UDC 336
JEL Classification: G20; G21; G28

THE APPLICATION OF ARTIFICIAL INTELLIGENCE FOR THE PURPOSE OF COMBATING BANK FRAUD

©2023 CAPRIAN I.

UDC 336
JEL Classification: G20; G21; G28

Caprian I.

The Application of Artificial Intelligence for the Purpose of Combating Bank Fraud

Artificial intelligence (AI) is a technological (informational) complex designed to imitate human intelligence to perform tasks that previously required human input. AI has become an important component of the new economic and financial processes, with applications in various fields, including in the banking sphere. The purpose of this publication is to present the essence of AI through the lens of benefits and specific areas of the banking industry, including for combating bank fraud. For this, the author used the publications accessible in the form of analytical reports and expert views. Then a synthesis image was formed on the topic addressed and the related conclusions were formulated. The conducted study demonstrated the high potential of AI for promoting the innovative process on the banking market, raising the quality level of banking products based on deep knowledge of market trends, preferences and customer behavior. In the same way, AI has become an important applicable component within the banking institutions' divisions for management of placements and risks. AI has also become an important component in the activity of ensuring the cybersecurity of banks and the security of customers' banking operations, as well as combating bank fraud in different forms.

Keywords: *artificial intelligence, bank, customer fraud, fighting, protection.*

DOI: *https://doi.org/10.32983/2222-0712-2023-2-204-212*

Bibl.: *39.*

Caprian Iurie *– Postgraduate Student, State University of Moldova (60 Alexei Mateevici Str., Kishinev, MD-2009, Moldova)*

E-mail: *iuriecaprian@gmail.com*

ORCID: *https://orcid.org/0000-0001-5484-3087*

УДК 336
JEL Classification: G20; G21; G28

Капріан Ю. Застосування штучного інтелекту з метою протидії банківському шахрайству

Штучний інтелект (ШІ) – це технологічний (інформаційний) комплекс, призначений для імітації людського інтелекту з метою виконання завдань, які раніше вимагали участі людини. ШІ став важливою складовою нових економічних і фінансових процесів, знаходячи застосування в різних галузях, у тому числі в банківській сфері. Метою цієї публікації є висвітлення сутності ШІ через призму переваг і конкретних сфер застосування в банківській галузі, зокрема для боротьби з банківським шахрайством. Для цього автор використав доступні публікації у вигляді аналітичних звітів та експертних думок. На основі дослідження літератури сформовано синтетичну картину з досліджуваної теми та сформульовано відповідні висновки. Проведене дослідження продемонструвало високий потенціал ШІ для сприяння інноваційному процесу на банківському ринку, підвищення рівня якості банківських продуктів на основі поглибленого обізнання з ринковими тенденціями, уподобаннями та поведінкою клієнтів. Так само AI став важливим прикладним компонентом у підрозділах банківських установ з менеджменту ризиків та розміщення коштів. ШІ також став важливим компонентом у діяльності із забезпечення кібербезпеки банків і безпеки банківських операцій клієнтів, а також у боротьбі з банківським шахрайством у різних формах.

Ключові слова: *штучний інтелект, банк, клієнт, шахрайство, боротьба, захист.*

Бібл.: *39.*

Капріан Юрій *– аспірант, Державний університет Молдови (вул. Олексія Матеєвича, 60, Кишинів, MD-2009, Молдова)*

E-mail: *iuriecaprian@gmail.com*

ORCID: *https://orcid.org/0000-0001-5484-3087*

Introduction. Since the beginning of the 21st century, the global community has entered a new era, characterized by the development of the fourth industrial revolution (also called Industry 4.0 or 4IR), which is a consecutive phase in the digitization of the manufacturing sector, including the growth of data and connectivity, analytics, human-machine interaction, increased performance in robotics, automation and the application of advanced manufacturing technology [23].

This process accelerated in the mid-2010s and is considered to hold significant potential for future production and economic development in the future.

The basic features of 4IR are [23]:

- *Connectivity, data and computing power*: application of cloud technology, use of the Internet, blockchain technology and sensors;
- *Analysis and intelligence*: advanced analysis, machine learning, application of artificial intelligence;
- *Human-machine interaction*: the use of virtual reality (VR) and augmented reality (AR), the use of robotics and automation, autonomous guided vehicles;
- *Advanced engineering:* deployment of additive manufacturing (such as 3-D printing), use of renewable energy and nanoparticles.

The increasingly widespread application of digital technologies in economic processes, transactions, interactions and other activities has led to the emergence of the digital economy [7].

Such transformations are also taking place in the global banking industry, which can be examined both qualitatively and quantitatively.

In terms of quality, Bank 3.0 and Bank 4.0 models are being developed.

Banking 3.0 is a model of conducting banking activity, which combines the traditional activities of the 20th century with the wide development of self-service banking, the use of digital technologies and devices, as well as a new range of banking experiences, including through the personalization of banking services [25].

Bank 4.0 is a model for organizing banking activity, which entirely uses digital technology, without any form of physical contact with the bank's customers [1].

The implementation of the Banking 4.0 concept provides for the following important elements [25]:

- Applying data science to discover essential customer and operational data;
- Developing and implementing artificial intelligence models and promoting automation;
- Setting up banking services on the cloud;
- Fortifying the security of the cyber environment for customers and banks;
- Using blockchain technologies to secure data through decentralized identity and other privacy mechanisms.

