Journal homepage: https://devma.com.ua/en

DEVELOPMENT MANAGEMENT

UDC 656:338.48
Doi: 10.57111/devt/4.2024.45

Vol. 23, No. 4. 2024

The impact of artificial intelligence on risk management in the operational activities of financial institutions

Mykyta Savchenko*

Master, Assistant
State University of Trade and Economics
02156, 19 Kyoto Str., Kyiv, Ukraine
https://orcid.org/0009-0004-9754-748X

Abstract. The purpose of the study was to determine the impact of artificial intelligence (AI) on the quality of management decisions in the process of risk assessment and forecasting. For this purpose, the role of AI in risk management was analysed, and the practices of using AI in risk management were studied. The study results confirmed that the introduction of AI significantly improves the speed and quality of risk management decisions. It was found that with the help of machine learning algorithms that use numerous variables to analyse the creditworthiness of customers, financial institutions are more efficient in credit scoring. The algorithms allow banks to reduce default rates and at the same time improve the quality of their loan portfolio by making assessments more informed. In addition, machine learning technologies are used to quickly identify suspicious activities or abnormal patterns of customer behaviour, reduce the number of fraudulent transactions, improve customer security and reduce the cost of identifying and eliminating such threats. Another result of the study was the confirmation of the effectiveness of automating routine processes, such as updating risk registers and generating reports, which can significantly reduce operating costs and speed up management decision-making. Importantly, the use of AI not only improves the accuracy of risk forecasting and decision-making, but also contributes to the personalisation of services for customers, which increases their loyalty and satisfaction. Together with the implementation of compliance systems, AI technologies ensure compliance with legal requirements and increase transparency in financial transactions, which reduces the likelihood of non-compliance with regulatory standards and minimises the risks involved. The findings indicated that the introduction of AI for risk management requires not only technological optimisation, but also a deep review of ethical standards, transparency of algorithms and adaptation of regulatory mechanisms, which will ensure both increased efficiency and trust in such systems

Keywords: machine learning; credit scoring; algorithms; transparency of decision-making; fraud prevention

INTRODUCTION

The use of artificial intelligence (AI) in risk management has increased significantly since the early 2010s. With the emergence of Industry 4.0, characterised by a high level of digitalisation, big data processing and the integration of AI into various sectors of the economy, traditional risk management methods have begun to show their limitations. This is especially evident in the financial sector, where processes are becoming increasingly complex and the amount of data that needs to be analysed to predict risks is growing significantly. The inability of organisations to adapt to new challenges can lead to a number of problems. For example, banking institutions that do not implement AI for risk forecasting or fraud detection risk incurring financial losses due to the inefficiency of traditional risk analysis models. However, the use of AI is also accompanied by challenges: transparency of AI algorithms, bias in decision-making, ethical aspects, management of large amounts of data, and customer privacy. If these issues are not effectively addressed, the introduction of AI may create more risks than it solves.

Research in the field of digital banking and financial technology has covered various aspects of the implementation of digital solutions in financial institutions and

Article's History: Received: 14.06.2024; Revised: 06.11.2024; Accepted: 17.12.2024

Suggested Citation:
Savchenko, M. (2024). The impact of artificial intelligence on risk management in the operational activities of financial institutions. *Development Management*, 23(1), 45-54. doi: 10.57111/devt/4.2024.45.

*Corresponding author

their impact on the financial services market. A. Medvid & D. Dmitrishyn (2024) studied the transformation of Ukraine's banking system due to the impact of digital banking. The authors found that digital banks not only increase the availability of financial services, but also stimulate other banks to innovate, which contributes to the development of market competition. K. Kraus *et al*. (2021) researched the success of Monobank as an example of the effective integration of digital technologies into the Ukrainian banking sector. Thanks to its mobile approach and continuous innovation, Monobank has managed to significantly improve the user experience and reduce operating costs, H. Arslanian & F. Fischer (2019) expanded the understanding of the impact of FinTech, AI, and cryptocurrencies on traditional banking models and demonstrated how these technologies accelerate automation and increase the efficiency of financial transactions. At the same time, the researchers described the regulatory and security challenges that arise in the process of technology adoption.

The reviewed studies on the use of AI in project management have revealed important aspects of the introduction of innovative technologies to improve project management efficiency and minimise risks. E. Vyhmeister & G.G. Castane (2024) developed a risk management system based on trust in AI systems and the ethical and responsible aspects of its implementation. The authors emphasised the importance of integrating AI into project management processes, taking into account the new requirements of Industry 5.0, which can contribute to safer and more efficient project management.

The issues of AI for improving risk management in financial and production systems have been addressed in the works by G. Baryannis *et al*. (2019), H. Zhou *et al*. (2019) and G. Piao & B. Xiao (2022). The use of IoT technologies in combination with big data and neural networks for financial risk management was investigated by H. Zhou *et al*. (2019). The researchers found that the use of particle swarm optimisation and neural networks allows for more accurate processing of large amounts of data and a quicker response to changing market conditions. Research by G. Piao & B. Xiao (2022) complemented this topic by confirming the effectiveness of identifying behavioural patterns of customers and investors by integrating behavioural financial theory with neural networks to more accurately predict risks in commercial banks. G. Baryannis *et al*. (2019) reviewed the ways in which AI can be applied to supply chain risk management and found that traditional risk management methods are not always effective in the context of globalisation and the complexity of modern supply chains.

The reviewed studies pointed to insufficient research on the behavioural aspects of AI in risk management, ethical issues in the use of AI, and the lack of research covering the comprehensive impact of AI on various areas of risk management. The purpose of this study was to analyse the effectiveness of AI in risk management in financial projects. To achieve this goal, the following objectives were set: to study global trends in the use of AI; to analyse risk management practices and identify key challenges to the implementation of AI by financial institutions; to provide recommendations for the implementation of AI in risk management processes.

