Annual International Scientific Conference
"Competitiveness and Innovation in the Knowledge Economy"
September 26-27, 2025
Chisinau, Republic of Moldova

DOI: https://doi.org/10.24818/cike2025.70

PROSPECTS FOR THE INTRODUCTION OF ARTIFICIAL INTELLIGENCE TO DETECT AND BLOCK CYBER THREATS IN THE FINANCIAL SPHERE OF THE MINISTRY OF INTERNAL AFFAIRS

YULIIA SYNYTSINA
Associate Professor of the Department of Information Technologies
Dnipro State University of Internal Affairs, Ukraine
e-mail: ysynytsina0@gmail.com,
ORCID ID: 0000-0002-6447-821X

Abstract: The modern financial and economic processes within the Ministry of Internal Affairs of Ukraine face increasing complexity and exposure to sophisticated cyber threats. Traditional protection methods, including antivirus programs, filtering systems, and firewalls, have become insufficient due to the dynamic and targeted nature of contemporary cyberattacks. In response, the implementation of artificial intelligence (AI) and machine learning (ML) technologies has emerged as a critical approach for detecting, predicting, and mitigating threats in the financial sector. AI-based systems, including neural networks, enable intelligent decision support by analyzing user behavior, detecting anomalies, and forecasting risks in real time, thereby reducing the incidence of fraud, money laundering, and unauthorized access. Research has demonstrated that modeling antagonistic agent behavior and integrating adaptive AI systems can significantly decrease hybrid threat implementation, financial losses, and incident response time. The application of AI in public-sector financial operations involves automated monitoring of payments, contracts, and public procurement, as well as verification of counterparties and anomaly detection in transactions. Technical implementations employ flow analytics, graph models, behavioral profiling, and deepfake detection, supported by human-in-the-loop operational models. Compliance with regulatory and ethical standards, particularly the NIST AI Risk Management Framework, ensures transparency, reliability, and explainability of AI decisions. Challenges include high-quality data requirements, cost of implementation, offensive AI threats, and regulatory adherence. Pilot projects for AI/ML-based financial threat detection demonstrate the potential for rapid anomaly identification, improved fraud prevention, and enhanced overall financial security. Integrating intelligent systems thus strengthens the cyber resilience of the Ministry of Internal Affairs, supporting both operational efficiency and strategic risk management.
Keywords: AI strengthens MIA financial cyber security.
JEL Classification: G21, G28, G32, O33, C45

The modern development of financial and economic processes in the system of the Ministry of Internal Affairs of Ukraine is accompanied by an increase in the number and complexity of cyber threats. Traditional methods of protection (antivirus programs, filtering systems and firewalls) are increasingly insufficient as cyberattacks become more targeted, dynamic and technologically sophisticated. In this context, the introduction of artificial intelligence (AI) and machine learning technologies to detect, predict and block threats in the financial sphere is relevant. The application of neural networks in the intelligent decision support system at the enterprise is described in (Synytsina et al., 2022; Synytsina et al., 2019). Based on the results of the study, an analysis model was formulated and practical aspects of the application of neural networks (NM) in the marketing information system (MIS) of the enterprise were considered in order to improve the information system of the enterprise by implementing an intelligent decision support system (ISDS) using a neural network (Synytsina et al., 2022; Synytsina et al., 2019). The authors of the paper (Milov et al., 2020) propose the Concept of modeling the behavior of interacting agents, the basis of which is a three-level structure of modeling subjects and business

processes in the contours of the functioning of the organization and the security system. This concept is based on modeling the behavior of antagonistic agents. The financial sector is one of the most vulnerable to cyber threats, fraudulent operations and abuse. A large number of transactions are processed every day, creating significant risks of unauthorized access, data falsification or manipulation. Traditional methods of control are gradually losing effectiveness due to the growth of information volumes and the complexity of attacks, therefore the use of artificial intelligence (AI) and machine learning technologies is becoming more and more relevant. AI-based systems automatically monitor every financial transaction, detecting unusual or risky actions in real time, allowing you to instantly block suspicious transactions. Machine learning is used to build models that analyze user behavior and detect deviations from normal patterns, allowing fraud and money laundering to be detected. Such systems help in the fight against phishing, forged payment documents and illegal transactions.