On the other hand, there is a global expansion of the volume of banking activity, with presence of certain quantitative characteristics:

- In 2023, the global commercial banking market size is forecast to reach USD 2.8 trillion [18].
- In 2020, the total amount of loans offered by banks globally was USD 95 trillion [16].
- The number of global bank accounts is forecast to grow from 11.5 billion in 2021 to 13 billion in 2026 [17].
- The global value of digital payments in 2023 is forecast to be USD 9.5 trillion and by 2027 it may reach the level of USD 14.8 trillion [10].

At the same time, there is a qualitative and quantitative development of bank fraud.

According to the Association of Certified Fraud Examiners 2022 report, up to 5% of corporate revenue is lost to fraud each year, which is approximately USD 4.7 trillion globally [28].

A study by the United Nations Office on Drugs and Crime estimated that nearly 3.6 percent of global GDP is laundered each year [19].

The Nilson report projects card fraud losses at USD 32.3 billion in 2021, a 14% increase over 2020, when losses totaled USD 28.4 billion [24].

The expert Jimmy Fong found that every dollar of fraud costs US financial services USD 4.2 in legal, processing, investigation and recovery costs [14].

At the moment, it can be seen that the innovation process within commercial banks generates innovations in the field of bank fraud.

For example, Jimmy Fong notes that financial institutions and lenders reported that mobile fraud accounted for 32% of all fraud [14].

Another example worth mentioning is the study conducted by Nelda Biltauere, specifying the increase in popularity of the Buy Now Pay Later (BNPL) service. In the US four out of five consumers use BNPL for everything from clothing to cleaning supplies [5].

The criminal world responded with the Buy Now Pay Later Fraud (BNPL Fraud), exploiting weaknesses in the application process which essence is as follows: “Customers attempting to purchase goods or services using stolen identities and credit cards, with no intention of making repayments. These materialize in chargebacks and “Never Payment” defaults. [39]”

According to the Nelda Biltauere's payments expert forecasts, the BNPL will account for USD 680 Billion in global e-commerce transactions by 2025 [5].

At the current stage, artificial intelligence has become an important tool for preventing and combating bank fraud, which will be presented in this article.

Analysis of specialized literature. The specialized literature in the addressed field can be conventionally divided into two groups of sources. The first group consists of bibliographic sources directly dedicated to the assigned topic, and the second group includes literature with tangential approaches.

Thus, the topic of combating bank fraud with the help of Artificial Intelligence was addressed by the following authors:

- The expert Ronald Schmelzer's research has demonstrated the main benefits of implementing AI in banking.
- Courtney Lacomblez presented the basic ways to combat bank fraud with the help of artificial intelligence.
- Andrea Di Stefano examined the possibilities of using fraud detection and prevention systems based on machine learning.

As for the second group of literary sources, it contains a certain diversity of tangential approaches to the basic theme:

- The evolution of banking activity models can be found in the works of the authors Siddharth Pant, Abdillah Luthfi, Hussein Ananda Sabil, Ratnawati Kusuma;
- The trends in the evolution of bank fraud can be found in the works of the authors Jimmy Fong, Caitlin Mullen, Nelda Biltauere, Niall Whelan;
- The particularities of using Artificial Intelligence in banking were reflected by Joy Dumasia, Anjum Khurshid.

Also of particular interest are reports from the Federal Trade Commission, McKinsey&Company, NVIDIA and Allied Market Research.

Research methodology. The research was conducted in the form of an examination of recent bibliographic sources on trends in the development of banking activity and the evolution of bank fraud worldwide. Then the essence of Artificial Intelligence and the particularities of its application in the banking field were studied, including for the purpose of preventing and combating bank fraud. As a result, a complex picture of the synthesis of the discussed topic was obtained and the related conclusions were formulated.

Results.

The essence of artificial intelligence.

Artificial intelligence (AI) is the ability of information systems to perform certain functions, for the performance of which human intelligence is usually used [8].

The European Parliament proposes the following approach to AI: "AI is the ability of a machine to imitate human functions such as reasoning, learning, planning and creativity. AI allows technical systems to perceive the environment in which they operate, process this perception and solve problems, acting to achieve a certain goal. The computer receives the data (already prepared or collected through its own sensors, such as a video camera), processes it and reacts. AI systems are able to adapt their behavior to some extent by analyzing the effects of previous actions and operating autonomously [9]."

Likewise, this source presents two types of AI [9]:

- *Software*: virtual assistants, image analysis software, search engines, voice and facial recognition systems;
- *Embedded AI*: Robots, Autonomous Cars, Drones, Internet of Things.

The COVID-19 pandemic has become a fundamental factor for the adoption of AI in the corporate sphere.

The expert Joy Dumasia asseverates: "The adoption of AI in different enterprises has increased due to the COVID-19 pandemic. Since the pandemic hit the world, the potential value of AI has grown significantly. The focus of AI adoption is restricted to improving the efficiency of operations or the effectiveness of operations. However, AI is becoming increasingly important as organizations automate their day-to-day operations and understand the COVID-19 affected datasets. It can be leveraged to improve the stakeholder experience as well [12]."

The particularities of the application of artificial intelligence in commercial banks.

According to Joy Dumasia, AI enables banks to manage data at high speed and gain valuable insights. AI encompasses a complex of technologies including, but not limited to, machine learning, natural language processing, expert systems, vision, speech, planning, robotics, etc. [12].