MATERIALS AND METHODS

The statistical data and current trends in the use of AI in risk management were considered (Sizing the prize..., 2017; Agarwal *et al*., 2021; Governing AI responsibly, 2022; Calvery, 2024; IBM cost..., 2024). The reports considered the areas of application and weaknesses of the following technologies: automation of risk identification, risk analysis, monitoring and early detection of risks, decision support, automation of routine tasks, cybersecurity, and information risk management. The next step was to study the areas of AI application in banks. To analyse how financial institutions use AI for risk management, available information was collected from open sources, including academic sources, publications in specialised organisations, and other documents. The study of credit scoring analysed the machine learning methods and algorithms used to assess creditworthiness, as well as the factors that influence the speed and accuracy of credit decision-making. The process of collecting and analysing customer data considered included financial history, demographic and behavioural data, and other variables used to train machine learning models. To study the fraud detection process and assess its effectiveness, the algorithms used to analyse real-time transactions and detect suspicious activity were reviewed. Procedures for using anomaly and suspicious behaviour detection algorithms to prevent fraudulent transactions were considered, and the way to integrate these solutions into the overall banking cybersecurity strategy was analysed.

The data collected allowed analysing in detail the process of integrating AI-based threat detection systems and their role in ensuring the information security of banks. The study also looked at compliance processes: anti-money laundering and countering the financing of terrorism. This stage of the study analysed how AI is used to automate the process of detecting suspicious transactions and to comply with regulatory requirements. Data was collected on how algorithms analyse customer transactions and identify abnormalities that may indicate a possible financial crime. The analysis process included consideration of the use of AI in the "know your customer" procedure and its role in reducing operational risks. The information was processed using the synthesis method, which allowed to formulate recommendations for the successful implementation of AI in risk management, as well as outline the prospects for using AI in business processes.

RESULTS

Theoretical foundations of AI impact on risk management of financial institutions' operational activities

In the business environment of the early 2020s, AI has become an integral element of risk management strategies. Organisations of various sizes and industries are actively implementing AI technologies to improve the efficiency of risk identification, analysis and monitoring, driven by the growing complexity of risk factors, the speed of market changes and the need to process large amounts of data. Global trends in the implementation of AI in risk management cover several key areas. The use of machine learning to predict financial risks is becoming a standard practice in financial institutions. Algorithms are used to analyse data, identify patterns, and predict possible scenarios, allowing companies to proactively manage financial threats.

In addition, natural language processing is used to analyse unstructured data such as reports, news and social media. This practice helps to identify potential risks related to a company's reputation, changes in the regulatory environment, or market trends; textual data analysis provides a more complete picture of the risk landscape and allows for informed decision-making. In cybersecurity, AI plays a critical role in detecting and preventing cyber threats: deep learning algorithms are used to analyse network traffic and user behaviour in real time, identifying anomalies and potential attacks. This is especially important as the number and complexity of cyber threats increase, requiring a quick and effective response.

Statistical data from a survey conducted by A. Agarwal *et al*. (2021) have shown that more than 50% of companies already use AI in business processes, including risk management, which increases forecasting accuracy by 10-15% and reduces costs by 5-10%. According to PwC, the use of AI is expected to increase global gross domestic product by up to 14% by 2030, with the financial services sector becoming one of the most profitable (Sizing the prize..., 2017). Gartner predict that by 2025, 45% of all organisations will be subject to cyberattacks (Gartner identifies..., 2022), and according to IBM, companies that implement AI for security can reduce the time to detect cyber threats by 108 days compared to those that do not use these technologies (IBM cost..., 2024). In addition, organisations that use AI and automation save an average of USD 1.76 million per incident, which demonstrates the potential of technology to reduce operational risks. At the same time, according to KPMG, 61% of executives do not trust AI systems, which may slow down their adoption (Governing AI responsibly, 2022).

These trends have shown that AI is becoming a key tool in risk management, enabling organisations to more accurately predict, effectively respond to, and strategically plan actions in the face of uncertainty. AI has significantly changed approaches to risk management, affecting various aspects of the process; it has automated risk identification and assessment processes that were traditionally labour-intensive and dependent on subjective assessments by specialists. With the help of machine learning and big data analytics, organisations can process large amounts of information from various sources, including financial indicators, market trends and internal operational data, which helps to identify potential risks at an early stage and provides more informed assessments of their impact.

AI has enabled organisations to conduct deeper and more accurate risk analysis: deep learning algorithms and neural networks are able to identify complex patterns and relationships between different risk factors that may not be available to traditional analysis methods. Technology has made it possible to predict the likelihood of risks and their potential impact with high accuracy, which is critical for strategic planning and informed decision-making. AI technologies have enabled continuous monitoring of internal and external factors affecting an organisation's risks. Real-time systems are able to quickly detect deviations from normal behaviour or anomalies in processes, which is especially important in areas where risks can progress rapidly (e.g., financial markets or cybersecurity). Early detection of risks allows organisations to respond in a timely manner and minimise potential negative consequences.

In addition, AI can act as a decision support tool, providing managers with access to up-to-date and detailed information. AI-powered analytics systems can model different scenarios, assess potential outcomes, and suggest optimal response strategies to help allocate resources efficiently and maximise the effectiveness of investments. AI can automate many routine and repetitive risk management tasks, including updating risk registers, generating regular reports, monitoring compliance, and other administrative processes. Automating these tasks can reduce the likelihood of human error, increase efficiency, and allow staff to focus on more strategic aspects of risk management.

In the digital world, cybersecurity has become one of the key areas of risk management, and AI plays a crucial role in detecting and preventing cyber threats. Machine learning algorithms are aimed at analysing network traffic, user behaviour, and system logs to detect anomalies that may indicate unauthorised access attempts or cyberattacks. The use of AI in cybersecurity allows organisations to proactively respond to threats, reducing the risk of data breaches and financial losses. At the same time, it should be borne in mind that the introduction of AI can create problems that require additional attention to identify and resolve (Table 1).

