DOI https://doi.org/10.30525/2661-5150/2025-2-4

AI AND BANK'S OPERATIONAL RISK MANAGEMENT

Dmytro Bezshtanko[1]

Abstract. In modern conditions, the use of AI is an advantage for business. This allows you to free up additional human resources and direct them to other tasks, speed up operations, and move to new areas of development. At the same time, the use of AI leads to an increase in risks, cyber threats, costs, and the possibilities of minimizing risk using AI determine the relevance of this study. In this scientific work, the subject of research is the process of applying and using AI in the banking business and in the banking risk management. The topics specified for the study were applied standard scientific methods of analysis, synthesis, deduction, and induction, it is possible to determine the directions of using AI in the banking sector and identify the possibilities of using AI together with risk management tools. The main goal of the research is to identify the advantages and threats of using AI in the banking sector. Taking into account the clear regulation of banks' activities, the paper highlights risk management tools: creation and maintenance of a database of internal and external operational risk events, key operational risk indicators, operational risk self-assessment, scenario analysis, mathematical modelling, analysis of process maps, comparative analysis. Today, almost all bank operations can be performed based on AI or systems that use it. Examples of where such tools are used include financial monitoring, active or treasury operations, securitization, Chat-bots and social networks, remote identification and office management. At the same time, AI systems are also used to control the risks arising in these processes: for process control and risk management. Each of the above risk management tools can be based on AI systems, which opens up significant opportunities for control, risk minimization and the release of human resources. However, one should not forget about potential threats that can worsen the quality of risk management: lack of specialists, data fragmentation in banks, validation problems, the cost of connecting AI, imperfection of existing models, and the possibility of data loss. In conclusion, it is worth noting that the use of artificial intelligence, along with significant advantages for banks, generates numerous risks that can be minimized with the use of the same artificial intelligence. This situation indicates a transition to a new stage of banking risk management – the stage of cooperation with artificial intelligence.

Keywords: operational risk, AI in risks, risk management.

JEL Classification: E58, G21

1. Introduction

Modern trends in the development of the IT industry involve the active use of AI elements. The banking sector, joining global trends, is interested in expanding the use of AI in its activities: attracting customers, accelerating the processing of customer requests and finding individual offers for customers, etc. At the same time, along with new development opportunities, new threats and risks arise, and old vulnerabilities are intensified, which determines the relevance of this study.

Various aspects of the application of AI in banking are devoted to the work of Ukrainian scientists and scholars, such as: Azmuk N., Baryshevska I., Batayesva A., Bey G., Dumanska A., Zayonts A., Irnazarov D., Prytsyuk, L., Puzyrova P., Polishchuk, Yu., Sogunyako D., Solodkyi V., Shishkina O. and others. At the same time, a number of issues regarding the involvement of AI in risk management, the use of controls based on AI in banking, potential benefits, threats and losses from such cooperation between a bank employee and AI are not covered in scientific publications, which determined the choice of the topic of this study.

This work is based on the use of various scientific methods. The deduction method identified the main areas of use of AI in banks, and the statistical analysis method was used to assess the level of influence of AI on the activities of banking institutions. The author to analyze Ukrainian legislation and its impact on

[1] Joint Stock Company "KREDOBANK", Ukraine
E-mail: Homozavr@meta.ua
ORCID: https://orcid.org/0000-0002-0344-5828

building a risk management system using AI used the induction method. The analysis method was applied in studying threats and obstacles from the introduction of AI into the bank's activities, including in the context of operational risk management, an analysis of the possibility of including AI in operational risk control tools was also conducted, and recommendations and proposals, based on the results of the study, were formed using the synthesis method.

2. The Role of AI in Modern Banking

It is worth starting with an analysis of the essence of operational risk, and taking into account the regulatory order of the banking sector, there is an unambiguous interpretation of this concept used by banks. Thus, according to the Resolution of the National Bank No. 64 of 2018, which regulates the main issues of risk management in the banking sector, the essence of operational risk is clearly defined. It interpreted as the probability of losses or additional losses or failure to receive planned income due to shortcomings or errors in the organization of internal processes, intentional or unintentional actions of bank employees or other persons, failures in the operation of bank systems or due to the influence of external factors. Operational risk includes legal risk, but should exclude reputational risk and strategic risk (National Bank of Ukraine, 2018).

