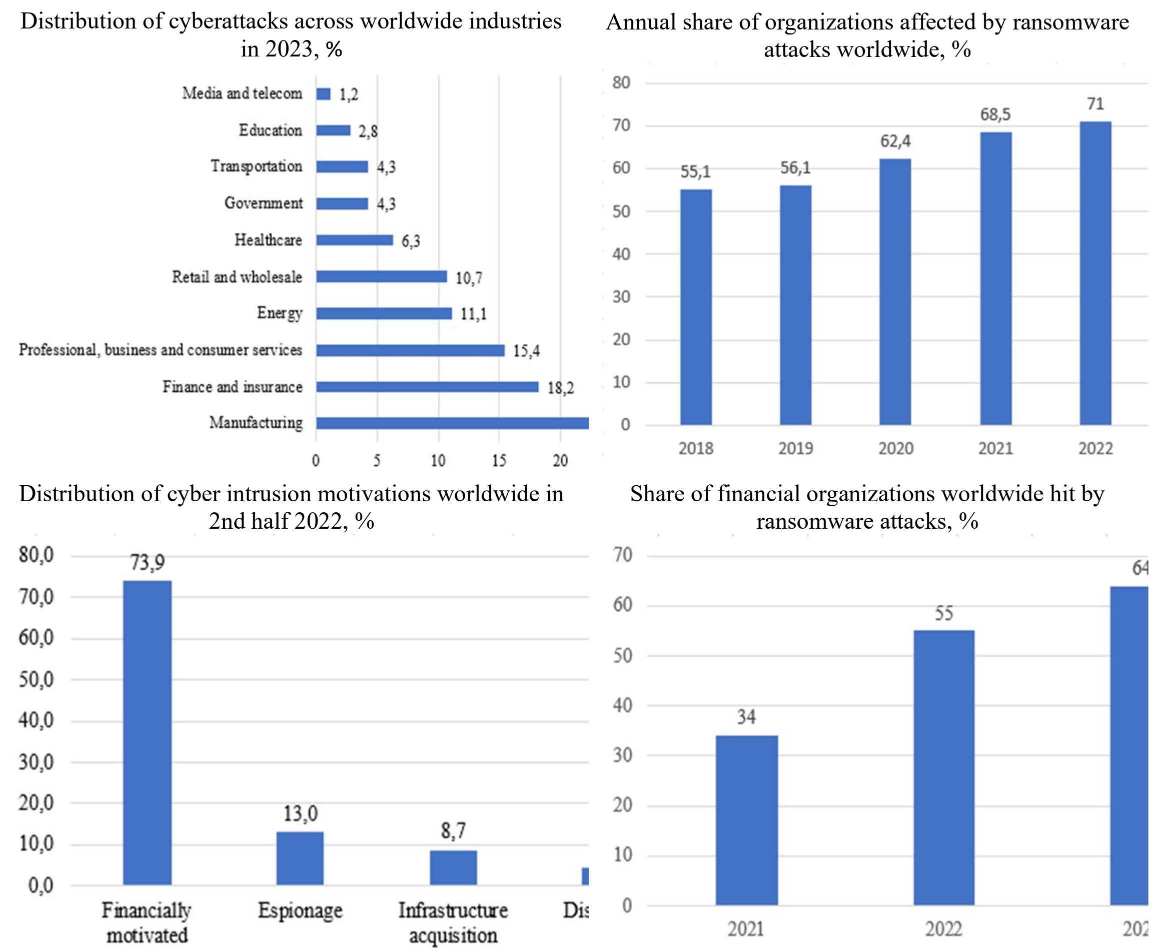


Figure 2: Information on the state of cyberattacks in the world

Source: https://www.statista.com/topics/9918/cyber-crime-and-the-financial-industry-in-the-united-states/#statisticChapter

Journal of Theoretical and Applied Information Technology
15th October 2024. Vol.102. No. 19

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Data on cyberattacks and their impact specifically on the activities of economic entities in the USA once again confirms their rapidly growing influence on the functioning of economic entities. The corresponding information is presented in Fig. 3.

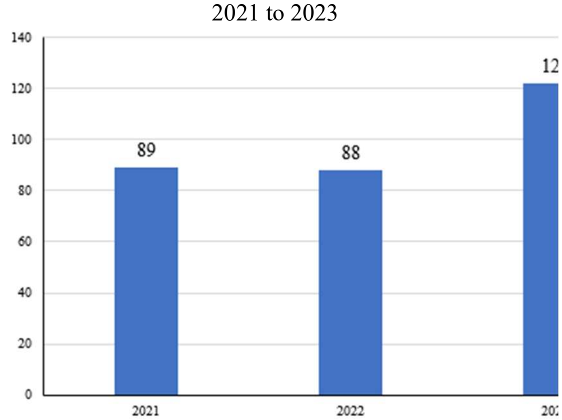
Among various types of the economic activity, operation financial institutions is in second place in terms of the number of cyberattacks on their stable work. In 2020, there were 138 such cases, and in 2023 – 744. This growth is the largest among all industries. The number of annual requests for cyberattacks is also increasing. In 2023, their number was 122 units, although just two years ago in 2021 - 89 units. According to Fig. 3 in the USA, people aged 35 to 54 are most affected by cyberattacks among citizens. This is quite understandable, since this group of citizens is the most economically active and uses financial services most often.

The outlined once again confirms that the construction of effectively functioning information security systems becomes important for economic entities that carry out their activities stably, are highly profitable institutions, or their functioning is connected with the movement of significant amounts of financial resources. Accordingly, the analysis of modern trends in the functioning and development of cybersecurity systems, primarily of banking institutions, is important from the standpoint of ensuring and stable operation of the banking and, accordingly, the financial system of any country.

