УДК 338.49

THE USE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN THE BANKING SECTOR

D. Y. Vaishnur
Scientific supervisor: M. P. Mishkova, Candidate of Economics, Associate Professor
Brest State Technical University,
Republic of Belarus, Brest, Moskovskaya str., 267
arishakom@tut.by

This research paper explores the application of artificial intelligence (AI) technologies in the banking sector to improve operational efficiency and customer service. The author analyses key areas including ML, natural language processing and solutions based on neural network algorithms. Successful examples of AI implementation in various financial institutions such as HSBC and Sber are reviewed, emphasising their impact on credit scoring and fraud countermeasures. In addition, special attention is given to process automation using Robotic Process Automation (RPA), which can significantly reduce operational costs. The article also focuses on challenges related to data security and ethical aspects, confirming that proper AI implementation creates a more personalised customer experience and improves banks' competitiveness.

Keywords: artificial intelligence (AI), machine learning (ML), process automation, credit scoring, financial fraud, Robotic Process Automation (RPA), personalised customer experience.

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В БАНКОВСКОМ СЕКТОРЕ

Д. Ю. Вайшнур
Научный руководитель: М. П. Мишкова, к. э. н., доцент
Брестский государственный технический университет,
Республика Беларусь, г. Брест, ул. Московская, 267
arishakom@tut.by

В данной исследовательской работе рассматривается применение технологий искусственного интеллекта (ИИ) в банковском секторе для повышения операционной эффективности и обслуживания клиентов. Автор анализирует ключевые области, включая машинное обучение, обработку естественного языка и решения, основанные на алгоритмах нейронных сетей. Рассматриваются успешные примеры внедрения ИИ в различных финансовых институтах, таких как HSBC и Sber, с акцентом на их влияние на кредитный рейтинг и меры противодействия мошенничеству. Кроме того, особое внимание уделяется автоматизации процессов с использованием роботизированной системы управления процессами (RPA), которая может значительно снизить операционные расходы. В статье также рассматриваются проблемы, связанные с безопасностью данных и этическими аспектами, подтверждая, что правильное внедрение искусственного интеллекта создает более персонализированный клиентский опыт и повышает конкурентоспособность банков.

Ключевые слова: искусственный интеллект (ИИ), машинное обучение (ML), автоматизация процессов, кредитный рейтинг, финансовое мошенничество, роботизированная автоматизация процессов (RPA), персонализированный клиентский опыт.

The banking sector is one of the key sectors of any country's economy. Under conditions of phenomenal technological progress and fierce competition for customers, banks are striving to improve the quality of customer service and increase the efficiency of their operations. One of the promising areas for achieving the above goals is the use of AI technologies.

The term ‘artificial intelligence’ was coined by British mathematician and computer scientist Alan Turing in 1950. It was first used in a scientific article entitled ‘Computing Machinery and Intelligence’, the main question of which can be reflected as follows: ‘Can machines think?’ This simple question radically changed not only the world of technology, but also such fields as law, medicine, marketing and, in particular, the banking sector [1].

The continuous growth of data volumes and the need to quickly analyse bank information is forcing banks to look for new ways to increase the efficiency of their operations and improve customer experience. AI offers solutions that can significantly change approaches to managing risk, improving security and personalising services.

The objective of this study is to identify the key areas of application of AI in banks. In order to achieve this objective, several main objectives need to be addressed.

1. To review the current AI technologies used in the banking industry.
2. To analyse examples of successful implementation of AI in international practice.
3. To study the impact of AI on credit scoring and assessment of clients' solvency.
4. Examine the application of ML to counter fraud.
5. Evaluate the impact of automation of routine operations on banks' operating costs.
6. Identify the key barriers to the large-scale implementation of AI in financial institutions.

AI is transforming traditional processes and improving the customer experience. Key AI technologies used in banking include machine learning (ML), natural language processing (NLP), big data analytics and neural network algorithms.

ML algorithms can be used to assess creditworthiness, prevent fraudulent transactions, and personalise service offerings by analysing both structured and unstructured data, thereby improving the accuracy of assessments [2]. Natural Language Processing (NLP) technology underpins chatbots and virtual assistants that provide round-the-clock customer support, subsequently analysing dialogues and identifying weak areas in the bank's products. Through big data analytics, market trend forecasting, cross-selling and upselling, as well as assessing market conditions and risk management are carried out. Continuous preparation and training of models, identification of customers when making financial transactions in bank branches and using mobile applications have become possible with the help of neural network algorithms.