It should be noted that the bank's operational risk includes information and communication technology risk and information security risk (National Bank of Ukraine, 2023):

– Information security risk – the probability of losses or additional losses, or failure to receive planned income due to a violation of the confidentiality, integrity, or availability of data in the bank's information systems, shortcomings or errors in the organization of internal processes, or the occurrence of external events, including cyberattacks or inadequate physical security. Information security risk includes cyber risk;
– Information and communication technology risk – the probability of losses or additional losses or failure to receive planned income due to malfunction or non-compliance of information and communication technologies with the business needs of the bank, which may lead to disruption of their sustainable functioning, or shortcomings in the organization of management of such technologies

It should be emphasized that in Resolution No. 64 of the National Bank of Ukraine dated June 11, 2018, several sections are devoted to the issue of operational risk management and the implementation of relevant control measures. As for the tools, the regulator has clearly defined mandatory and auxiliary risk management tools. According to Article 291 of the above-mentioned resolution (National Bank of Ukraine, 2018), mandatory tools include:

– Analysis of the results of inspections carried out by the internal audit unit and the external auditor;
– Creation and maintenance of a database of internal operational risk events and analysis of the information accumulated in it;
– Key operational risk indicators, which are quantitative indicators that change over time and reflect changes in the nature of operational risk. KRI is used by the bank for early detection of negative trends/ phenomena associated with increased operational risk inherent in processes;
– Self-assessment of operational risk in products, processes and IT services;
– Scenario analysis is applied by forming judgments by employees of the risk management unit and first line of defense units regarding the identification of possible unlikely operational risk events with significant consequences for the bank and their quantitative assessment.

In addition, according to Article 292 of the aforementioned resolution, as additional operational risk management tools, banks may apply:

– Creation and maintenance of a database of external operational risk events and analysis of the information accumulated in it;
– Measurement, as a mathematical model for assessing possible losses from operational risk based on statistical data on operational risk events;
– Analysis of process maps in order to identify process stages, types of activities and organizational functions, as well as operational risks inherent in processes;
– Comparative analysis by comparing the results of applying different tools in order to objectively assess (measure) the bank's operational risk.

According to the above-mentioned resolution of the National Bank, namely Article 21, banking institutions do not have the right to outsource the risk management function. At the same time, there is no ban on using external information to build scenarios, stress tests or use it as a basis for other risk management tools. It is also worth noting that according to Article 292, a bank may form a database of external operational risk events and use such information for its own risk management purposes (National Bank of Ukraine, 2018). Therefore, a bank may not outsource risk management, but may use external information for its own tools.

Guided by the above approach, even before the COVID-19 pandemic, banks were actively implementing AI tools. The Ukrainian banking sector is also gradually entering this wave, which opens up both new opportunities for risk management and new challenges. Thus, in 2023, more than 15% of losses of financial institutions in the EU were associated with

operational risks (according to the European Banking Authority) (European Banking Authority, 2024).

Returning to the use of AI in the banking sector, the following areas should be noted:

– Machine learning for building risk models, detecting anomalies;
– Natural language processing analysis of customer complaints, email communications;
– Computer vision for document recognition, signatures;
– Robotic automation of processes for processing typical transactions, scoring.

Each of the above areas has already been implemented by banks, including Ukrainian ones (in one form or another) using the so-called elements of AI – high-tech processes with an extremely complex architecture and algorithms.

For example, financial monitoring units have carried out the assessment of customer banking transactions, their history and dynamics since the beginning of 2010, including using complex algorithms. Numerous cases of fines imposed by the regulator for violations of financial monitoring only confirmed the need to involve elements, and later AI systems, since: manual processing is not effective, the number of transactions increases with the increase in products and the expansion of the client base, the development of so-called "optimization schemes" – methods of money laundering, etc.

The next example of the application of AI in Ukrainian banking can be Chat Bots in social networks and on the official pages of banks. Such assistants have algorithms developed by programmers and business units to help clients without involving bank employees. Over time, sound assistants began to appear that voiced scenarios and required clients to indicate further steps. Their functioning was based on AI language models.

Remote identification of clients is another relevant banking tool; it helps to refuse to involve Bank employees in identification processes. Ukrainian banks have a high level of digital adaptation: more than 80% of transactions are carried out online by customers, which creates a high-quality data set for AI training (National Bank of Ukraine, 2023).

In the context of security, AI is extremely relevant, as it allows you to identify opportunities for fraud and penetration into the periphery of banking protection, bottlenecks, Deep Fake, etc.