Table 1. Areas of AI application and potential weaknesses

Areas of AI application	Execution	Possible weaknesses
Automation of risk identification	Big data analysis: AI processes large amounts of structured and unstructured data to identify potential risks. Machine learning: Algorithms are trained on historical data to predict possible future risks.	Data quality: It is necessary to ensure that the data is accurate, complete, and up-to-date. Confidentiality: Compliance with regulations on the protection of personal information.
Risk analysis	Predictive analytics: Modelling development scenarios and assessing the likelihood of risks. Natural language processing: Analysing text documents to identify potential risks missed by manual analysis.	Interpretability of models: It is important to understand how AI models make decisions. Algorithm biases: Checking models for biases that may affect the accuracy of the analysis.
Monitoring and early detection of risks	Real-time monitoring: Continuous tracking of indicators with alarms in case of deviations. Sentiment analysis: Tracking team or stakeholder sentiment through communication platforms.	False alarms: The possibility of an overabundance of alerts that may be ignored. False positives: AI systems produce a result with a percentage of probability, and may provide false positives or false negatives.

Table 1, Continued

Areas of AI application	Execution	Possible weaknesses
Decision support	Recommendation systems: Suggesting optimal risk response strategies. Resource optimisation: Algorithms help in the allocation of resources to minimise the impact of risks.	Dependence on technology: Avoiding over-reliance on AI, maintain critical thinking. Staff training: The team must understand the principles of AI systems.
Automation of routine tasks	Robotic process automation (RPA): Automation of repetitive tasks, such as updating risk registers or generating reports.	Resistance to change: Effective change management must be ensured to avoid resistance. Technical failures: Having backup plans in place in case of system failures.
Cybersecurity and information risk management	Anomaly detection: Detecting unusual activity on networks and systems. Attack prediction: Analysing cyber threat patterns to predict possible attacks.	Updating algorithms: Regularly updating AI models to keep up with new threats. Compliance: Compliance with regulatory requirements for cybersecurity and data protection.

Source: compiled by the author

The integration of AI into risk management contributes to the efficiency and resilience of organisations. It provides more accurate and timely analysis, allows for a better understanding of complex risk environments, and allows for a greater degree of confidence in responding to them. However, successful AI adoption requires consideration of technical, ethical and legal aspects, including data quality, privacy and regulatory compliance.

The use of AI in risk management in financial organisations

Banks of the 21st century are actively using mobile applications to reduce operating costs and provide convenient access to financial products. AI and machine learning help to increase the efficiency of operations and improve the customer experience. Technology also allows for the automation of risk management processes, especially in the area of credit scoring, and the use of machine learning algorithms to quickly analyse large amounts of data helps to reduce credit risks, detect fraudulent transactions and make informed financial decisions. Banks are focused on implementing technological innovations to improve the convenience and security of customer service. Among the most common AI tools are systems for analysing customer behavioural data, which allow for quick adaptation of products to the needs of users, and automated support services that provide advice and answers to customer questions in real time. Studies show that the use of such technologies has become a standard among leading financial institutions seeking to ensure the accuracy of assessments and efficiency of operations (Dunas & Bilokrynytska, 2019; Yanenkova *et al.*, 2021; Grabovets & Temelkov, 2024). As AI becomes an integral part of the banking sector, further development and implementation of innovative solutions aimed at improving the efficiency of financial services is expected.

The introduction of machine learning algorithms has significantly improved the speed and accuracy of credit decision-making: customers can receive a loan decision within a short time after applying through a mobile application, and the use of AI has improved the quality of the loan portfolio and reduced credit risks (Agarwal *et al.*, 2021; Edunjobi & Odejide, 2024). In other words, the use of AI in credit scoring and credit risk assessment has enabled financial institutions to increase process efficiency, reduce the risk of loan default, and improve customer service, which has a positive impact on the bank's financial stability.

Systems that use algorithms to detect anomalies and suspicious behaviour analyse customer transaction patterns, taking into account parameters such as transaction amounts, transaction frequency, geolocation and previous transaction history. When deviations from normal behaviour are detected, the system automatically generates alerts for further verification. The anomaly detection algorithms are based on machine learning techniques, including clustering models and deep neural networks. They are able to detect complex fraud schemes that may be invisible to traditional systems. For example, if a transaction is made from an unusual location for the customer or there is unusual activity at night, the system can temporarily block the transaction and send a confirmation request to the customer (Ali *et al.*, 2022).

As financial organisations such as JP Morgan and Gartner actively use AI to monitor transactions in real time to detect fraud and ensure cybersecurity, the technology allows them to analyse large amounts of transactional data, identify anomalies in user behaviour and respond quickly to potential threats (Gartner identifies..., 2022; How AI..., 2023). AI-based systems are constantly learning from new data, which helps to quickly identify fraudulent transactions, such as phishing, identity theft, or attempts to use stolen card data. This significantly increases the effectiveness of protection and reduces the risk of financial losses from cyber threats, which is also confirmed by many sources analysing current trends in the financial sector (Aschi *et al.*, 2022; Afriyie *et al.*, 2023; Al-hchaimi *et al.*, 2024). Fraud prevention measures include multifactor authentication and the use of biometrics to verify the customer's identity and a behavioural biometrics system that analyses unique patterns of customer interaction with a mobile application, such as typing speed and mouse movements. This is known to further increase the level of economic security at the micro level and reduce the risk of unauthorised access (Koba, 2021).

The results of the introduction of AI in cybersecurity are also positive: AI's rapid response to potential threats minimises operational risks and losses for banks, and its use in cybersecurity helps to comply with regulatory requirements for data protection and prevent money laundering. The introduction of AI for fraud detection and cybersecurity can increase the effectiveness of financial transaction protection, reduce the number of fraudulent transactions, and improve customer security, which has had a positive impact on the reputation and financial stability of banks (Managing artificial..., 2024).