Over the last two decades, AI has demonstrated the ability to transform business in the banking system on a global scale. One of the basic aspects of this process was to ensure the ability of banking institutions to provide the convenience of remote banking. The research conducted by Insider Intelligence showed that more than 45% of respondents considered mobile banking among the top three features that influence their selection of financial institutions [19].

Some experts consider AI as a tool for the continuous development of banking services. It has advanced data analytics potential to combat fraudulent transactions and improve compliance. AI also enables commercial banks to handle huge volumes of data at high speed in order to derive valuable insights from it. AI bots, digital payment advisors and biometric fraud detection mechanisms lead to a higher quality of customer service. As important results of the implementation of AI are enlarged revenues, reduced costs and increased profits [21].

Leveraging AI technologies gives banks the edge of digitization and helps them face direct and indirect competition. The results of the joint research carried out by the National Institute for Business Research and Narrative Science, have shown that approximately 32% of banks already use AI technologies such as Predictive Analytics, Voice Recognition and others [26].

The global AI banking market value was estimated at USD 3.9 billion in 2020 and is expected to reach USD 64.0 billion by 2030 [26].

Experts from McKinsey&Company are of the opinion that the potential for AI value creation for banks can be USD 1022.4 billion annually, of which USD 660.9 billion from AI and traditional analytics and USD 361.5 billion from advanced AI [6].

At present, commercial banks offer AI-integrated services and products to customers according to their preferences and needs. One of the most prominent features of AI in banking is its ability to learn. AI-based systems mature and become smarter over time. Thus, AI has become an important banking marketing tool, which allows performing complex data analyzes and adjusting marketing strategies, which consequently increases the efficiency of banking institutions' activity [19].

Benefits and problems of using artificial intelligence in commercial banks. Experts Ronald Schmelzer [27] and Anjum Khurshid [21] presented the following main benefits of implementing AI in banking:

1. *Prediction of future results and trends.* AI allows predicting future scenarios by analyzing past behaviors. Thus, AI helps banks predict future outcomes and trends. For example, it is about identifying fraud, detecting money laundering patterns and making recommendations to customers. AI is able to detect suspicious data patterns among huge volumes of data to identify fraud. Additionally, with its key recommendation engines, AI studies the past to predict future behavior in order to optimize cross-selling.
2. *Automation of cognitive processes.* AI enables the automation of many costly and error-prone banking services. Cognitive process automation solves a set of tasks, which take into account previous iterations through constant machine learning.
3. *Use of realistic interactive interfaces.* Chatbots identify context and emotions in the chat text and respond in the most appropriate way.
4. *Robotic process automation.* AI enables the automation of approximately 80% of repetitive work processes, allowing workers to focus on value-added operations that require a high level of human intervention.
5. *Reduction of operational costs and risk.* Many banks to date face significant operational cost and risk issues

due to human error. Simultaneously with the phasing out of handwriting, natural language processing and other AI technologies, robots are becoming intelligent tools to automate banking technology processes previously handled by humans.

6. *Improving the customer experience.* The implementation of AI eliminates customer dissatisfaction related to banks' work schedules, as well as long waiting for a response from call centers. Based on past interactions, AI enables a better understanding of customer needs and interests and their behavior. This enables the personalization of banking products and services, adding personalized features and intuitive interactions to provide meaningful customer engagement and contribute to customer loyalty.
7. *Improving fraud detection.* In the information age, related to the need to combat cyber fraud, which tends to increase and change permanently, AI has demonstrated the high capabilities of detecting financial fraud.
8. *Ensuring compliance with the regulations in force.* At the moment, banking regulations are very voluminous and sophisticated, and non-compliance has serious consequences for both the bank and its staff. At the moment, AI has the ability to analyze the content of banking legislation and determine compliance errors on the part of the banking institution, which facilitates the process of removing admitted violations.
9. *Effective decision making.* AI-based systems capable of thinking and responding like human experts provide solutions based on available real-time information. These systems store the information in the knowledge database. Bankers use these cognitive systems to make strategic decisions. For example, banks use AI-based systems to help drive lending decision-making. Some banks are applying AI in their smart systems to assist investment decision-making and support their investment banking research. AI-based systems are able to scour markets for untapped investment opportunities and inform their algorithmic trading systems. Many financial services companies also offer robo-advisors to help their clients with portfolio management.

Experts from McKinsey&Company mention the following advantages of using AI in commercial banks [6]:

- AI technologies can help increase revenue through increased personalization of customer (and employee) services;
- Contributing to cost minimization generated by greater automation, reduced error rates and better utilization of resources;
- Spotting new and previously unrealized opportunities based on an improved ability to process and generate insights from vast troves of data.

The use of AI has, at the same time, certain risks and disadvantages.

The expert Ronald Schmelzer is of the opinion that AI banking technologies, being developed very quickly, have a number of disadvantages and generate a number of risks [27]:

- *AI bias* can become an important risk, if in the process of designing and developing AI decision-making models the empowered people introduce their subjective views and wrong assumptions into the formation of the machine learning model.
- *Explainability and ethics.* Banking institutions in accordance with existing regulations are required to provide explanations for their decisions regarding the service requested by customers, which is difficult in the case of applying AI tools. The decision-making logic of the AI-based system may not be accessible to the average customer. That is, explanations to the client are mandatory, but it is a complicated task to explain how a certain decision of the bank was reached regarding his request. The lack of such explanations will most likely be treated as unethical behavior on the part of the bank by the client.
- *Customer distrust.* In the case of applying AI technologies, customer trust is very important. In the case of admitting operational errors, customers will lose their trust and refuse the bank's respective services.
- *Implementation costs.* Implementing AI-based banking innovations is expensive. There is often a lag between when the information product is developed and when it is implemented, simply because the process itself requires substantial financial efforts. Even mass-market AI products may prove too expensive to provide the necessary level of profitability.