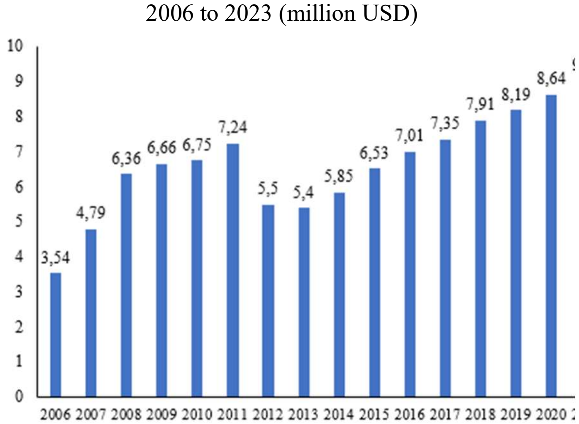
Number of cases of the data violation due to cyberattacks in the United States from 2020 to 2023, by industry

Characteristic	2020	2021	2022
Healthcare	306	330	343
Financial services	138	279	269
Manufacturing and utilities	70	222	249
Profwssional servoces	144	184	223
Education	42	125	100
Technology	67	79	87
Government	47	66	74
Non-profit/NGO	31	86	72
Retail	53	102	65
Transportation	21	44	36
Hospitality	17	33	34
Other	172	308	250

Annual number of complaints about ransomware attacks in financial industry in the United States from 2021 to 2023



Average cost of a data breach in the United States from 2006 to 2023 (million USD)



Share of Americans being a victim of financial cybercrime or fraud, by age group

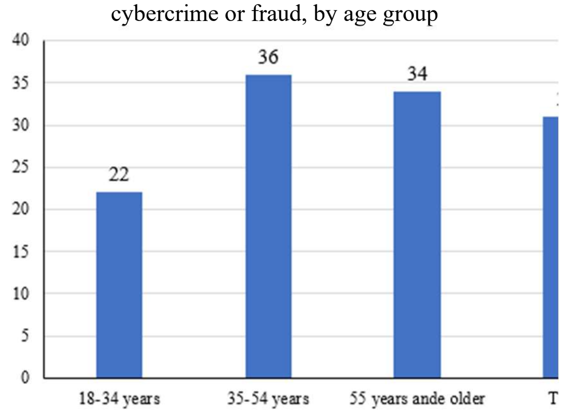


Figure 3: Information about the state of cyberattacks in the USA

Source: https://www.statista.com/topics/9918/cyber-crime-and-the-financial-industry-in-the-united-states/#statisticChapter

We will conduct an analysis of the essence and features of the functioning of the cybersecurity system of banking institutions. It should be noted that this system arose and gradually developed within the functioning of any commercial bank in the process of changing the external environment in

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

which such a bank develops and the reasons for this were as follows:

– active use of automated financial information processing systems;

– use of information and communication technologies to ensure smooth operation of banking institutions;

- attractiveness of commercial banks for fraudulent activities aimed at stealing financial resources and management information;

– speeding up the processes of collecting and processing information within the banking institution, increasing its amount, which requires the use of appropriate technologies;

– constant increase in the number of cyberattacks on banking institutions;

- growing popularity of mobile applications developed by banking institutions for clients and, accordingly, creating new opportunities for fraudsters to intervene in the banking institution's information system;

- significant growth of the volumes of private information about customers, which the bank institution is obliged to keep;

- development of non-contact payments that requires development and using corresponding informative security;

- significant role of the cybersecurity system of the banking institution in shaping its reputation, and therefore competitiveness in the banking services market, etc.

Considering the objectivity of cyberattacks and their constant existence, commercial banks in today's digital world agree to spend significant financial resources to ensure the creation of reliable information systems that would, on the one hand, contribute to the high quality of providing financial services to customers, and on the other hand, would not allow unauthorized internal and external penetration into the information security system of a banking institution. At the same time, the importance of the effective functioning of the cybersecurity system of banking institutions in modern conditions is also determined by the increase in the volume of financial services provided online. According to experts' forecasts, in 2024, the volume of online payments will also grow significantly and reach approximately 11.55 trillion US USD. It is quite clear that the field of financial services is becoming very attractive for fraudsters, given its dynamic development and the number of financial resources used in it. Accordingly, this determines the importance of building effective cybersecurity systems of banking institutions. Schematically, a typical scheme of such a system is presented in Fig. 4.

Of course, in modern realities, commercial banks are constantly trying to find ways to improve the effectiveness of their own cybersecurity system and generally ensure profitability. Without the use of digital technologies, it is extremely difficult for these institutions to do this today. Commercial banks involve various types of such technologies for working with information, performing analytical work. One such technology that has significant potential for use in banking is artificial intelligence (AI) technology.

penetrates into various spheres of the society's functioning. Its growing role in the development of financial institutions (banking and non-banking) is especially noticeable. This is possibly due to the fact that financial institutions have financial resources to develop and implement new, not always cheap, innovative solutions for their own activities. Moreover, the entire sphere of financial services is built on the implementation of risky activities, the level of risk depends on the quality of the processing of information available to financial institutions. And most of the modern digital technologies are developed just for this.

Artificial intelligence is a set of digital technologies that allow performing complex operations, including those that require the involvement of an intellectual resource for their implementation, processing of large amounts of information, with the aim of quick analysis. Artificial intelligence technology is especially useful and important for organizing the work of those systems in which information resources and the efficiency of working with them play a key role in the development of such systems. Of course, all financial institutions can be attributed to such systems, since the entire sphere of financial services is an intangible sphere of the national economy, in which the circulation of financial resources occurs as a result of managerial decisions by a significant number of economic entities.