Financial institutions are actively using AI to analyse customer behaviour in order to provide personalised services and effectively manage customer risks. Machine learning algorithms analyse customer transaction history, financial activity, and other relevant data, allowing banks to create detailed customer profiles, identify their financial needs, and anticipate potential risks. Based on the collected data, they generate individual offers and recommendations that meet the unique needs of each client. For example, a bank may offer special loan products, favourable deposit terms or personalised loyalty programmes. Such an approach is known to increase customer satisfaction and strengthen long-term relationships with the bank (Jaiwant, 2022; Gigante & Zago, 2022). Credit limits are managed based on the client's risk profile generated by AI. By analysing payment discipline, income, and other financial indicators, banks can dynamically adjust credit limits, which helps reduce the risk of default and ensure more responsible lending.

The use of AI in know-your-customer and anti-money laundering procedures is gradually being seen as a standard for modern financial institutions (Ridzuan *et al.*, 2024). In know-your-customer procedures, financial institutions use automatic facial recognition and document analysis technologies to identify customers quickly and accurately: customers can upload photos of documents and selfies when registering via a mobile application, and AI checks the data and authenticity of documents, reducing the risk of fraud and errors in the verification process.

To combat money laundering, machine learning algorithms can also be used to analyse customer transactions in real time. Such algorithms identify suspicious behaviour patterns, atypical amounts or frequency of transactions, transfers to accounts in high-risk countries, etc. When anomalies are detected, the system generates alerts for the compliance department for further investigation. The use of AI in compliance processes helps to reduce operational risks, as automation of routine tasks reduces the likelihood of human error, increases the efficiency of the compliance department and allows employees to focus on more complex analytical tasks. This helps banks avoid fines and penalties from regulators, maintain financial stability and retain customer confidence.

It is important that AI risk management practices are in line with international standards and recommendations in the banking sector. Banks should use advanced machine learning and data analytics technologies in line with the recommendations of the Basel Committee on Banking Supervision to improve risk management through the use of modern technologies (Digitalisation of finance, 2024) and recommendations of scientists (Thach *et al.*, 2021). The use of AI should be based on ethical principles and compliance with regulatory requirements, in line with industry best practices. In the area of anti-money laundering and countering terrorist financing, the use of AI to automate anti-money laundering and countering terrorist financing processes should comply with the recommendations of the Financial Action Task Force and the requirements of the national bank of the country in which the bank operates, contributing to the effective detection and prevention of illegal financial transactions (FATF, 2021).

The use of AI has raised important ethical issues regarding the processing and protection of personal data. Collecting and analysing large amounts of data allows banks to improve their risk management, but at the same time requires high standards of confidentiality and ethics. As banks process significant amounts of their customers' information, including financial transactions, behavioural patterns and other personal data, this raises concerns about potential privacy breaches and the possibility of misuse. Ethical issues also relate to the transparency of AI algorithms used to make lending and risk management decisions. Lack of clarity on how algorithms make decisions can lead to discrimination or bias. For example, an algorithm may unknowingly favour certain groups of customers based on indirect indicators.

Aware of these risks, leading financial institutions are implementing measures to ensure the ethical use of data, including regular audits of algorithms for bias, ensuring transparency of processes, and providing customers with the opportunity to challenge decisions made by automated systems (Bias in algorithmic..., 2019). Banks should also inform customers about what data is collected, how it is used, and what rights customers have over their data. In addition, cybersecurity issues are critical, as a data breach or compromise could have serious consequences for customers. Institutions are required to invest in up-to-date data protection technologies, train staff on how to handle information securely, and respond to incidents in accordance with industry best practices. Ethical aspects also include responsibility for decisions made on the basis of AI, as automated systems should not violate the rights of customers, but rather act in their best interests. This requires a balance between the efficiency of technology and the ethical obligations of banks to their customers. Banks must comply not only with national laws but also with international standards, such as the Regulation of the European Parliament and of the Council No. 2016/679 (2016), if they serve EU customers.

Implementation of AI-based risk management in the financial sector

The introduction of AI in risk management opens up new opportunities to improve the efficiency of business processes. However, in order to maximise the benefits of these technologies, organisations need to follow specific strategic guidelines, including effective change management and optimisation of internal processes (Fig. 1).

Integrating AI into all stages of the risk management process requires organisations to consider data and data quality, as AI models require reliable and structured data to achieve accurate results. By implementing big data systems in conjunction with AI, financial institutions will be able to reduce operational risks, detect threats in advance, and minimise losses. Organisations that use real-time data significantly increase their ability to respond to potential threats. Another important aspect is the ongoing development and training of staff. As the introduction of AI is accompanied by significant technological changes, it is important to create training programmes for employees. They should not only understand the technological aspects of AI, but also be able to integrate new tools into their daily work. As the introduction of AI often changes the structure of processes, making them more automated and faster, it is worth paying attention to process management. Reviewing existing business procedures and optimising them to take into account new technologies can be done, for example, by integrating automated risk management systems into existing banking reporting platforms to facilitate decision-making.