Areas of application of artificial intelligence in commercial banks.

Joy Dumasia presented the following five applications of AI in banking [12]:

- *Chatbot* is a specific form of application of AI in the form of a computer program, which uses natural language processing to understand customer questions and provide automated responses, simulating human conversation [30]. Chatbots are efficient, providing cost savings. Chatbots in most cases are used for balance inquiry, accessing mini-statements, fund transfers, etc., which reduces the burden on other channels like contact centers, internet banking, etc.
- *Robo Advisor* is a digital platform designed to provide automated financial planning and investment services based on algorithms with minimal human supervision. Typically, a robo-advisor asks questions about the client's current financial situation, financial history, and future goals through an online survey. It then uses the data obtained to consult the client in order to make appropriate placements (investments) in certain financial instruments [15].
- *Predictive Analytics* is the process of using data to predict future outcomes. This process involves data analysis, machine learning, artificial intelligence, and statistical models to find patterns that could predict future behavior [37]. AI is able to detect specific patterns and correlations in data that could indicate untapped opportunities in market activity, leading to a positive impact on revenue.
- *Cybersecurity* is the totality of activities to protect systems, networks and programs against digital at-

tacks [32]. AI can improve cybersecurity by analyzing past threats and studying seemingly unrelated patterns and indicators to detect and prevent cyber threats. It's about preventing external threats, as well as monitoring internal dangers or breaches.

- *Credit Scoring* is a statistical analysis performed by banking institutions to determine the financial credibility of a customer [31]. AI is increasingly being used to assist the customer lending process by analyzing data from traditional and non-traditional sources. The application of AI makes the credit score applicable even for customers with a limited credit history.

Some informational sources link the use of IAC in the banking activity to the implementation of the following:

- *Edge to Cloud* refers to the fact that an economic entity's data is no longer confined to the data center, but is generated at the edge in significant quantities, processed and stored in the cloud, and used by a global workforce. A driving factor for today's edge-to-cloud approach is the growing need for real-time, data-driven decision making [34].
- *Internet of Things (IoT)* represent the network of physical objects – "things" – that are embedded with sensors, software and other technologies that provide connection and data exchange with other devices and systems via the Internet [35]. IoT allows physical locations to act more like online channels.
- *Self-service kiosks.* Global studies have shown that around 85% of scientists have used at least one self-service kiosk and are satisfied with the service [13]. The functionality of self-service kiosks is wider than that of traditional ATMs. Customers can not only withdraw cash, but also open accounts, make deposits, monitor investment portfolios, pay bills and more. They can perform all these tasks whenever it is convenient for them.
- *Interactive Teller Machines* are essentially "branch-in-a-box" systems that use a combination of touch screens and video technology to provide a virtual version of the banking experience [20]. It is the particular application of AI aimed at reducing waiting time and simplifying customer service.
- *Virtual avatars* – this is a non-verbal AI solution that improves the use of self-service kiosks by customers and enables the dimensioning of the customer experience.

The possibilities of using artificial intelligence in commercial banks for the purpose of combating bank fraud

The convergence of the banking sector with the IT, telecommunications and retail sectors has increased the transfer of critical information over virtual networks that are vulnerable to cyber-attacks and fraud. These incidents not only affect banks' profitability but also hamper banks' trust and customer relationship [21].

Hackers and scammers are constantly devising new ways to siphon off funds. Between 2020 and 2021, fraud losses reported to the Federal Trade Commission increased by more than 70% to a total of $5.8 billion. Banks, along with Fintechs and other financial institutions, are making every possible effort to anticipate the activity of fraudsters. AI is increasingly being used to prevent financial fraud. According to an NVIDIA survey, 10% of financial service providers said they used AI-based anti-fraud technology in 2021. By 2022, this figure has grown to 31%, tripling year-over-year [22].

AI helps banks fight fraud in several ways. In particular, AI can improve the ability to detect fraud in real time and reduce false positives, which increases accuracy and protects the customer's interests. Customers do not want to become victims of fraud, nor do they want to face the problems of closing accounts or refused transactions, including due to the assignment by the banking information system of a legitimate transaction as a fraudulent one [3].

In this context, the experts from SQN Banking Systems highlighted the benefits of applying AI to combat fraud:

- *Real-time detection* — AI can process large amounts of data at high speed. It can also compare the data to datasets about a user's normal behavioral patterns. It can then quickly determine anomalies in banking app usage, payments, and other transactions.
- *Accuracy* — AI reduces the risk of false positives. This means that it is less likely, compared to manual fraud detection or using rules-based anti-fraud software, to flag a legitimate transaction as fraudulent.
- *Machine learning* – AI never stops learning, which improves the fraud detection approach over time. When the system admits errors, the information system learns from its mistakes and improves its accuracy in the future.
- *Regulatory compliance* — Global statistics show that in 2021, banks incurred over $5 billion in regulatory fines related to data breaches. This is an important stimulus for the application of AI in fraud reduction activities.

Combating fraud in commercial banks through the application of AI is a multidimensional function.

First of all, it is about creating a protection within banking institutions of customer service, thus maintaining the high level of quality of banking products.

Second, it is important to insure commercial banks themselves against losses caused by bank fraud.