In the international arena, many banks are actively using AI. For example, JPMorgan Chase uses the COiN blockchain system to automate the analysis of legal documents, control of payment gateway transactions, and deposit accounts [3]. HSBC utilises the AI system developed in partnership with Ayasdi, this system detects suspicious activity when logging in and using the bank's products to improve payment security and operational efficiency, identifying potential fraudulent transactions, monitoring transactions for anti-money laundering and sanctions screening, countering bribery, insider trading and corruption [4]. In Russia, Sber introduced a facial recognition system back in 2020 to identify customers at its branches and in the online applications. In 2024, the system was improved to facilitate sales in other subsidiaries of Sber's ecosystem, such as SberMarket, MegaMarket, so that not only faces, but also each item in the video being viewed is recognised, with the ability to click and follow an active link to order a similar item on Sber's resources [5].

In the context of credit scoring, ML and AI algorithms are used to evaluate a customer's financial history, project NPVs, and behavioral patterns, using Wendell Smith segmentation criteria (geographic, demographic, psychographic and behavioural criteria) and publicly available information on social media profiles. To perform this operation, the model is first trained on historical data about customers who have received loans and paid them off, this way prediction errors are minimised and hidden patterns that prevent customers from guaranteeing repayment of loans are identified, some borrowers are rated as ‘risky’ but after detailed analysis they may turn out to be profitable and solvent. The model usually works as follows: after a test run on a limited cohort of users, the model is fully implemented on all bank customers, allowing banks to make more informed decisions.

JPMorgan Chase implemented similar model, which allowed the company to significantly reduce the level of loan defaults compared to traditional valuation methods. Pursuing the excellence, US startup ZestFinance applied neural network models to

assess the creditworthiness of customers without credit histories. The company's proprietary ZestAI model assesses borrowers using a risk rating that is 2–4 times more accurate than genAI-based models [6]. Thus, the use of ML models in credit scoring allows banks to lend to a responsible and solvent range of borrowers.

Fraud in the financial sector is ubiquitous problem, scammers are introducing more complex and insidious schemes each year. According to the FTC's 2023 report, U. S. consumers lost $300 million to fraudulent sms in 2022, a remarkable rise from $131 million in 2021 and $86 million in 2020. Thus, the average loss for individual victims doubled each year. Mock bank call scam is considered to be the most common type of fraud, where criminals impersonate a reputable financial service or bank by texting to confirm large purchases. By creating a false sense of urgency, the fraudster gets the victim to call a fake bank representative who gets their information [7].

To prevent fraudulent transactions and combat financial crime, banks are actively applying ML models, particularly classification algorithms such as logistic regression, decision trees and neural networks. These algorithms are trained on historical transaction data, where each transaction is labelled as either 'fraudulent' or 'legitimate'. The implementation of ML techniques assumed to avoid false positives and omissions, whilst a traditional system may block a legitimate transaction due to its unusual nature, resulting in customer inconvenience. In addition, traditional methods require continuous updating of rules, which is time and resource consuming [8]. Therefore, implementing ML to counter fraud has become an effective solution to protect customer data and funds while reducing operational costs.

The process of automating routine banking operations involves using robotic process automation (RPA), a technology that employs software robots to automate repetitive tasks. Its cost-effectiveness stems from the ability to integrate with existing systems without complete replacement. RPA automates tasks such as account opening, loan application processing, managing customer data and documentation, as well as handling data sets, executing transactions, and ensuring compliance.

Global practice shows that many banks have already successfully implemented RPA into their processes. For example, Bank of America uses RPA to perform monotonous tasks, automatically sift out irrelevant data, prioritise different cases, and perform predictive analytics. As a result, loan application processing time fell by 50 % [9]. Likewise, Deutsche Bank decreased the cost of routine tasks by 70 %, such cost optimisation across the national bank has allowed resources to be reallocated to more strategic areas [10]. In some cases, RPA can reduce operating costs by 25–60 % [11].

The growing role of chatbots and virtual assistants is also worth mentioning. The use of chatbots can reduce the waiting time for a response to a few seconds. Virtual assistants can perform more complex tasks such as managing accounts, providing financial advice and assisting with transactions. By integrating with AI systems, they can learn from customer interactions, allowing them to become increasingly efficient over time. According to estimates by Juniper Research, a UK-based fintech company, organisations' spending on gen AI-based chatbots is expected to increase by 1250 % over 4 years, i. e. from the beginning of 2024 to the end of 2028 [12].