As for treasury operations, AI has significant capabilities and helps in choosing a way to fill a financial investment portfolio, in trading, in searching for insider information, identifying trends, etc.

An important application of operational risk is text recognition and transcription of conversations, which allows you to speed up the preparation of information, products or services, forms archives of conversations and determines the needs and interests of customers.

The most important, in our opinion, is the use of AI to analyze the databases of a banking institution in order to:

– Train AI in the characteristics of a particular banking institution;
– Develop new products;
– Form individual offers;
– Detection of potential fraud;
– Reporting;
– Assistance in individual communication with the client, etc.

The use of AI has two approaches: development of its own systems and use of those offered by the market. Both approaches have both positive and negative manifestations, and depend on the financial, technical, and organizational capabilities of the bank. In our opinion, the most active use of AI elements is by Privatbank, Universal Bank (through its Monobank product), FUIB, OTR and others.

When using AI, a number of issues arise, that must be resolved before implementation: certification and licensing, analysis of costs and revenues from implementation, market research for services, responsibility and deadlines. The banking institution must formulate conclusions and present results on all these issues. Thus, the process from idea to implementation can last from several months to several years.

The regulator or other authorities can accelerate the implementation process through regulatory regulation, development of new products for the banking sector, etc. An example of such an incentive is the Experimental Project on Providing State Monetary Assistance to Buyers of Ukrainian-Made Goods and Services within the Framework of the All-Ukrainian Economic Platform "Made in Ukraine" (Cabinet of Ministers of Ukraine, 2024). This project involves a large number of automated operations with fuzzy parameters, which can best be implemented by systems with elements of AI.

Banking institutions are interested in implementing AI, given the significant advantages:

– Forecasting: AI models are able to predict process failures with an accuracy of up to 85–90% based on historical data;
– Speed of response: AI operates 24/7, responding instantly;
– Cost reduction: According to Deloitte, banks that have implemented AI in the area of risk management have reduced related costs by 15–25% on average (Deloitte, 2023);
– Scalability: AI systems are easily scalable without the need for additional staff.

Overall, according to Statista, global bank investments in AI exceeded US$30 billion in 2022, with a forecast

for 2025 of US$64 billion (Statista, 2023). In Ukraine, according to USAID Financial Sector Reform estimates, AI is used in about 30% of large banks, mainly in the front office (USAID Financial Sector Reform Project, 2023), but is gradually being introduced in risk management.

3. AI in Operational Risk Management

Considering the above regulatory features, the application of AI elements in operational risk management can be divided into 2 large arrays:

– Controls using AI elements;
– Risk management tools using AI.

The essence of controls is to prevent the realization of risks inherent in a specific type of banking activity (for example: corporate business, online banking, property management, cyber security etc.) using organizational, technical, software, and regulatory tools.

Thus, the use of AI allows you to analyze large arrays of internal and external data: log files, calls to contact centers, changes in personnel behavior, which allows you to identify potential risks earlier. Example: in 2022, one of the systemic banks in Poland reduced incidents related to human errors by 18%, thanks to an AI system that predicts "vulnerable" changes in operations (Komisja Nadzoru Finansowego, 2023).

After analysis, the same AI, establishing a list of bottlenecks, can determine the minimum or optimal list of controls to ensure the smooth, optimal and efficient operation of processes and systems. It should be noted that it is not the bank employee, but the AI system that forms the controls. A person, in the person of a bank specialist, should approve/reject the control and submit the issue to the collegial body for consideration. In addition, the ability of AI systems to form appropriate proposals and submit calculations, and develop a presentation is important.

Behavioral management theory assumes that human behavior is patterned, and therefore, AI can become an assistant in controlling unauthorized personnel activities. Thus, AI models allow detecting anomalous activity in real time. For example, EU banks are implementing systems that monitor changes in the work style of individual departments, identifying signs of potential internal fraud.

Applying this to Ukrainian realities, according to unofficial market estimates, up to 10% of operational risk incidents are associated with the human factor, and this share is potentially reduced through appropriate monitoring (ICU Research & USAID, 2023). Since viewing a video by a security officer takes a lot of time and marker situations can be missed, AI is best suited for this area of the Bank's activity.