It is also worth noting that the use of the artificial intelligence technology in the work of banking institutions is possible not only in the field of providing financial services by these institutions to their clients, but also in the direction of the organization of their economic activities, analysis of financial services markets from the position of not the providers of these services, but their consumers (interbank lending markets, other non-bank financial services markets). Intuitively analyzing the peculiarities of banking institutions, we can conclude that the artificial intelligence technology can be used in virtually all types of financial services provided and consumed by these institutions, and it is quite difficult to clearly outline the potential of its use.

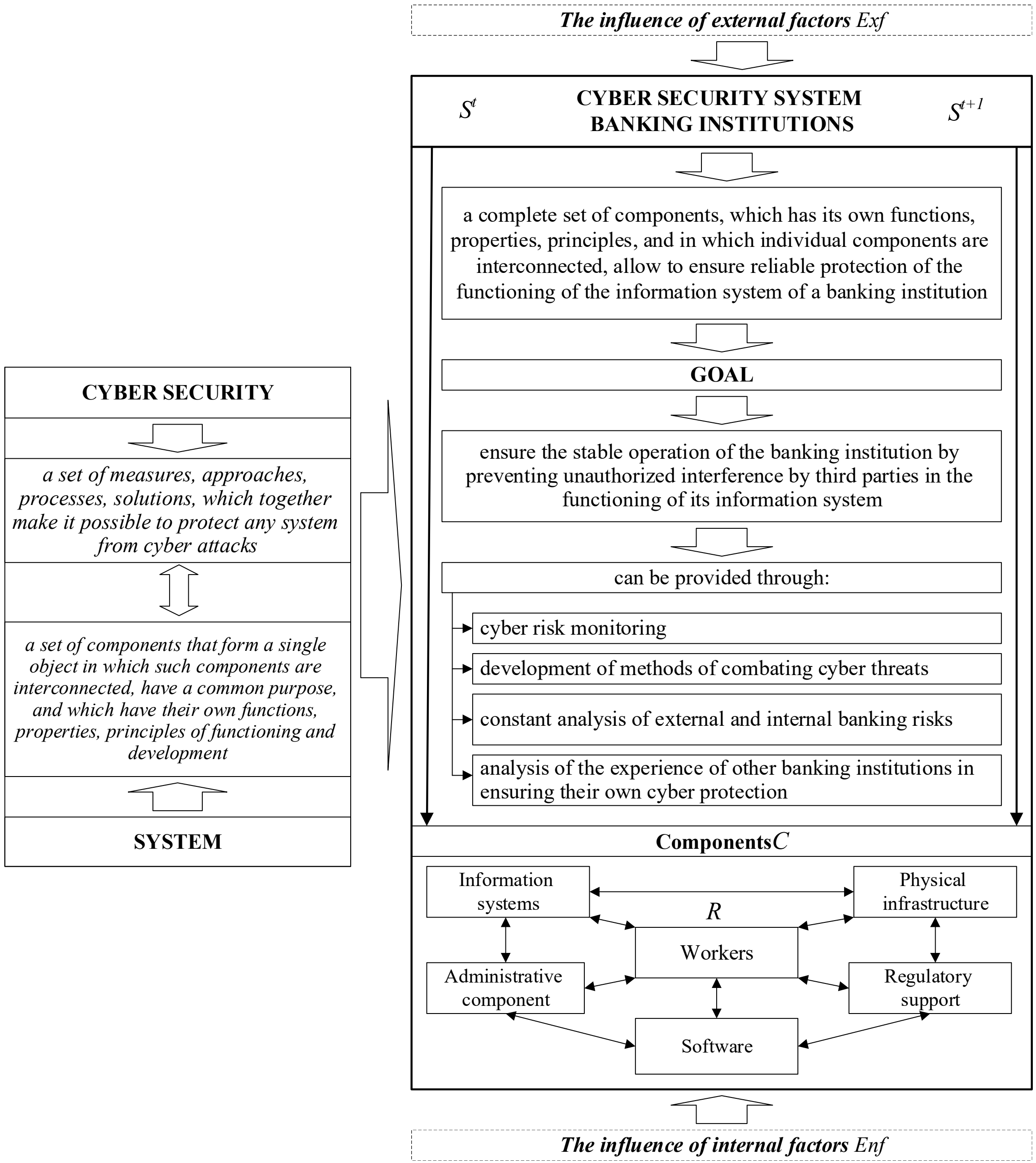


Figure 4: Cybersecurity system of the banking institution

Source: constructed by the authors

In the activity of banking institutions today, the artificial intelligence technology is already used, but the potential of its application to increase the efficiency of the work of these institutions is enormous. This technology allows:

– reduce the operational costs of the banking institution;

- implement mechanisms for automatic verification and analysis of legal documents;

- digitize paper documents, internal reports;

– create chatbots for promotion quality informative service clients (households, subjects entrepreneurial activities);

- simplify implementation routine processes which before performed by the employees themselves (introduction data, registration reports, preparation analytical reports, etc.);

- increase quality service customers, first of all households through introduction algorithms effective work with them requests, including automatic solution of typical problems and requests;

- rationally use the time of bank employees for implementation more intellectually complex tasks;
- increase the quality of the loan portfolio through deeper analysis of the creditworthiness potential of loan sharks, faster adoption issuing decisions loan;
- contribute to the improvement work with creditors debt through implementation algorithms more thorough analysis financial status of potential borrowers, studying non-financial open information about them;
- contribute in general increase of the functioning systems management by all banking risks (the best analysis, search for best direction by detecting potential risks);
- carry out search for new directions in the attachment of banking resources;
- conduct more systemic analysis of the modern trends of the financial market functioning, determine competitive positions of banking institution in the banking services market;
- to develop new individual banking products, especially for subjects of the entrepreneurial activities, which inherent to the implementation of significant number of features of economic activities;
- create more realistic forecasts on further development of banking institution based on the results analysis of its current state, research of the external environment in which it develops, analysis of individual markets of banking services and the state of competitors in this market and other directions.