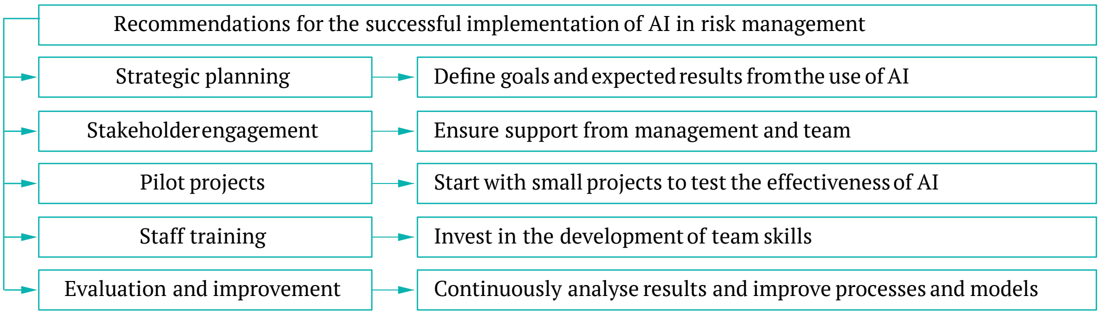
Recommendations for the successful implementation of AI in risk management
Strategic planning
Define goals and expected results from the use of AI
Stakeholder engagement
Ensure support from management and team
Pilot projects
Start with small projects to test the effectiveness of AI
Staff training
Invest in the development of team skills
Evaluation and improvement
Continuously analyse results and improve processes and models

Figure 1. Recommendations for the successful implementation of AI in risk management

Source: compiled by the author

Cybersecurity is another area where AI is needed; machine learning technologies help monitor transactions and detect anomalies in user behaviour, allowing banks to identify potentially fraudulent activities in time and protect themselves from cyberattacks. In this context, the prospects for the development of threat detection technologies are becoming one of the key tasks for ensuring the stability of financial institutions in the future. The prospects for AI implementation also lie in the opportunities to use the technology not only for risk management, but also to improve customer experience and develop new products and services. For example, personalised financial offers based on user behaviour analysis will help institutions better understand customer needs and increase customer loyalty. In addition, AI can become a tool for building predictive models that will allow banks to adapt their strategy to changing market conditions.

DISCUSSION

The study analysed in detail the impact of AI on risk management processes, particularly in the financial sector. It was found that AI is an effective tool for predicting financial risks, monitoring transactions in real time, and automating routine tasks. Thanks to the introduction of machine learning and anomaly detection algorithms, modern financial institutions have significantly improved the quality of credit risk management, fraud detection, and cybersecurity. The personalisation of customer services and compliance procedures, which are an integral part of effective risk management using AI, were also discussed.

An analysis of how banks are using AI technologies to analyse large amounts of structured and unstructured data has shown that AI allows them to identify potential risks based on the analysis of financial indicators, market trends and internal operational data. Automating processes with AI has significantly improved the accuracy of risk forecasting and simplified data processing, enabling organisations to respond to risks more quickly and make informed decisions. However, the challenges of this approach include the need to ensure high data quality and confidentiality. The study by A.M.A. Musleh Al-Sartawi *et al*. (2022) also examined the role of AI in big data processing, but in the context of sustainable finance. AI's assistance in analysing big data related to environmental, social, and governance factors can improve environmental risk assessment and forecasting the sustainability impact of investments.

The study examined the impact of AI-assisted automation on banking consumers. The use of AI in credit scoring, fraud detection, and customer behaviour analysis has allowed banks to improve the efficiency of their processes and provide more accurate risk assessment and personalised services. Consumers have gained faster access to banking products and greater protection from cyber threats, which has had a positive impact on their experience and increased trust in the bank. F. Königstorfer & S. Thalmann (2020) found that AI in commercial banks opens up new opportunities to study the behavioural aspects of customers' financial decisions, meaning that the use of AI can allow banks to better understand customer needs, offer more personalised services, and improve service. However, the issue of using AI to predict customers' financial behaviour remains unresolved.

Innovative technologies, including AI, not only help to improve the efficiency of financial operations, but can also provide access to financial services to a wider range of users. With the help of AI, financial institutions can automate routine processes, reduce costs, and increase the speed of processing applications for loans and other financial services. In addition, AI can better analyse customer behaviour and offer personalised solutions, which greatly simplifies access to financial products, especially for customers who previously faced restrictions due to complexity of procedures or lack of credit history. These findings are consistent with the study by D. Mhlanga (2020), who discussed the interaction of AI with the Fourth Industrial Revolution to address the problems of unequal access to financial services. The scientist noted that process automation and improved customer analysis really help to reduce barriers for those who previously had limited access to financial resources. The study by S. Ahmed *et al*. (2022) also confirmed the effectiveness of AI in the financial sector by systematising scientific publications on operations' automation, risk management, and data analysis, which can contribute to more informed decision-making in financial institutions.

AI technologies help optimise management decisions, increase efficiency and minimise risks. The introduction of AI allows for the automation of routine processes such as updating registers and generating reports, which can increase the speed and accuracy of management decisions. AI has also had a significant impact on improving cybersecurity, as machine learning algorithms help detect anomalies in systems and prevent cyber threats. AI-based analytical tools can help predict potential risks, assess the impact of management decisions on various aspects of organisations, make informed decisions, and reduce potential financial losses. Research by H. Pallathadka *et al*. (2023) similarly showed that AI automates routine tasks, improves the quality of decisions, and contributes to more accurate forecasting of risks and market trends in business, e-commerce, and financial services. In the financial sector, AI helps to optimise risk management processes, as well as improve the accuracy of financial forecasts and asset management. L. Cao (2022), in turn, emphasised the challenges associated with ensuring data quality and transparency of algorithms, which coincides with the need to comply with ethical standards in the use of AI in the financial sector.

The study analysed the practices of using AI in various financial processes and highlighted their strengths and weaknesses. The introduction of AI has allowed for the automation of important business processes, such as risk management and credit scoring, which has reduced human error and accelerated decision-making. The strengths of these practices include AI's ability to work with large amounts of data, detect fraudulent transactions quickly, and improve customer security. At the same time, weaknesses include the need to ensure the transparency of algorithms, avoid bias, and comply with regulatory requirements. These findings are consistent with the study by A. Ashta & H. Herrmann (2021), which also analysed the impact of AI on financial processes. The authors identified significant opportunities for AI to transform banking, investment, and microfinance, while also highlighting the risks associated with cyberattacks, data protection, and regulatory challenges. The study by J.W. Goodell *et al.* (2021) further demonstrated that key research areas are focused on risk management and forecasting, but there is a need to address issues of algorithmic interpretation and data protection.