AI contributes to compliance with banking regulations, which are numerous. Some of them require banks to know their customers, respect customer privacy, monitor bank transfers, prevent money laundering and other fraud, and so on. For this, banks use intelligent AI-powered virtual assistants to monitor transactions, track customer behavior, and audit and record information in various compliance and regulatory systems [27].

Likewise, AI is meant to assist in cybersecurity and fraud detection [2].

Customers make many digital transactions every day to pay bills, withdraw money, deposit checks, etc., which are increasingly done through apps or online accounts. AI helps banks identify fraudulent activity, track gaps in their systems, minimize risk and improve the overall security of online finance.

As an example, the application of the deep learning tool within Danske Bank (Denmark) increased the ability to detect fraud by 50% and reduced counterfeiting by 60%. The AI-based fraud detection system also automated a lot of important decisions, while directing some cases to human analysts for further inspections [2].

A recent KPMG report states: "The anti-fraud engine can reduce fraudulent transactions by up to 40% on top of existing AI fraud prevention measures, for the benefit of banks, merchants and cardholders, as well as society in general [4]."

AI can help banks manage cyber threats. In 2019, the financial sector was the object of 29% of all cyber attacks. With the continuous monitoring capabilities of AI in financial services, banks can deal with potential cyber attacks before they affect employees, customers or internal systems.

Today's top performing banks use real-time AI-based risk management technologies to determine customer behaviors and transaction patterns to combat terrorist financing and money laundering. It monitors high-risk accounts by examining a customer's estimated turnover against their actual transactions for red flags. This helps banks carry out checks to protect against losses and fraud [19].

Fraud prevention using big data has already had a significant impact on credit card and lending processes. By examining customer behaviors and patterns, AI-based systems help banks practice proactive regulatory compliance while reducing overall risk [27].

Currently, many banks are limited to using credit scores, credit history, customer references and bank transactions to determine whether or not a person or company is creditworthy [27].

Ronald Schmelzer notes that credit reporting systems are far from perfect and are often riddled with errors, missing transaction history and misclassifying lenders. In addition to using available data, AI-based credit decision systems and machine learning algorithms can analyze behaviors and patterns to determine whether a customer with limited credit history might actually become a good customer for credit.

The expert Courtney Lacomblez presented five eloquent examples of the application of anti-fraud AI for banking and Fintech [22]:

1. *Machine Learning for Data-Driven Fraud Detection.* Machine learning-based fraud detection and prevention systems are based on Machine Learning algorithms that can be trained with historical data about past examples of fraud and autonomously understand the characteristic patterns of these events to recognize them once they are repeated. [11] As AI matures, the following technologies are used to prevent AI fraud:

- *Data mining* is the process of sorting through large data sets to identify patterns and relationships that can help solve business problems through data analysis. Data mining enables predicting future trends and making more competent business decisions [33]. It works like this: a computer system accumulates a huge set of data about consumer behavior (including fraudulent activity). When a transaction falls outside the pattern, the system flags it for review.
- *Machine learning* is a branch of AI and computer science that focuses on using data and algorithms to mimic the way humans learn, gradually improving their accuracy, where algorithms are continuously improving, ensuring accuracy over time [36].

By using data mining and machine learning in combination, fraud detection is always improving, and fraud detection is the first step to fraud prevention. Today's anti-fraud technology detects fraudulent transactions and stops them before they can be completed. Of course, from time to time, a legitimate transaction might run into a fraudulent one, and then reciprocal communication with customers is necessary.

2. *Push Notifications for Unusual Account Activity* is an alert system for unusual activity in the customer's account. An example would be if a fraudster has obtained the bank customer's debit card number and tries to buy something, either online or in person, using the customer's identity. Anti-fraud AI can detect this attempt and block the transaction. A notification can then be sent asking the customer if they are trying to make the transaction. If an error has been admitted, the customer can release the account. Today, many of these notifications arrive in the form of emails or text messages, but voice AI is currently on the rise.
3. *Conversational AI for Transaction Verification* enables an automated system to react to human speech in real time, creating dynamic and realistic conversations. This enables the achievement of two essential objectives for fraud detection. First, it helps consumers trust their voice bot. Second, it allows voters to collect the data their systems need to verify proper transactions and void fraudulent ones. Checking information with customers bridges the gap between aggressive fraud deterrence and consumer convenience, and with conversational AI these checks can be fully automated.
4. *Voice AI to Prevent Voice Phishing (or Vishing) Scams.* A classic phishing scam involves sending a fraudulent email to a recipient to trick them into clicking on a malicious link to divulge sensitive data. Vishing is similar to phishing, except that the scam is carried out via a voice call instead of email [29]. This form of fraud is a growing problem for banking institutions. In these voice phishing scams, fraudsters call bank customers, often using poor quality TTS voices to automate the attempt. No matter how they present themselves, they ask for personal information that they can use to remove account credentials. This is a challenge for banks because their systems are not involved in fraud and can control it. The key to preventing vishing is to give customers the power to authenticate the bank and its workers. An innovative way to achieve this goal is to present a unique, unmistakable voice for the bank's brand. They are also more likely to trust the bank's voice AI systems in use cases from fraud prevention to customer service.
5. *Voice Biometrics for User Authentication* is the science of using an individual's voice to authenticate them. This biological feature, along with

fingerprints, facial features and palm characteristics, is increasingly used to provide access to virtual and physical spaces [38].