Also, the artificial intelligence technology can be very useful for provisioning physical security employees of banking institution in separate branches and representative offices. In particular, application of these technologies allows analyze materials of video surveillance, conduct video analytics and determine potential criminals, analyze the work of banks institutions, behavior of employees of individual structural subdivisions of commercial banks, explore the surrounding perimeter of the territory in relation to the location of the banking institution.

In Fig. 5, the data and poll results of the employees of financial companies that provide services in the field of payments, regarding the prospects of using the artificial intelligence technology in their activities are presented.

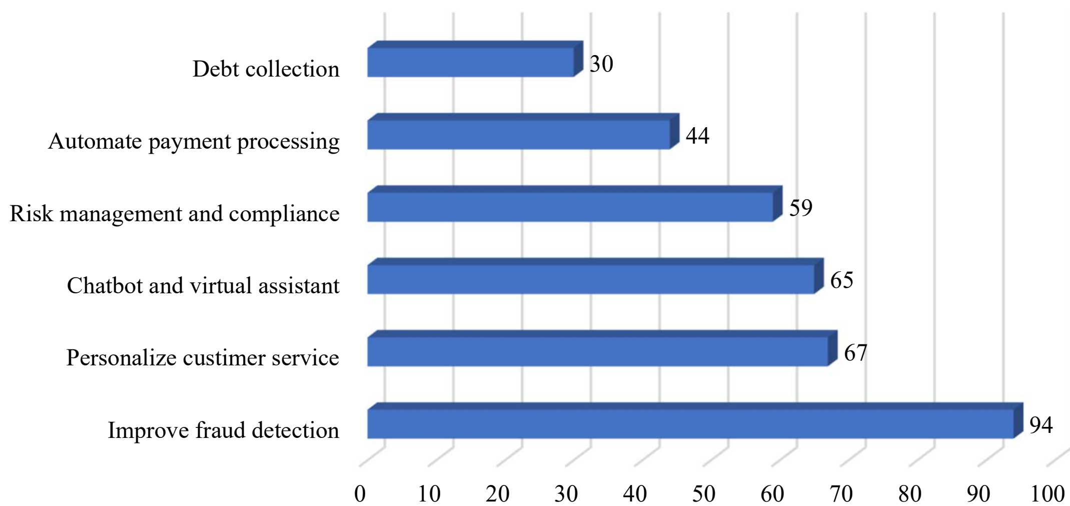


Figure 5: Prospects using technologies of artificial intelligence in payments, %

Source: https://www.edgardunn.com/articles/the-impact-of-artificial-intelligence-and-machine-learning-on-the-payments-industry/

Thus, the data analysis confirms that, according to experts, the greatest potential of using the improvement of the artificial intelligence technology is in the direction of improving the quality of the functioning of cybersecurity systems through the mechanisms for detecting and preventing cyber risks using such technology (94%). In second place is the use of artificial intelligence for development of individual financial products and personalization of financial services (67%). Using chatbots and virtual service assistants' customers - on the third levels (65%).

So, there exists a significant number of benefits and potential opportunities at work of the banking institution where artificial intelligence technologies are used, and they really can be useful and contribute to the development However, it is also worth understanding what to use this one technology in any direction, it is necessary to develop from the beginning the corresponding informative solutions, algorithms and methods for its application in that or another sphere. It requires from banking institutions already relevant resources: financial, intellectual, time.

Of course, active using of artificial intelligence technologies has its own disadvantages, which are also not always at once understandable Risks of using this technology in the first place, as evidenced by world experience, lie in its still insufficient development and adaptation to the activities of commercial banks. Accordingly, there are constant threats that the use of this technology, a long period of its development, implementation, adaptation to the business model of a specific banking institution will not allow to achieve the expected results, it will require more time, additional financial resources, professional training, etc.

Sometimes introduction of new information innovations leads to a decrease in information security of banking institutions. The cybersecurity system of the banking institutions also becomes more vulnerable to improper use of the artificial intelligence technology by providing banking services. At the same time, highly qualified specialists can be distracted from traditional tasks and get involved in developing new solutions based on the use of this technology, which temporarily negatively affects the functioning of the banking institution.

Unsuccessful using artificial intelligence technologies in operation of banking institution can lead not only to losses of investment resources that were spent on the development of these technologies, but also to have more serious consequences for a commercial bank, namely:

- lead to financial losses of customers from improper functioning of the informative systems of banking institutions;
- occurrence of fraudulent actions due to imperfect new digital innovations in operations of bank institutions;
- decrease reputation of the commercial bank;
- outflow potential customers of commercial banks that they can refuse from work with banking institution as a result reluctance use of new ones in the own activities of the digital technology, etc.

It should be noted that customers are not always ready to adapt to enough fast changes in the field of granting financial services, actively use new banking products and services. For subjects of the entrepreneurial activity banking services are more infrastructural as an element software stability in their business. Accordingly, with great attention spent to using new products, technologies in this sphere, not everyone is eager to become a client. That is why the introduction of any digital innovations in operation of commercial banks should be balanced and thoroughly planned. Maybe after making enough thorough evaluations of implementation features of new digital innovations, their potential for change, resources that must be spent on their implementation, influence on all business processes in the banking institution.