The study analysed the implementation of AI-assisted process automation, including robotic process automation, which automates repetitive tasks such as updating risk registers and generating reports. Machine learning algorithms used to predict risks and analyse large amounts of data were also discussed. As AI has increased the efficiency of real-time risk monitoring and enabled the detection of anomalies in user behaviour, it has facilitated timely response to threats. These findings are in line with the study by H.A. Javaid (2024), in which the author concluded that AI significantly improves the efficiency of financial services by reducing costs and increasing the accuracy of decision-making. Integration of AI allows financial institutions to adapt their operating models to changing market conditions, ensure flexibility and resilience of business models, and improve the quality of customer service in a changing market environment.

Among the main threats and weaknesses in the use of AI technologies is the quality of the data on which the algorithms operate. False or incomplete data can lead to erroneous decisions and increased risks. Another weakness is the transparency of AI models – the difficulty in explaining how an algorithm makes certain decisions can cause concern among customers and regulators. It also creates potential legal risks, as unclear decisions can cause distrust and conflicts. In their paper, N. Bussmann *et al*. (2021) confirmed the above weaknesses and emphasised the need for transparency in machine learning models, especially in the area of credit risk management. Complex and opaque models can lead to legal and ethical problems due to a lack of clarity in the decision-making process. The authors suggested the introduction of explanatory methods in AI models to increase trust in such systems and improve risk management.

The study revealed the process of how financial institutions collect and use customer data. This data may include information on customer behavioural patterns, financial transactions, and other personal data to improve customer service and mitigate risks. Further processing with AI algorithms allows banks to assess the risk profile of a customer, dynamically adjust credit limits and offer personalised products. However, the collection of large amounts of data also raises ethical questions about privacy and transparency of decision-making, requiring banks to ensure high standards of data processing, including compliance with international and national standards. V. Moscato *et al*. (2021) complemented this data by investigating different approaches to using machine learning to predict credit scores. The researchers compared several algorithms for assessing borrowers' creditworthiness and found that the use of different machine learning models allows financial institutions to choose the most effective approaches to reduce risks and improve decision-making. The studies reviewed highlighted the importance and prospects of using AI to increase the efficiency of financial transactions, mitigate risks, and improve customer interactions. At the same time, the need to increase the transparency of AI algorithms and implement ethical principles when working with large amounts of data remains a common problem.

CONCLUSIONS

The study demonstrated the significant impact of AI on risk management in various areas, especially in the financial sector. The analysis found that AI technologies significantly improve the processes of risk identification, assessment, and monitoring and help organisations achieve greater efficiency and resilience in a challenging market environment. It was found that the implementation of machine learning algorithms allows banks to predict risks faster and more accurately, which has a positive impact on management strategies. Real-time data analytics and machine learning have made it possible to automate labour-intensive processes, such as credit scoring and fraud detection. As a result, organisations can identify potential threats faster, respond to them and minimise potential losses.

AI technologies significantly improve the accuracy of risk analysis by being able to process large amounts of information. The use of deep learning and natural language analysis techniques allows financial institutions to identify market trends, assess reputational risks, and detect cyber threats faster. In areas such as cybersecurity, AI has become a key tool for detecting cyber threats by analysing network traffic and user behaviour in real time, as well as for improving credit risk management and cybersecurity. Implemented machine learning algorithms have allowed banks not only to make faster credit decisions, but also to significantly reduce credit risks. The use of AI helps automate routine tasks such as updating risk registers and regulatory reporting. This is especially true for anti-money laundering and countering the financing of terrorism. By integrating AI into these processes, organisations can perform know-your-customer procedures faster and more accurately and prevent money laundering and terrorist financing risks. In addition, AI technologies significantly increase the ability of decision support systems to model various scenarios, allowing management to better allocate resources and improve overall risk management efficiency. In particular, in the area of anti-money laundering and countering the financing of terrorism, process automation allows organisations to meet regulatory requirements and reduce operational risks.

However, the study also identified certain challenges associated with AI integration, including ensuring data quality and compliance with legal regulations, especially in the context of personal data protection. The transparency of the algorithms used for decision-making remains an important issue, as they may affect the fairness and accuracy of risk assessment. For further research, it is recommended to pay attention to the analysis of specific technological solutions implemented in financial institutions that are willing to provide more open data on their functioning. This will allow obtaining expanded data on the impact of AI on risk management. In addition, further research is recommended to focus on ethical issues related to the use of AI, in particular, transparency of decision-making and avoidance of algorithmic bias. An in-depth analysis of these topics will allow for a better understanding of how AI can not only improve risk management efficiency, but also expand opportunities for the development of new products and services in the banking sector.

ACKNOWLEDGEMENTS

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] Afriyie, J.K., Tawiah, K., Pels, W.A., Addai-Henne, S., Dwamena, H.A., Owiredu, E.O., Ayeh, S.A., & Eshun. J. (2023). A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. *Decision Analytics Journal*, 6, article number 100163. doi: 10.1016/j.dajour.2023.100163.

[2] Agarwal, A., Singhal, C., & Thomas, R. (2021). *AI-powered decision making for the bank of the future*. Retrieved from http://surl.li/jyoylx.

[3] Ahmed, S., Alshater, M.M., Ammari, A.E., & Hammami, H. (2022). Artificial intelligence and machine learning in finance: A bibliometric review. *Research in International Business and Finance*, 61, article number 101646. doi: 10.1016/j.ribaf.2022.101646.

[4] Al-hchaimi, A.A.J., Alomari, M.F., Muhsen, Y.R., Sulaiman, N.B., & Ali, S.H. (2024). Explainable machine learning for real-time payment fraud detection: Building trustworthy models to protect financial transactions. In A. Alnoor, M. Camilleri, H.A. Al-Abrrow, M. Valeri, G.E. Bayram & Y.R. Muhsen (Eds.), *Explainable artificial intelligence in the digital sustainability administration* (pp. 1-25). Cham: Springer. doi: 10.1007/978-3-031-63717-9_1.