Voice authentication is a new form of biometrics that can prevent identity theft in voice-based interactions between banks and consumers. Voice biometrics uses AI to identify a speaker's voice as theirs and theirs alone.

Conclusions. The current realities related to the expansion of banking activity on a global scale and its deepening in informational cybernetics require the use of artificial intelligence as a tool for solving a wide spectrum of banking problems. It is about promoting the innovative process on the market of banking products, raising the level of the quality of banking services, performing risk management, ensuring the security of banks' activities and their customers. The application of artificial intelligence promises efficiency, consumer satisfaction and improved profitability in banking. AI not only leads to the automation of technological processes in banks, but also makes this automation process intelligent enough to eliminate cyber risks. AI has become an integral part of bank processes and operations and continues to evolve and develop over time. AI will enable banks to optimally use human and machine capabilities to increase operational and cost efficiency and provide personalized services. By adapting AI, banking leaders have already taken due diligence actions to reap these benefits. As progress is made in these areas, there are constant changes in the field of bank fraud, which requires constant prevention and detection work. Data protection remains a challenge for banks. Implementing robust data protection protocols is necessary to counter such threats. The ability of AI to process massive amounts of data and the ability to learn self-learning allows the development and implementation of banking information systems capable of analyzing and predicting the behavior of customers and other representatives of environmental factors not only for the purpose of obtaining marketing advantages, but also to detect possible problems of various forms of banking placements, as well as to prevent various forms of bank fraud. The last aspect remains particularly important in order to ensure the operational, legal and financial security of the bank.

LITERATURE

1. Abdillah L., Abdillah L. Bank 4.0 experiential quality and its effect on word of mouth behavior, satisfaction and intentions. 2020. URL: https://www.researchgate.net/publication/343816886_BANK_40_EXPERIENTIAL_QUALITY_AND_ITS_EFFECT_ON_WORD_OF_MOUTH_BEHAVIOR_SATISFACTION_AND_INTENTIONS

2. AI in Banking – How Artificial Intelligence is Used in Banks. URL: https://appinventiv.com/blog/ai-in-banking/

3. Artificial Intelligence in Bank Fraud Detection and Prevention – SQN Banking Systems. URL: https://sqnbankingsystems.com/blog/artificial-intelligence-in-bank-fraud-detection-and-prevention/#:~:text=Benefits%20of%20Using%20AI%20to,and%20safeguards%20the%20customer%20experience

4. Artificial intelligence prevents fraud. URL: https://kpmg.com/dk/en/home/insights/2020/04/artificial-intelligence-prevents-fraud-.html

5. Biltauere N. BNPL fraud insight. URL: https://www.ravelin.com/blog/why-is-buy-now-pay-later-fraud-a-problem#:~:text=What%20does%20BNPL%20fraud%20look,abuse%2C%20and%20friendly%20fraud.%E2%80%9D

6. Suparna B., Brant C., Violet C., Shwaitang S., Renny T. AI-bank of the future: Can banks meet the AI challenge? URL: https://www.mckinsey.com/industries/financial-services/our-insights/ai-bank-of-the-future-can-banks-meet-the-ai-challenge

7. Ce este economia digitală? - definiție din techopedia. URL: https://ro.theastrologypage.com/digital-economy

8. Ce este inteligența artificială și ce rol joacă ea în viitorul copilului tău? URL: https://www.logiscool.com/ro/blog/ghid/inteligenta-artificiala

9. Ce este inteligența artificială și cum este utilizată? URL: https://www.europarl.europa.eu/news/ro/headlines/society/20200827STO85804/ce-este-inteligenta-artificiala-si-cum-este-utilizata

10. Digital Payments – Worldwide. URL: https://www.statista.com/outlook/dmo/fintech/digital-payments/worldwide

11. Di Stefano A. Machine learning for fraud detection: fighting crime with algorithms. URL: https://www.itransition.com/machine-learning/fraud-detection

12. Dumasia J. 5 applications of Artificial Intelligence in banking. URL: https://ibsintelligence.com/ibsi-news/5-applications-of-artificial-intelligence-in-banking/

13. Explore the Branch of the Future. URL: https://www.intel.com/content/www/us/en/financial-services-it/banking/branch-of-the-future.html

14. Fong J. Global Banking Fraud Index 2023. URL: https://seon.io/resources/global-banking-fraud-index/#h-costs-of-fraud

15. Frankenfield J. Robo-Advisor. URL: https://www.investopedia.com/terms/r/roboadvisor-roboadviser.asp#:~:text=Robo%2Dadvisors%20are%20digital%20platforms,based%20on%20modern%20portfolio%20theory

16. Global banking industry overview. URL: https://money-gate.com/global-banking-industry-overview/

17. Global Banking Trends in 2022. URL: https://www.reportlinker.com/clp/global/8830#:~:text=Global%20Banking%20Trends%20in%202022&text=The%20global%20number%20of%20bank,billion%20bank%20accounts%20in%202021

18. Global Commercial Banks – Market Size 2005–2029. URL: https://www.ibisworld.com/global/market-size/global-commercial-banks/

19. How artificial intelligence is changing the face of banking. URL: https://www.worldfinance.com/banking/how-artificial-intelligence-is-changing-the-face-of-banking

20. Interactive Teller Machine (ITM): Pros, Cons, & Future. URL: https://www.tidalcommerce.com/learn/interactive-teller-machines

21. Khursid A. Why banks need artificial intelligence. URL: https://www.wipro.com/business-process/why-banks-need-artificial-intelligence/