Effective using of artificial intelligence technologies in banking institutions in the future should be accompanied by:

- compliance with ethical aspects of commercial banks by application of the technologies of artificial intelligence by granting own financial services;
- permanent increase of security of the customers' confidential information, both households and especially subjects of the entrepreneurial activities for which preservation management information is an important aspect of security for own economic sustainability, competitiveness and information security;
- taking into account the restrictions of artificial intelligence technologies by adopting the decisions, if necessary, individual social, psychological, mental, emotional factors must be considered;
- specification of the strategies implementation of the artificial intelligence technology in activity bank institution, description of the expected effects from using this technology, risks which directly will arise with its use.

Undoubtedly, one of the most important roles should be played by the artificial intelligence technology in construction of effective cybersecurity systems of banking institutions. Exactly this technology better may cope with tasks regarding detection of potential threats in information spacious, estimates their possible impact for the bank's operation, using the measures leveling the cyberattack impact.

Using artificial intelligence technologies by providing security in the effective functioning systems, namely cybersecurity in the banking institution can allow:

- determine hacking attacks in real time by analyzing changes in information system of the banking institution, external environment, with elements with which this system interacts;
- consider and analyze features of hacker attacks, their nature, and in the future use these ones to protect information from new, similar hacker attacks;

- periodically carry out the detailed analysis of the internal state cybersecurity systems of the banking institution to determine potentially dangerous threats;

- suggest directions for promotion the efficiency of the functioning cybersecurity systems of the banking institution, analyze characteristics and specific features which are already effective in the current model systems in other banks;

- create models and technologies that are unique in the essence of the prototypes of real operational processes, however actually which are called distract to confuse cybercriminals in their actions and do not allow carrying out real negative impact on the functioning banking institution;

- provide necessary reliability level of cybersecurity systems on different stages of development of banking institution; multiply the quantity of structural branches may reduce the security level of the banking institution from external intervention, however exactly using artificial intelligence technologies allows avoiding without involving additional specialists;

- formation of synergistic effects from effective using of the artificial intelligence technology to provide actual cybersecurity system of the banking institution which consist in demotivation of cybercriminals to carry out attacks in individual banking institutions because of the bigger number of them are looking for always more simple and safe methods to carry out fraudulent actions;

- form positive reputation to the banking institution through its reliability, security of financial, informational resources that helps involvement of new customers looking for services, etc.

The use of the artificial intelligence technology in ensuring effective functioning in the cybersecurity system of the banking institution currently consists in the use of the following types of digital innovations:

1) biometric authentication – a change in the approach to the identification of a person who wishes to receive a financial service, access to the use of financial resources. If before such access was provided using digital verbal data (pin-codes, secret words, etc.), then today banking institutions and fintech companies go to the identification system of the client using fingers' prints, face recognition, voice recognition. This approach provides more reliable way of the customers' identification, makes it impossible of the information kidnapping about access to their own accounts and their using by another person A disadvantage of this is what it has today certain problems and not enough reliable and efficient in the process of the customers' identification.

2) behavioral biometrics is a new technology that is the best to implement in the cybersecurity system of the banking institution precisely because of using the capabilities of artificial intelligence. This technology consists in analysis the customers' behavior of banking institutions through study the features of their use of mobile application of this institution, its website, results of the actions in online offices. When detected a typical behavioral pattern for this client, which was not implemented before, the system can either block actions the client or limit his opportunities of using financial services for a certain time.

3) identification language - detailed analysis of the client's languages, his usual intonation in conversations. The results of this analysis allow accurate the client's identification and perform his authorization exclusively through voice teams It much simplifies receiving financial services, their speed for the client.

Today, using the voice of citizens in the field financial services and in other areas of the economic activity acquires significant popularity because it much accelerates purchase goods and services by the customers. However, in many cases technologies of voice processing is not perfect yet. In many cases, as shown by the results carried out during the experiments, the voice can be imitated by others consumers. It indicates insufficient depth of the analysis of conversational style of customers However, in the future this technology will be rapid to be developed and used in various fields, as it significantly simplifies the process using different services due to lack of need for conducting constant personal identification, set of passwords, confirmation in applications by carrying out different operations.

The advantages of using the artificial intelligence technology in the cybersecurity system of the banking institution are presented in Fig. 6. Analyzing the data of this figure, the essence of the artificial intelligence technology, the nature of the banking activity, it can be argued that in the process of building a cybersecurity system, this technology can play a dual role. On the one hand, this technology makes it possible to increase the resilience of the cybersecurity system to external threats, to ensure its flexibility, efficiency, and quick response to new threats from the external environment for the banking institution.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