Monitoring and auditing of Bank operations, as already noted, is best suited for the implementation of appropriate systems with elements of AI. Control, financial monitoring, security, controlling and audit departments will be able to detect, within their powers, suspicious, threatening, erroneous transactions and take steps to minimize risks. In addition, a positive side of such implementation may be the reduction of personnel whose activities were aimed at routine operations. This can be confirmed by the fact that McKinsey estimates that automation reduces internal audit costs by an average of 20–30% (McKinsey & Company, 2022).

The next set of questions regarding the implementation of AI systems for managing operational risk concerns the tools for such management. In our opinion, it is worth focusing on only some of the tools.

1. Creation and maintenance of a database of operational risk events. Given that, employees, including risk coordinators, register such events there is a high probability of absence, distortion or incorrect registration of operational risk events. Building a registration process based on the above controls with the subsequent determination of responsible persons in the person of the heads of structural units will allow:

– Promptly and qualitatively filling, analyze the risk event database;
– identify bottlenecks in processes and products;
– be able to respond to identified problems quickly, etc.

2. Key indicators of operational risk. Their development and analysis of values is slowed down due to the potential reluctance of structural units to receive additional controls, generate regular reports, and be responsible for possible errors, inaccuracies, failures.

At the same time, the use of AI systems when building key indicators will allow:

– Develop new indicators and not only analog, but also synthetic ones;
– Carry out monitoring not only on a monthly basis (as required by the above resolution of the National Bank), but also more promptly;
– Involve less bank specialists in monitoring, which will increase the objectivity of the data;
– Monitor the results of risk minimization measures.

3. Self-assessment of operational risk of processes, products, IT services. This process requires significant resources from business units, control units and IT. The process is still long in time and poorly correlated with significant changes in the Bank's activities or external factors. Self-assessment of operational risk of the lending process, carried out annually (as required by the above-mentioned resolution of the National Bank), may not take into account numerous changes in the legislation of Ukraine, changes of a political or socio-economic nature. This happens because the effect of such changes is remote from the moment of issuing a loan, but in fact, risks arise immediately after the specified changes.

The use of AI elements in terms of identifying relevant threats, violations, changes in the organizational structure or procedures of the bank will allow to speed up self-assessment, take into account more factors and determine the level of risk taking into account control and audit measures.

4. Scenario analysis and stress testing. Scenarios for identifying threats, reactions of units to risk factors, potential losses from risk realization, etc. can be generated with sufficient quality by AI systems that have already been trained on bank processes. Losses, opportunities and potential from scenarios, taking into account the multifactorial nature of models, can be generated faster based on a larger set of data and record the problem areas for a banking institution. In general, this toolkit, in our opinion, is best suited for the application of AI

5. The external event database, as an operational risk tool, is best used in conjunction with AI search engines. Parsing as such has been used by leading Ukrainian banks for quite some time, but it is AI that can superimpose on the bank's functioning model. This tool is an auxiliary tool for analyzing the operational risk event database, scenario analysis and stress testing, and risk self-assessment.

It is worth emphasizing that only a few of the mandatory operational risk control tools are listed. In fact, banks use a much wider range of risk management tools: from capital management elements to the use of training attendance indicators.

However, there are a number of threats and risks related to the implementation of such tools:

– Lack of analytics and data science specialists;
– Fragmentation of data in banks, especially in old IT infrastructures;
– Problems with validating AI models;
– The cost of connecting/developing/engaging AI;
– Reluctance of risk management units to change existing processes;
– Fears of AI;
– Imperfections of existing AI models;
– The possibility of data loss (personal, confidential, bank secrecy), etc.

These threats can be reduced through additional training, enhanced security measures, involvement of third-party specialists, even the simple will of the bank's management. However, these are additional costs, and in the context of the unstable socio-economic situation in the country and military threats, these costs may be recognized as inexpedient.

Discussion. The question of the scope of AI involvement in the risk management system remains unresolved: whether it is possible to replace the risk manager with AI or not. In addition, the issue for discussion is the issue of information security when involving AI; in fact, sensitive information can go beyond the security perimeters, and therefore – the loss of control over the data. The willingness of the bank to develop AI on its own data also generates new risks: incorrect interpretation of information, redundant data for specialists, etc.

4. Conclusion

Artificial intelligence and the systems that use it are not just a trend, but also a real tool used by banks to improve business efficiency, additional controls, and risk reduction. Ukrainian legislation has not defined the role and place of artificial intelligence, but it clearly identifies the risk management system and regulates the bank's activities in all its aspects.