While the use of AI in the banking sector offers new prospects, the accompanying opportunities also entail a number of challenges, such as ethical standards, high technology costs and legal compliance. Banks hold vast amounts of their customers' personal information, including financial data, transaction information and other sensitive

information. Therefore, making decisions based on data collected and processed by AI algorithms raises moral, ethical and legal issues, and the use of generative AI tools must be responsible and lawful [13]. The pitfall of AI decisions is that they can be motivated by racial discrimination, gender, ethnic bias or inconsistency with legislation. This is called a 'Pandora's Box' – situations where algorithms make decisions that are difficult to interpret [14]. Such actions directly harm both customers, who cannot fulfil the intended use of the bank's funds, and the bank's reputation. The problem is that ChatGPT, Gemini, Claude, Llama, etc. imply proprietary software and trained on unknown data sets, which may also be in closed access, i. e. there is a question of the legality of the use of intellectual property and copyright infringements. The scandal that erupted around the new Make Designs tool from the popular Figma design app in July 2024 is due to the fact that Figma's AI tool created designs extremely similar to Apple's Weather App. This proves that frequently even large but unspecialised companies in the technology sector are often absolved of responsibility for output results as they outsource the training of models on datasets. And even Figma CTO Kris Rasmussen said in an interview that he had no information about the training process of the new Make Designs tool, as Figma outsourced training to a third-party organisation. Andy Allen, CEO of Not Boring Software believes that such incidents should be prevented by thorough testing and modification of the results, otherwise both the company and the user could face lawsuits [15] and be burdened with the additional costs associated with reputational remediation activities.

However, the reason for user data leakage may also be due to the fact that small and medium-sized businesses store data in public cloud storage, additionally data are stored across multiple platforms, resulting in an average breach cost of $5,17 million. IBM states that organisations adopting AI save around of $2,22 million [16].

Meanwhile, existing banking systems may not be compatible with new technology solutions, requiring replacement of current equipment, building up technical capacity, retraining specialists or finding new qualified ones to implement and monitor such transitions.

Solutions may include engaging compliance professionals such as data protection, privacy and legal specialists within your organisation at the start of your journey, as well as seeking legal advice on intellectual property equality, fairness and data protection issues in your use of generative AI [13]. And also state support, implementation control and legislative regulation of the technology industry, which implies the need to pass inspections and obtain authorisations for the use of certain data and technologies in order to receive reduced tax rates. But even this solution is not perfect, as it entails bureaucratic hindrance of innovation and complication of business processes. Successful implementation of technology requires careful attention to safety and ethical issues. And the right implementation of AI can significantly increase the efficiency of banking operations and improve customer experience.

According to reports prepared by consulting firms McKinsey and Deloitte, in 2024, 70 % of banks have been using AI on a large scale to optimise their operations and improve customer service. Centralised management based on AI allows enterprises to focus human resources on solving more complex problems related to production and scaling. Globally, according to a McKinsey Institute (MGI) study, genAI could save the industry between $200 billion and $340 billion, or 2,8–4,7 % of total revenue, mainly by improving productivity and minimising errors [17]. This frees up resources for staff to focus on strategical goals, cross-sector connectivity and scaling [18].

The review of modern AI technologies has demonstrated their diversity and potential for optimising banking processes. The author highlighted successful examples of AI implementation in international practice, which serve as evidence that AI is an effective tool in improving the quality of customer service and reducing operational risks.

Analysing the impact of AI on credit scoring and customer solvency assessment has shown that modern algorithms can significantly improve the accuracy of forecasts, which in turn contributes to more informed lending decisions. [19] The introduction of ML to counter fraud has opened new horizons in the fight against financial crime, allowing banks to respond quickly to suspicious activities.

In addition, RPA, chatbots and virtual assistants had a positive impact on operating costs, allowing banks to redirect resources to more strategic tasks. Thus, our results support the hypothesis that the use of AI in banking not only enhances customer service but also reduces credit and fraud risks.

Thus, this study emphasises the importance and relevance of applying AI in the banking sector to improve operational efficiency and customer satisfaction.

List of sources used

1. Turing, A. M. Computing machinery and intelligence / A. M. Turing // Mind. – 1950. – Vol. LIX. – Iss. 236. – P. 433–460.