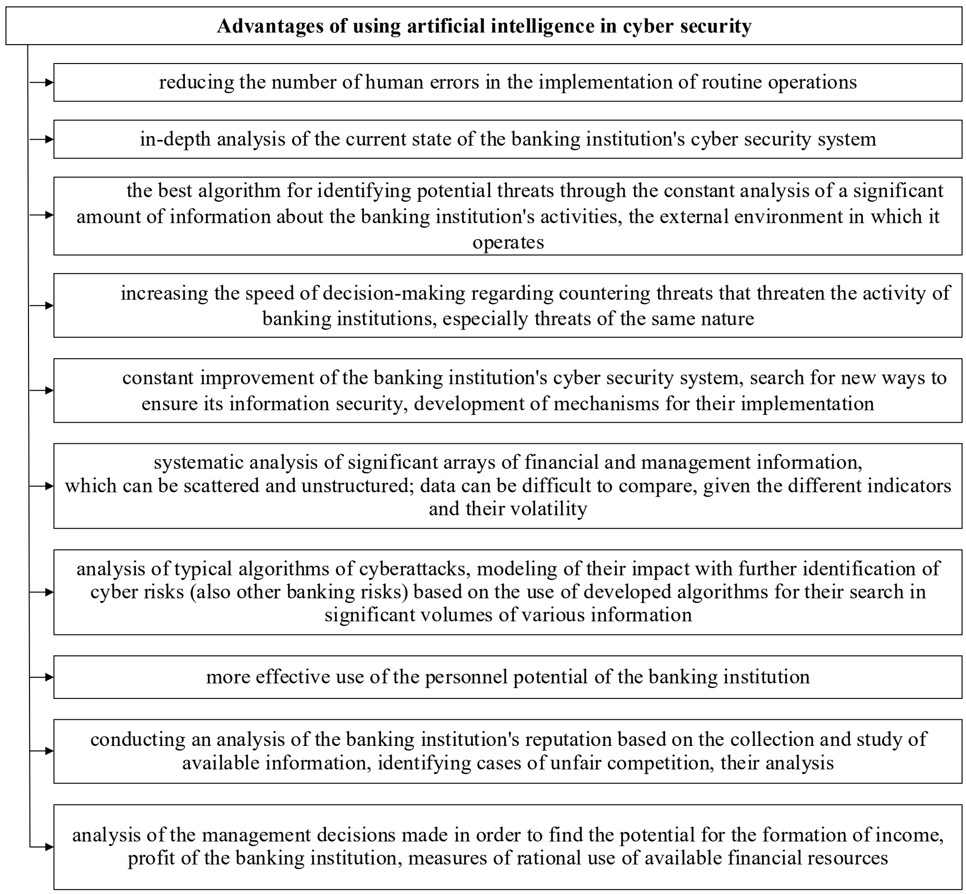


Figure 6: Advantages of using the artificial intelligence in cybersecurity system

Source: compiled by the authors

On the other hand, artificial intelligence as a technology also carries certain risks and threats when using it for the banking institution, since the potential of this technology has not been studied enough. This technology, in its essence, remains a set of digital innovations that are developed directly by specialists. Accordingly, there is always a possibility of external intervention in the work and the technology of artificial intelligence itself, which can have extremely complex consequences for the functioning of commercial banks.

In Fig. 7, the results of a survey of experts regarding the threats of using the artificial intelligence technology in the activities of financial companies are presented.

The use of the artificial intelligence technology is not fully adapted to the activities of financial institutions. This process only happens gradually within the limits of their activity. Accordingly, it is impossible to guarantee completely safe use of this technology for banks, their clients, financial resources of economic entities. At the same time, artificial intelligence as a technology can be actively used in the future to find vulnerabilities in the protection of the information system of banking institutions, analyze data about competitors, and find vulnerabilities in their activities in order to use such information in the highly competitive market of banking services.

Another disadvantage of the use of the artificial intelligence technology is that quite often its use within the cyber protection system of a banking institution requires not only additional financial resources, but also changes to the information system already formed over a certain period of time, its modernization and adaptation to the capabilities of this technology. This, in turn, requires a change in approaches to ensuring the flow of information between structural divisions, its analysis, retraining of employees, etc.

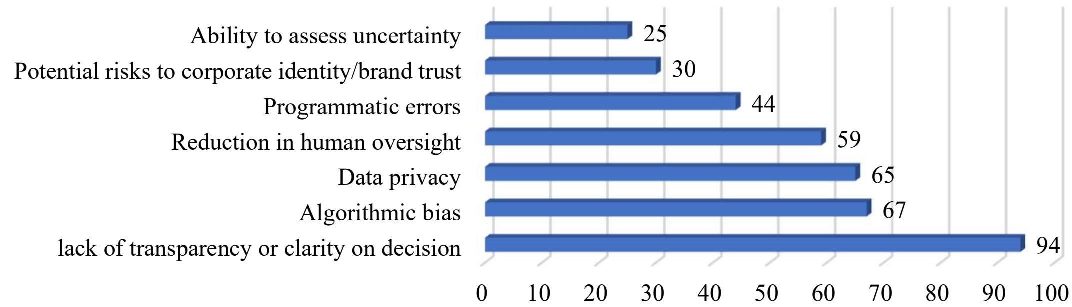


Figure 7: The main risks associated with the implementation of the artificial intelligence and machine learning technology in the activities of financial institutions, %

Source: https://www.edgardunn.com/articles/the-impact-of-artificial-intelligence-and-machine-learning-on-the-payments-industry

Also, the use of the artificial intelligence technology in the banking sector is currently not specifically regulated at the state level. However, most countries are gradually developing requirements for the use of this technology by commercial banks, which will directly affect the activity of its use.

However, today it is quite clear that the prospects for the development of artificial intelligence in the banking sector, in increasing the effectiveness of the cyber protection system of commercial banks, are irreplaceable and important, since, in addition to banking institutions, the same technology can also be used by criminals to interfere in the work of these institutions for the purpose of enrichment, violation of their operational activity, which ultimately negatively affects the work of banks, their reputation and stability of functioning.

Undoubtedly, today, conducting research in the field of building effectively functioning cyber security systems of banking institutions remains relevant, taking into account the constant variability of the economic and informational environment in which such institutions function. However, there are certain difficulties and limitations for the implementation of such studies. In our opinion, they include, first of all, the lack of reliable statistical information on the number of cyberattacks on the activities of commercial banks, the losses that such institutions received. Quite important for the search for tools to support the reliability of information systems of commercial banks is the direction of analysis of information about violations of the normal functioning of such systems in specific banking institutions, which would make it possible to single out among them those that have used more successful digital solutions to ensure their own cyber security. Another limitation that does not make it possible to conduct a more in-depth study of the role of artificial intelligence in the formation of cyber security systems of banks based on the use of analytical data is the lack of developed methods of collecting information about the use of this technology in general in the work of commercial banks, partial concealment of such information from competitors.