[5] Ali, A., Abd Razak, S., Othman, S.H., Eisa, T.A.E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial fraud detection based on machine learning: A systematic literature review. *Applied Sciences*, 12(19), article number 9637. doi: 10.3390/app12199637.

[6] Arslanian, H., & Fischer, F. (2019). *The future of finance: The impact of fintech, AI, and crypto on financial services*. Cham: Palgrave Macmillan. doi: 10.1007/978-3-030-14533-0.

[7] Aschi, M., Bonura, S., Masi, N., Messina, D., & Profeta, D. (2022). Cybersecurity and fraud detection in financial transactions. In J. Soldatos & D. Kyriazis (Eds.), *Big data and artificial intelligence in digital finance* (pp. 269-278). Cham: Springer. doi: 10.1007/978-3-030-94590-9_15.

[8] Ashta, A., & Herrmann, H. (2021). Artificial intelligence and fintech: An overview of opportunities and risks for banking, investments, and microfinance. *Strategic Change*, 30(3), 211-222. doi: 10.1002/jsc.2404.

[9] Baryannis, G., Validi, S., Dani, S., & Antoniou, G. (2019). Supply chain risk management and artificial intelligence: State of the art and future research directions. *International Journal of Production Research*, 57(7), 2179-2202. doi: 10.1080/00207543.2018.1530476.

[10] Bias in algorithmic decision making in financial services. Barclays response. (2019). Retrieved from http://surl.li/njuxif.

[11] Bussmann, N., Giudici, P., Marinelli, D., & Papenbrock, J. (2021). Explainable machine learning in credit risk management. *Computational Economics*, 57, 203-216. doi: 10.1007/s10614-020-10042-0.

[12] Calvery, J. (2024). *Harnessing the power of AI to fight financial crime*. Retrieved from http://surl.li/dqtqvz.

[13] Cao, L. (2022). AI in finance: Challenges, techniques, and opportunities. *ACM Computing Surveys*, 55(3), article number 64. doi: 10.1145/3502289.

[14] Digitalisation of finance. (2024). Retrieved from https://www.bis.org/bcbs/publ/d575.pdf.

[15] Dunas, N., & Bilokrynytska, M. (2019). Implementation of credit scoring system by Ukrainian banks for consumer credit. *Pryazovskyi Economic Herald*, 5(16), 263-269. doi: 10.32840/2522-4263/2019-5-45.

[16] Edunjobi, T.E., & Odejide, O.A. (2024). Theoretical frameworks in AI for credit risk assessment: Towards banking efficiency and accuracy. *International Journal of Scientific Research Updates*, 7(1), 92-102. doi: 10.53430/ijsru.2024.7.1.0030.

[17] FATF. (2021). Opportunities and challenges of new technologies for AML/CFT. Paris: FATF.

[18] Gartner identifies top security and risk management trends for 2022. (2022). Retrieved from https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022.

[19] Gigante, G., & Zago, A. (2023). DARQ technologies in the financial sector: Artificial intelligence applications in personalized banking. *Qualitative Research in Financial Markets*, 15(1), 29-57. doi: 10.1108/QRFM-02-2021-0025.

[20] Goodell, J.W., Kumar, S., Lim, W.M., & Pattnaik, D. (2021). Artificial intelligence and machine learning in finance: Identifying foundations, themes, and research clusters from bibliometric analysis. *Journal of Behavioral and Experimental Finance*, 32, article number 100577. doi: 10.1016/j.jbef.2021.100577.

[21] Governing AI responsibly. (2022). Retrieved from https://kpmg.com/kpmg-us/content/dam/kpmg/pdf/2022/governing-ai-responsibly.pdf.

[22] Grabovets, K., & Temelkov, Z. (2024). Interplay between digital-only strategy and financial performance: A case of neobanks. In A.M. Yazıcı, A. Albattat, M. Valeri & V. Hassan (Eds.), *New strategy models in digital entrepreneurship* (pp. 214-235). London: IGI Global. doi: 10.4018/979-8-3693-3743-1.ch011.

[23] How AI will make payments more efficient and reduce fraud. (2023). Retrieved from https://www.jpmorgan.com/insights/payments/payments-optimization/ai-payments-efficiency-fraud-reduction.

[24] IBM cost of a data breach report 2023 reveals huge business data breach costs. (2024). Retrieved from https://10guards.com/en/articles/ibm-cost-of-a-data-breach-report-2023-reveals-huge-business-data-breach-costs/.

[25] Jaiwant, S.V. (2022). Artificial intelligence and personalized banking. In V. Garg & R. Goel (Eds.), *Handbook of research on innovative management using AI in industry 5.0* (pp. 74-87). Hershey: IGI Global. doi: 10.4018/978-1-7998-8497-2.

[26] Javaid, H.A. (2024). The future of financial services: Integrating AI for smarter, more efficient operations. *MZ Journal of Artificial Intelligence*, 1(2).

[27] Koba, O. (2021). System of economic security and levels of its formation. *Economics of Development*, 20(3), 40-47. doi: 10.57111/econ.20(3).2021.40-47.

[28] Königstorfer, F., & Thalmann, S. (2020). Applications of artificial intelligence in commercial banks – a research agenda for behavioral finance. *Journal of Behavioral and Experimental Finance*, 27, article number 100352. doi: 10.1016/j.jbef.2020.100352.

[29] Kraus, K., Kraus, N., & Shtepa, O. (2021). Case 4: Diya.Business. In A. Botti, R. Parente & M. Vesci (Eds.), *How to do business in digital era?* (pp. 32-41). Cracow: Cracow University of Economics.