22. Lacomblez C. 5 Ways AI Prevents Fraud in Banking and Fintech. URL: https://www.readspeaker.com/blog/anti-fraud-ai/

23. MCKINSEY&COMPANY (2022) What are Industry 4.0, the Fourth Industrial Revolution, and 4IR? URL: https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-are-industry-4-0-the-fourth-industrial-revolution-and-4ir#:~:text=Industry%204.0%2C%20the%20Fourth%20Industrial%20Revolution%2C%20and%204IR%20all%20refer,transforming%20global%20business%20for%20years

24. Mullen C. Card industry's fraud-fighting efforts pay off: Nilson Report. URL: https://www.paymentsdive.com/news/card-industry-fraud-fighting-efforts-pay-off-nilson-report-credit-debit/639675/#:~:text=Card%20fraud%20losses%20globally%20amounted,over%20%2410.09%20billion%20in%202020

25. Pant S. Banking 4.0: where do humans stand in this new revolution? URL: https://bfsi.eletsonline.com/banking-4-0-where-do-humans-stand-in-this-new-revolution/

26. Pramod B., Shadaab K., Vineet K. AI in banking market. URL: https://www.alliedmarketresearch.com/ai-in-banking-market-A11871#:~:text=The%20global%20AI%20in%20banking,32.6%25%20from%202021%20to%202030

27. Schmelzer R. The top 5 benefits of AI in banking and finance. URL: https://www.techtarget.com/searchenterpriseai/feature/AI-in-banking-industry-brings-operational-improvements

28. The Top Banking Fraud Types to Watch in 2023. URL: https://www.netguardians.ch/the-top-banking-fraud-to-watch-in-202**3/**

29. Vishing vs. Phishing vs. Smishing: All You Need to Know. URL: https://www.mimecast.com/blog/vishing-vs-phishing-vs-smishing-all-you-need-to-know/#:~:text=A%20classic%20phishing%20scam%20involves,voice%20call%20instead%20of%20email

30. What is a chatbot? URL: https://www.ibm.com/topics/chatbots

31. What Is Credit Scoring? Purpose, Factors, and Role in Lending. URL: https://www.investopedia.com/terms/c/credit_scoring.asp#:~:text=Credit%20scoring%20is%20a%20statistical,to%20extend%20or%20deny%20credit

32. What Is Cybersecurity? URL: https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

33. What is data mining? URL: https://www.techtarget.com/searchbusinessanalytics/definition/data-mining#:~:text=Data%20mining%20is%20the%20process,make%20more%2Dinformed%20business%20decisions

34. What is Edge to Cloud? URL: https://www.hpe.com/us/en/what-is/edge-to-cloud.html

35. What is IoT? URL: https://www.oracle.com/internet-of-things/what-is-iot/#:~:text=The%20Internet%20of%20Things%20(IoT)%20describes%20the%20network%20of%20physical,and%20systems%20over%20the%20internet

36. What is machine learning? URL: https://www.ibm.com/topics/machine-learning#:~:text=the%20next%20step-,What%20is%20machine%20learning%3F,rich%20history%20with%20machine%20learning

37. What is predictive analytics? URL: https://cloud.google.com/learn/what-is-predictive-analytics#:~:text=Predictive%20analytics%20is%20the%20process,that%20might%20predict%20future%20behavior

38. What You Need to Know About Voice Biometrics. URL: https://www.aware.com/blog-what-you-need-to-know-about-voice-biometrics/

39. Whelan N. Fraud in the Buy Now Pay Later Industry. URL: https://ekata.com/blog/fraud-buy-now-pay-later/

REFERENCES

"AI in Banking - How Artificial Intelligence is Used in Banks". https://appinventiv.com/blog/ai-in-banking/

"Artificial Intelligence in Bank Fraud Detection and Prevention - SQN Banking Systems". https://sqnbankingsystems.com/blog/artificial-intelligence-in-bank-fraud-detection-and-prevention/#:~:text=Benefits%20of%20Using%20AI%20to,and%20safeguards%20the%20customer%20experience

"Artificial intelligence prevents fraud". https://kpmg.com/dk/en/home/insights/2020/04/artificial-intelligence-prevents-fraud-.html

Abdillah, L., and Abdillah, L. "Bank 4.0 experiential quality and its effect on word of mouth behavior, satisfaction and intentions". 2020. https://www.researchgate.net/publication/343816886_BANK_40_EXPERIENTIAL_QUALITY_AND_ITS_EFFECT_ON_WORD_OF_MOUTH_BEHAVIOR_SATISFACTION_AND_INTENTIONS

Biltauere, N. "BNPL fraud insight". https://www.ravelin.com/blog/why-is-buy-now-pay-later-fraud-a-problem#:~:text=What%20does%20BNPL%20fraud%20look,abuse%2C%20and%20friendly%20fraud.%E2%80%9D

"Ce este economia digitala? - definitie din techopedia". https://ro.theastrologypage.com/digital-economy

"Ce este inteligenta artificiala si ce rol joaca ea in viitorul copilului tau?" https://www.logiscool.com/ro/blog/ghid/inteligenta-artificiala

"Ce este inteligenta artificiala si cum este utilizata?" https://www.europarl.europa.eu/news/ro/headlines/society/20200827STO85804/ce-este-inteligenta-artificiala-si-cum-este-utilizata

"Digital Payments - Worldwide". https://www.statista.com/outlook/dmo/fintech/digital-payments/worldwide