In our opinion, the topic explored in the article is topical for further research. In particular, an interesting direction is the development of scientific approaches to the formation, updating of the digitalization strategy of banking institutions, taking into account the capabilities of artificial intelligence and the objective need to build effective cyber protection systems of these institutions. Also, issues regarding the development of methodological procedures for the introduction of artificial intelligence technology into the specified system remain understudied.

The scientific novelty of the study is the substantiation of the role and determination of the possibilities of using artificial intelligence technology to increase the effectiveness of the functioning of the cyber security system of banking institutions, which, unlike existing studies, was implemented on the basis of a detailed analysis of the features of the use of AI technologies in the field of financial services and the specification of the advantages of its application in building a stable functioning information security system of commercial banks.

5. CONCLUSIONS

So, the article achieved the set goal of the research, which was to analyze the possibilities of using artificial intelligence technology to increase the efficiency of the functioning of banking institutions in conditions of instability of the external environment, in particular, the relevant tasks were solved.

The article conducts a thorough study of the potential of using the artificial intelligence technology in the construction of the cybersecurity system of banking institutions. It was found that active further use of digital technologies by all financial institutions, including commercial banks, creates new challenges for their managers to ensure the appropriate level of their information security. Only in such conditions is possible to ensure the stability of the work of banks and, accordingly, of the country's banking system in general.

Digitalization of the financial sphere is an objective process, and therefore the search for new directions for ensuring the reliability of cybersecurity systems of banking institutions is becoming very relevant. Already today, an integral component of the digital transformation of financial institutions is the use of the artificial intelligence technology. First, managers of financial institutions considered this technology as a convenient way to improve the quality of financial services. However, it later became clear that the potential in the use of artificial intelligence in the financial sphere is enormous. This especially applies to the field of cybersecurity.

In the article, the essence of the cybersecurity system of banking institutions is analyzed in sufficient detail, and it is clarified that this system consists of a significant number of interconnected components, ensuring the functioning of which is extremely important for the formation of information security of these institutions. Accordingly, considerable attention is paid to the issue of using the artificial intelligence technology in general in the development of commercial banks and, accordingly, their cybersecurity systems.

A detailed analysis of the nature of the artificial intelligence technology, the features of its use in the activities of various economic entities allowed us to determine both the advantages and risks of its use in banking. In the vast majority of cases, threats of this technology are associated with insufficient study of the potential of its use, opportunities to ensure the effective work of various economic entities. However, as the use of this technology becomes more widespread, commercial banks will better understand the possibilities of application that are safe for their work, and ready-made solutions for the use of artificial intelligence in certain areas of the activity of these institutions will be developed accordingly.

The process of active use of the artificial intelligence technology is already taking place, precisely because, as the results of the study proved, the issues of limiting the negative impact of this technology on the work of commercial banks and the banking system in general are becoming important. This will require the development of appropriate legal, organizational and institutional support, taking into account an important role of banking institutions in the development of the national economy and its sustainable functioning.

ACKNOWLEDGMENT

This research is carried out within the framework of the scientific project "Model of the post-war development of credit institutions based on the artificial intelligence: customization of financial services and prudent supervision" with the support of the Ministry of Education and Science of Ukraine, state registration no. 0124u000810 (order no. 1569 dated 27.12.2023).

REFERENCES:

[1] The role of artificial intelligence in cyber security: predicting and preventing attacks. https://eba.com.ua/rol-shtuchnogo-intelektu-v-kiberbezpetsi-peredbachennya-ta-zapobigannya-atakam.

[2] Baker, Mohammed Bani, Sihwail, Rami, Mizher, Manar. (2023). Integrating cyber security factors with TAM framework for implementation in the Jordanian banks. Proceedings of the 4th International Computer Sciences and Informatics Conference (ICSIC 2022), volume 2979, issue 1, 040004. https://doi.org/10.1063/5.017472.

[3] Selimoğlu, Seval Kardeş, Saldı, Mustafa Hakan. (2023). Internal audit functions in cyber security governance: Turkey's bank sector cas. Glocal Polity and Strategies for Blockchain: Building Ecosystems and Sustainability, pp. 223-254. DOI: 10.4018/978-1-6684-4153-4.ch010.

[4] Vyhovska, N., Voronenko, I., Konovalenko, A., Dovgaliuk, V., Lytvynchuk, I. (2023). Cyber Security of the System of Electronic Payment of the National Bank of Ukraine. Economic Affairs (New Delhi), 68: 881-886. DOI: 10.46852/0424-2513.2s.2023.34.

[5] Kuttiyappan, Damodharan, Rajasekar V. (2023). A Novel Deep Learning-Based Identification of Credit Card Frauds in Banks for Cyber Security Applications. International

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Journal of Communication Networks and Information Security, 15(4): 1-10.

[6] Razavi, Hooman, Jamali, Mohammad Rezab, Emsaki, Morvaridsadat, Ahmadi, Alic, Hajiaghei-Keshteli, Mostafa. (2023). Quantifying the Financial Impact of Cyber Security Attacks on Banks: A Big Data Analytics Approach. Canadian Conference on Electrical and Computer Engineering, pp. 533-538. DOI: 10.1109/CCECE58730.2023.10288963.

[7] Zeijlemaker, S., Rouwette, E.A.J.A., Cunico, G., Armenia, S., von Kutzschenbach, M. (2022). Decision-Makers' Understanding of Cyber-Security's Systemic and Dynamic Complexity: Insights from a Board Game for Bank Managers. Systems, 10: 49. https://doi.org/10.3390/systems10020049.

[8] Alghamdi, Mohammed I. (2022). A Comprehensive Analysis of Cyber Security Protection Approaches for Financial Firms: A Case of Al Rajhi Bank, Saudi Arabia. Journal of Cybersecurity and Information Management, 9(1): 8-17. https://doi.org/10.54216/JCIM.090101.