[30] Managing artificial intelligence-specific cybersecurity risks in the financial services sector. (2024). Retrieved from http://surl.li/zjqcab.

[31] Medvid, A., & Dmitrishyn, D. (2024). Digital banking in the financial services market of Ukraine. *Visnyk of Sumy State University. Economy Series*, 2, 18-27. doi: 10.21272/1817-9215.2024.2-02.

[32] Mhlanga, D. (2020). Industry 4.0 in finance: The impact of artificial intelligence (AI) on digital financial inclusion. *International Journal of Financial Studies*, 8(3), article number 45. doi: 10.3390/ijfs8030045.

[33] Moscato, V., Picariello, A., & Sperlí, G. (2021). A benchmark of machine learning approaches for credit score prediction. *Expert Systems with Applications*, 165, article number 113986. doi: 10.1016/j.eswa.2020.113986.

[34] Musleh Al-Sartawi, A.M.A., Hussainey, K., & Razzaque, A. (2022). The role of artificial intelligence in sustainable finance. *Journal of Sustainable Finance & Investment*. doi: 10.1080/20430795.2022.2057405.

[35] Pallathadka, H., Ramirez-Asis, E.H., Loli-Poma, T.P., Kaliyaperumal, K., Ventayen, R.J.M., & Naved, M. (2023). Applications of artificial intelligence in business management, e-commerce and finance. *Materials Today: Proceedings*, 80(3), 2610-2613. doi: 10.1016/j.matpr.2021.06.419.

[36] Piao, G., & Xiao, B. (2022). Risk management analysis of modern commercial banks using behavioral finance theory and artificial neural networks. *Wireless Communications and Mobile Computing*, 1, article number 1161784. doi: 10.1155/2022/1161784.

[37] Regulation of the European Parliament and of the Council No. 2016/679 "On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)". (2016, April). Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[38] Ridzuan, N.N., Masri, M., Anshari, M., Fitriyani, N.L., & Syafrudin, M. (2024). AI in the financial sector: The line between innovation, regulation and ethical responsibility. *Information*, 15(8), article number 432. doi: 10.3390/info15080432.

[39] Sizing the prize: What's the real value of AI for your business and how can you capitalise? (2017). Retrieved from https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf.

[40] Thach, N.N., Hanh, H.T., Gwoździewicz, S., Huy, D.T.N., Nga, L.T.V., Thuy, D.M., & Hong, P.V. (2021). Technology quality management of the industry 4.0 and cybersecurity risk management on current banking activities in emerging markets – the case in Vietnam. *International Journal for Quality Research*, 15(3), 845-856. doi: 10.24874/IJQR15.03-10.

[41] Vyhmeister, E., & Castane, G.G. (2024). TAI-PRM: Trustworthy AI – project risk management framework towards industry 5.0. *AI and Ethics*. doi: 10.1007/s43681-023-00417-y.

[42] Yanenkova, I., Nehoda, Y., Drobyazko, S., Zavhorodnii, A., & Berezovska, L. (2021). Modeling of bank credit risk management using the cost risk model. *Journal of Risk and Financial Management*, 14(5), article number 211. doi: 10.3390/jrfm14050211.

[43] Zhou, H., Sun, G., Fu, S., Liu, J., Zhou, X., & Zhou, J. (2019). A big data mining approach of PSO-based BP neural network for financial risk management with IoT. *IEEE Access*, 7, 154035-154043. doi: 10.1109/ACCESS.2019.2948949.

Вплив штучного інтелекту на управління ризиками в операційній діяльності фінансових установ

Микита Савченко

Магістр, асистент
Державний торговельно-економічний університет
02156, вул. Кіото, 19, м. Київ, Україна
https://orcid.org/0009-0004-9754-748X

Анотація. Метою роботи було визначити вплив штучного інтелекту (ШІ) на якість управлінських рішень у процесі оцінки та прогнозування ризиків. Для цього було виконано аналіз ролі ШІ в управлінні ризиками, досліджено практики використання ШІ в управлінні ризиками. Результати дослідження підтвердили, що впровадження ШІ значно підвищує швидкість і якість прийняття рішень, пов'язаних з управлінням ризиками. Було виявлено, що за допомогою алгоритмів машинного навчання, які використовують велику кількість змінних для аналізу кредитоспроможності клієнтів, фінансові установи ефективніше здійснюють кредитний скоринг. Алгоритми дозволяють банкам знижувати рівень дефолтів і водночас покращувати якість кредитного портфеля, що робить оцінки більш обґрунтованими. Крім того, технології машинного навчання використовуються для оперативної ідентифікації підозрілих дій або аномальних моделей поведінки клієнтів, зменшення кількості шахрайських операцій, підвищення рівня безпеки клієнтів та скорочення витрат на виявлення й усунення таких загроз. Іншим результатом дослідження стало підтвердження ефективності автоматизації рутинних процесів, таких як оновлення реєстрів ризиків та генерування звітів, що дозволяє суттєво знизити операційні витрати й прискорити процеси прийняття управлінських рішень. Важливо, що використання ШІ не лише підвищує точність прогнозування ризиків і прийняття рішень, але й сприяє персоналізації послуг для клієнтів, що підвищує їхню лояльність та задоволеність. Разом із впровадженням систем комплаєнсу, технології ШІ забезпечують дотримання правових вимог і підвищують прозорість у фінансових операціях, що знижує ймовірність невідповідності регуляторним нормам та мінімізує відповідні ризики. Отримані результати вказали на те, що впровадження ШІ для управління ризиками, потребує не лише технологічної оптимізації, але й глибокого перегляду етичних стандартів, прозорості алгоритмів та адаптації регуляторних механізмів, що в комплексі забезпечить як підвищення ефективності, так і довіру до таких систем

Ключові слова: машинне навчання; кредитний скоринг; алгоритми; прозорість прийняття рішень; запобігання шахрайству