2. Hassani, H. Deep Learning and Implementations in Banking / H. Hassani, X. Huang, E. Silva, // Annals of Data Science. – 2020. – Vol. 7. – P. 433–446.

3. JPM Coin System // J. P. Morgan Payments. – URL: https://developer.payments.jpmorgan.com/-docs/treasury/global-payments/capabilities/jpm-coin-system (access of date: 13.10.2024).

4. Here's How HSBC is Using Artificial Intelligence to Take Money Launderers to the Cleaners // Future Digital Finance Connect. – URL: https://futuredigitalfinance.wbresearch.com/blog/hsbc-artificial-intelligence-strategy-to-beat-money-launderers (access of date: 13.10.2024).

5. Как работает система распознавания лиц // Developers Sber. URL: https://developers.sber.ru/-help/smartface/how-work-face-recognition (дата обращения: 13.10.2024).

6. AI-Automated Underwriting // ZestAI. – URL: https://www.zest.ai/product/underwriting/ (access of date: 13.10.2024).

7. Louis Thompsett How AI can protect against bank fraud scams // FinTech Magazine. – 2023. – Vol. 20. – P. 26–30. – URL: https://fintechmagazine.com/articles/how-ai-can-protect-against-bank-fraud-scams (access of date: 15.10.2024).

8. Stephan Dreiseitla Classification models. / Stephan Dreiseitla, Lucila Ohno-Machado. – URL: https://www.sciencedirect.com/science/article/ pii/S1532046403000340 (access of date: 15.10.20240.

9. Case study on Bank of America: How robots help serve and protect the bank // FinTech Futures. – URL: https://www.fintechfutures.com/2019/11/case-study-on-bank-of-america-how-robots-help-serve-and-protect-the-bank/ (access of date: 15.10.2024).

10. Villar, Alice Robotic process automation in banking industry: a case study on Deutsche Bank / Alice Villar, Nawaz Khan // Journal of Banking and Financial Technology. – URL: https://www.sciencegate.app/source/327697 (access of date: 15.10.2024).

11. RPA in the banking industry: the expert guide // MaximaConsulting. – URL: https://www.maximaconsulting.com/newsroom/rpa-in-banking-expert-guide – (access of date: 23.10.2024).

12. Generative AI Spend on Mobile Messaging to Reach $11bn Globally by 2028 // Juniper Research]. – URL: https://www.juniperresearch.com/press/ pressreleasesgenerative-ai-spend-on-mobile-messaging-to-reach-11bn-globally-by-2028 (access of date: 23.10.2024).

13. Generative AI Framework for HMG (HTML) of the UK Government // The Government of the UK. – URL: https://www.gov.uk/government/publications/generative-ai-framework-for-hmg/generative-ai-framework-for-hmg-html (access of date: 25.10.2024).

14. A governance framework for algorithmic accountability and transparency // European Union Website. – URL: https://www.europarl.europa.eu/RegData/etudes/ STUD/2019/624262/-EPRS_STU (2019) 624262EN.pdf (access of date: 25.10.2024).

15. Jay Peters Figma pulls AI tool after criticism that it ripped off Apple's design // The Verge. – URL: https://www.theverge.com/2024/7/2/24190823/figma-ai-tool-apple-weather-app-copy (access of date: 25.10.2024).

16. Cost of a Data Breach Report 2024 // IBM. – URL: https://www.ibm.com/reports/data-breach (access of date: 25.10.2024).

17. Scaling genAI in banking // McKinsey. – URL: https://www.mckinsey.com/industries/-financial-services/our-insights/scaling-gen-ai-in-banking-choosing-the-best-operating-model (access of date: 25.10.2024).

18. Mishkova M. P. Klassifikaciya riskov intellektualnoj deyatelnosti / M. P. Mishkova, E. E. Ermakova // Vestnik BrGTU seryya Ekonomika. – 2024. – № 1 (131). – S. 194–197.

19. Mishkova, M. P. Problemy razvitiya informacionnyh tehnologij na sovremennom ekonomicheskom etape / M. P. Mishkova // Innovacii: ot teorii k praktike : sb. nauch. st. IX Mezh-dunar. nauch.-prak. konf., Brest, 19–20 okt. 2023 g. : v 2 ch. / Brest. gos. tehn. un-t. – Brest, 2023. – Ch. 2. – C. 44–48.