The use of artificial intelligence, being an auxiliary tool, provides significant benefits to banks: it stimulates the development of the client base, allows for the formation of new, improved, client-oriented products, and helps speed up business decisions.

For example, the use of artificial intelligence speeds up the quality of forecasts by 85-90%, reduces costs, including personnel costs – up to 25%, and allows a significant number of banking services to work around the clock – without the involvement of live specialists

At the same time, new threats are emerging that the bank is obliged to minimize and manage. For this purpose, an operational risk management system is used, and this article attempts to describe the possibilities of applying artificial intelligence to risk management tools.

Thus, the creation of a database of operational risk events (external and internal), when using artificial intelligence, allows you to respond to risks as quickly as possible, key risk indicators identify bottlenecks and reduce the cost of human resources for rapid response and management.

Risk self-assessment with the involvement of artificial intelligence allows you to eliminate the maximum number of factors affecting the business and their role in minimization and control models.

Scenario analysis and stress testing allow you to create the most objective models with minimal assumptions.

However, a number of threats, subjective fears and misunderstanding of the work of artificial intelligence create obstacles to implementation. These include lack of specialists, imperfection of banking and mathematical models, licensing costs, etc. In general, the use of artificial intelligence is the next step towards optimizing banking risk management in Ukraine.

References:

Cabinet of Ministers of Ukraine (2024). "National Cashback": you can now check the product for participation in the program in Action. Available at: https://me.gov.ua/News/Detail?lang=uk-UA&id=2b4948be-313a-4bd4-ad8f-0a8812ce735e&title=NatsionalniiKeshbek

Deloitte (2023). AI-driven Transformation in Financial Risk Operations. Available at: https://www2.deloitte.com

European Banking Authority (2024). Risk Dashboard Q4 2023. Available at: https://www.eba.europa.eu

ICU Research & USAID (2023). Operational Risk in Ukrainian Banking: Analytical brief. Available at: https://icu.ua

Kholyavko, N., Sadchykova, I., & Kolotyuk, M. (2023). Directions of using AI in banking institutions. *Problems and prospects of economics and management*, NVolo. 2, p. 192–203. DOI 10.25140/2411-5215-2023-2(34)-192-203

Komisja Nadzoru Finansowego (2023). Annual Report on Innovation in Financial Institutions. Available at: https://www.knf.gov.pl

McKinsey & Company (2022). The State of AI in Risk Management. Available at: https://www.mckinsey.com

Mykolaychuk, R. A., & Mykolaychuk, A. I. (2024). Using AI Technologies to Automate the Document Processing Process. *Modern information technologies in the field of security and defense*, Vol. 2, p. 111–117.

National Bank of Ukraine (2018), Resolution "Organization of the Risk Management System in Ukrainian Banks and Banking Groups". Available at: https://zakon.rada.gov.ua/laws/show/v0064500-18#Text

National Bank of Ukraine (2023), Resolution "On amendments to certain regulatory legal acts of the National Bank of Ukraine". Available at: https://zakon.rada.gov.ua/laws/show/v0040500-23#n2

National Bank of Ukraine (2023). Financial Stability Report, December 2023. Available at: https://bank.gov.ua

Prytsyuk, L. A. (2023). AI Technologies in Banks: Prospects and Caveats. *International Scientific Journal "Internauka". Series: Economic Sciences*, Vol. 4(2), p. 36–39.

Puzyrova, P., & Irnazarov, D. (2025). Specifics of Integration of AI into the Banking System of Ukraine. *Scientific Notes of the University "KROK"*, Vol. 1 (77), p. 66–78 DOI: https://doi.org/10.31732/2663-2209-2025-77-66-79

Solodkyi, V. V., & Polishchuk, Yu. A. (2023). Implementation of AI in Ukrainian Banks and Business: Prospects and Caveats. *Economic Bulletin of Dnipro Polytechnic,* Vol. 2, p. 119–127. DOI: https://doi.org/10.33271/ebdut/82.119

Statista (2023). AI (AI) Spending in Banking Industry Worldwide from 2018 to 2025. Available at: https://www.statista.com

USAID Financial Sector Reform Project (2023). Digitalization of Ukraine's Financial Sector: 2023 Overview. Available at: https://fsr.org.ua

Received on: 16th of April, 2025
Accepted on: 29th of May, 2025
Published on: 30th of June, 2025