Di Stefano, A. "Machine learning for fraud detection: fighting crime with algorithms". https://www.itransition.com/machine-learning/fraud-detection

Dumasia, J. "5 applications of Artificial Intelligence in banking". https://ibsintelligence.com/ibsi-news/5-applications-of-artificial-intelligence-in-banking/

"Explore the Branch of the Future". https://www.intel.com/content/www/us/en/financial-services-it/banking/branch-of-the-future.html

Fong, J. "Global Banking Fraud Index 2023". https://seon.io/resources/global-banking-fraud-index/#h-costs-of-fraud

Frankenfield, J. "Robo-Advisor". https://www.investopedia.com/terms/r/roboadvisor-roboadviser.asp#:~:text=Robo%2Dadvisors%20are%20digital%20platforms,based%20on%20modern%20portfolio%20theory

"Global banking industry overview". https://money-gate.com/global-banking-industry-overview/

"Global Banking Trends in 2022". https://www.reportlinker.com/clp/global/8830#:~:text=Global%20Banking%20Trends%20in%202022&text=The%20global%20number%20of%20bank,billion%20bank%20accounts%20in%202021

"Global Commercial Banks - Market Size 2005-2029". https://www.ibisworld.com/global/market-size/global-commercial-banks/

"How artificial intelligence is changing the face of banking". https://www.worldfinance.com/banking/how-artificial-intelligence-is-changing-the-face-of-banking

"Interactive Teller Machine (ITM): Pros, Cons, & Future". https://www.tidalcommerce.com/learn/interactive-teller-machines

Khursid, A. "Why banks need artificial intelligence". https://www.wipro.com/business-process/why-banks-need-artificial-intelligence/

Lacomblez, C. "5 Ways AI Prevents Fraud in Banking and Fintech". https://www.readspeaker.com/blog/anti-fraud-ai/

"MCKINSEY&COMPANY (2022) What are Industry 4.0, the Fourth Industrial Revolution, and 4IR?" https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-are-industry-4-0-the-fourth-industrial-revolution-and-4ir#:~:text=Industry%204.0%2C%20the%20Fourth%20Industrial%20Revolution%2C%20and%204IR%20all%20refer,transforming%20global%20business%20for%20years

Mullen, C. “Card industry's fraud-fighting efforts pay off: Nilson Report“. https://www.paymentsdive.com/news/card-industry-fraud-fighting-efforts-pay-off-nilson-report-credit-debit/639675/#:~:text=Card%20fraud%20losses%20globally%20amounted,over%20%2410.09%20billion%20in%202020

Pant, S. “Banking 4.0: where do humans stand in this new revolution?“ https://bfsi.eletsonline.com/banking-4-0-where-do-humans-stand-in-this-new-revolution/

Pramod, B., Shadaab, K., and Vineet, K. “AI in banking market“. https://www.alliedmarketresearch.com/ai-in-banking-market-A11871#:~:text=The%20global%20AI%20in%20banking,32.6%25%20from%202021%20to%202030

Schmelzer, R. “The top 5 benefits of AI in banking and finance“. https://www.techtarget.com/searchenterpriseai/feature/AI-in-banking-industry-brings-operational-improvements

Suparna, B. et al. “AI-bank of the future: Can banks meet the AI challenge?“ https://www.mckinsey.com/industries/financial-services/our-insights/ai-bank-of-the-future-can-banks-meet-the-ai-challenge

“The Top Banking Fraud Types to Watch in 2023“. https://www.netguardians.ch/the-top-banking-fraud-to-watch-in-2023/

“Vishing vs. Phishing vs. Smishing: All You Need to Know“. https://www.mimecast.com/blog/vishing-vs-phishing-vs-smishing-all-you-need-to-know/#:~:text=A%20classic%20phishing%20scam%20involves,voice%20call%20instead%20of%20email

“What is a chatbot?“ https://www.ibm.com/topics/chatbots

“What Is Credit Scoring? Purpose, Factors, and Role in Lending“. https://www.investopedia.com/terms/c/credit_scoring.asp#:~:text=Credit%20scoring%20is%20a%20statistical,to%20extend%20or%20deny%20credit

“What Is Cybersecurity?“ https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

“What is data mining?“ https://www.techtarget.com/searchbusinessanalytics/definition/data-mining#:~:text=Data%20mining%20is%20the%20process,make%20more%2Dinformed%20business%20decisions

“What is Edge to Cloud?“ https://www.hpe.com/us/en/what-is/edge-to-cloud.html

“What is IoT?“ https://www.oracle.com/internet-of-things/what-is-iot/#:~:text=The%20Internet%20of%20Things%20(IoT)%20describes%20the%20network%20of%20physical,and%20systems%20over%20the%20internet

“What is machine learning?“ https://www.ibm.com/topics/machine-learning#:~:text=the%20next%20step-,What%20is%20machine%20learning%3F,rich%20history%20with%20machine%20learning

“What is predictive analytics?“ https://cloud.google.com/learn/what-is-predictive-analytics#:~:text=Predictive%20analytics%20is%20the%20process,that%20might%20predict%20future%20behavior

“What You Need to Know About Voice Biometrics“. https://www.aware.com/blog-what-you-need-to-know-about-voice-biometrics/

Whelan, N. “Fraud in the Buy Now Pay Later Industry“. https://ekata.com/blog/fraud-buy-now-pay-later/

Стаття надійшла до редакції 18.05.2023 р.