[9] lacoviello, Giuseppina, Bruno, Elena, Cavallini, lacopo. (2021). Cyber security in the age of the Covid 19 pandemic: An empirical model to manage the risk in banks. 25th World Multi-Conference on Systemlcs, Cybernetics and Informatics, WMSCI2021, 1: 88-94.

[10] Putra, Adyan Pamungkas Ganefi, Humani, Figur, Zakiy, Faishal Wafiq, Shihab, Muhammad Rifki, Ranti, Benny. (2020). Maturity assessment of cyber security in the workforce management domain: A case study in bank Indonesia. 2020 International Conference on Information Technology Systems and Innovation, ICITSI 2020, pp. 89-94. DOI: 10.1109/ICITSI50517.2020.9264982.

[11] Alghazo, Jaafar M., Kazmi, Zafara, Latif, Ghazanfarb. (2017). Cyber security analysis of internet banking in emerging countries: User and bank perspectives. 4th IEEE International Conference on Engineering Technologies and Applied Sciences, ICETAS 2017, pp. 1-6. DOI: 10.1109/ICETAS.2017.8277910.

[12] Hrubliak O., Popelo O., Shaposhnykov K., Zhavoronok A., Ostrovska N., Krylov D. (2024). Digital currency of the central banks: trends of the euro area and prospects of the use within the implementation of the European green deal. Journal of Theoretical and Applied Information Technology, 102(7): 2954-2967.

[13] Dubyna, M., Popelo, O., Zhavoronok, A., Lopashchuk, I., & Fedyshyn, M. (2023). Development of the credit market of Ukraine under macroeconomic instability. Public and Municipal Finance, 12(1): 33-47. http://dx.doi.org/10.21511/pmf.12(1).2023.04.

[14] Tkachuk, I., Kobelia, M., Popelo, O., Zhavoronok, A., & Vinnychuk, O. (2023). Modelling financial influence of political and oligarchic interests of governed-sponsored enterprises on the creation and implementation of the financial policy in the state. Journal of Hygienic Engineering and Design, 42: 271-279.

[15] Alghadi, Mohammad Yousef, Alqudah, Hamzab, Lutfi,Abdalwali, Ananzeh, Husame, Marei, Ahmadf, Almaiah, Mohammed Amin, Al-Matari, Yahya Ali. (2024). Enhancing cyber governance in Islamic banks: The influence of artificial intelligence and the moderating effect of Covid-19 pandemic. International Journal of Data and Network Science, 8(1): 307-318. DOI:10.5267/j.ijdns.2023.9.023.

[16] Barış Armutcu, Ahmet Tan, Shirie Pui Shan Ho, Matthew Yau Choi Chow, Kimberly C. Gleason. (2024). The effect of bank artificial intelligence on consumer purchase intentions. Kybernetes. https://doi.org/10.1108/K-01-2024-0145.

[17] Tulchynska, S., Popelo, O., Solosich, O., Kasianova, N., Kostiunik, O., Shchepina, T. (2024). Artificial intellectualization in the assessment system of the safe development of economic entities. Journal of Theoretical and Applied Information Technology, 102(8): 3323-3334.

[18] Popelo, O., Tulchynska, S., Krasovska, G., Kistiunik, O., Raichava, L., Mykhalchenko, O. (2023). The impact of the national economy digitalization on the efficiency of the logistics activities management of the enterprise in the conditions of intensifying international competition. Journal of Theoretical and Applied Information Technology, 101(1):123-134. http://www.jatit.org/volumes/Vol101No1/11Vol101No1.pdf.

[19] Fanta, Nicolas, Horvath, Roman. (2024). Artificial intelligence and central bank communication: the case of the ECB. Applied Economics Letters.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

https://doi.org/10.1080/13504851.2024.2337318.

[20] Dreesbach, Michelle, Böhringer, Danielb, Kammrath Betancor, Paolac-d, Glegola, Mateusze, Maier, Philip Christian, Reinhard, Thomas, Heinzelmann, Sonjac. (2023). Quality control in the corneal bank with artificial intelligence: comparison of a new deep learning-based approach with conventional Endothelial Cell Counting by the 'Rhine-Tee Endothelial Analysis System'. Klinische Monatsblatter fur Augenheilkunde. DOI: 10.1055/a-2299-8117.

[21] Zhavoronok A., Shchur R., Zhezherun Y., Sadchykova I., Viadrova N., Tychkovska L. The Role of the Credit Services Market in Ensuring Stability of the Banking System. International Journal of Sustainable Development and Planning. 2022. Vol. 12, No. 6. pp. 667-679 https://doi.org/10.18280/ijsse.120602.

[22] Gupta, Mamta, Garg, Neh, Jain, Neetu, Saini, Pankaj, Roy, Sanjoy, Sati, Minakshi. (2024). Analysis of Financial Performance Pre and Post Use of Artificial Intelligence Applications Via CAMELS Lens: With Special Reference to HDFC Bank. Internationaljournal of Intelligent Systems and Applications In Engineering, 12(5s): 324-337. https://ijisae.org/index.php/IJISAE/article/view/3894

[23] Popelo, O., Tulchynska, S., Andriushchenko, O., Shepelenko, S., Falko, M., Shut, S. (2024). Blockchain technologies as a factor of the financial sustainability management of the enterprise and the e-commerce development. Journal of Theoretical and Applied Information Technology, 102(17), 6302-6316. https://www.jatit.org/volumes/Vol102No17/1Vol102No17.pdf.

[24] Rudenko, O., Mykhailovska, O., Kaplenko, H., Bazarko, I., Maksak, V. (2023). Global and Regional Threats to Human', Society', and State' Security. Economic Affairs (New Delhi), 68(4), pp. 2193–2206.