Intelligent algorithms are able to predict the probability of financial threats, based on historical data and current trends. This creates a basis for strategic risk management and allows forecasting of financial risks. AI is used to analyze logs, network traffic and user behavior, which allows for faster detection of hacking attempts and information leaks. The use of adaptive protection systems increases the reliability of saving personal and official data and contributes to the cyber protection of financial data. Artificial intelligence helps monitor compliance with regulatory and legal requirements in financial activities. This simplifies internal audits and reduces the risk of human error and automation of compliance and auditing. The main advantages of using AI-based systems include: increasing the accuracy of fraud detection; reduction of response time to incidents; reduction of financial losses; improving trust in financial transactions; the possibility of working with large volumes of data. At that time, it is necessary to note the main challenges of implementation AI-based systems, namely: the need for high-quality training datasets; the risk of false positives; high cost of developing and supporting AI solutions; the need to comply with legal requirements for the protection of personal data. Based on the results of a retrospective analysis of literary sources, the following research areas of AI-based systems were identified, namely:

- AI has already become the standard in financial fraud management. 2025 surveys and industry overviews record that most financial institutions are already using AI for fraud detection, AML/sanctions checks and transaction monitoring. Emphasis is on the transition from static rules to models that learn from streaming data, reducing false positives and speeding up response (Feedzai, 2025; Threatmark, 2025; IBM, 2025).

- Threats evolve thanks to "offensive AI" (deepfakes, generative content, automated phishing). European reports for 2024-2025 highlight the massive use of AI by criminals for phishing, defrauding payment systems and bypassing anti-fraud controls. This directly affects online payments, public procurement and internal financial processes of state bodies (Europol, 2024).

- The global context of risks: geopolitics + the growing complexity of the landscape. The WEF-2025 reviews note the overall complexity of cyberspace and the need for a systemic approach to cyber resilience, where AI is a key element of detection/response in the financial sector (World Economic Forum, 2025).

- Practical cases and platforms. The market is booming with AI solutions for AML/fraud (real-time, graph models, behavioral analysis). For the public sector, this means the possibility of connecting modules to financial systems (budget payments, treasury operations, purchases) for the purpose of fraud prevention.

- AI Risk Management Standards and Guidance. In the deployment of public AI solutions, it is critical to adhere to the risk management framework (NIST AI RMF 1.0): transparency, reliability, manageability, auditability of models, as well as compliance with cybersecurity and privacy requirements (National Institute of Standards and Technology, 2023a, 2023b).

- Effect and metrics. Industry reviews and materials from business practices note a significant increase in the effectiveness of fraud detection and prevention thanks to AI (reduction of false positives, faster decision-making). For state bodies, this translates into smaller budget losses and more prompt blocking of risk payments (BusinessInsider, 2025).

The implementation of artificial intelligence technologies in the financial and economic activities of the Ministry of Internal Affairs has a number of applied directions that determine the priorities of digital transformation. The primary areas of application are: automated monitoring of payments and contracts (in particular, public procurement), detection of anomalies in registers of payments, business trips and wages, verification of counterparties in accordance with Know Your Business/Know Your Customer (KYB/KYC) procedures, as well as anti-fraud mechanisms for business cards and cash transactions. The technical focus of the implementation is focused on the application of flow analytics, graph models for the detection of hidden connections, the construction of behavioral profiles of users and suppliers, the use of anomaly detection algorithms, as well as deepfake content detectors in order to protect payment processes and communications. The operational model of functioning involves the combination of incident monitoring and response centers (SOC analytics) with a financial control system in the human-in-the-loop format, which provides the possibility of escalation of complex cases. Regular retraining of models, support of catalogs and registers of signs of fraud, as well as standardized response scenarios (playbooks) are integrated into it. Aspects of governance and compliance cover the formation of data management policies (quality assurance, access and logging), compliance with NIST AI RMF recommendations, audit of training data, control and reduction of the influence of model biases, as well as ensuring the explainability of decisions for the needs of lawyers and auditors. The key indicators of success are the speed of blocking suspicious transactions, reducing the frequency of false positives, the amount of averted financial losses, reducing the time of investigation of incidents, as well as expanding the coverage of risk scenarios. Analysis of modern publications allows us to single out a number of key barriers and risks accompanying the use of artificial intelligence technologies in the field of financial and economic security of state institutions. Above all, data quality and manageability remain a critical constraint to scaling AI-based anti-fraud systems in the public sector, as evidenced by research from leading analytics platforms such as Feedzai. The second major challenge is adapting to the growing wave of offensive-AI — the use of generative models by attackers to create deepfake voices and videos, as well as falsified content for the purpose of invoice fraud. Countering these threats requires specialized detectors and an established mechanism for constant exchange of indicators of compromise between law enforcement agencies, which is emphasized in Europol reports. Special attention needs to be paid to regulatory and ethical compliance, which includes the introduction of internal processes for assessing the impact of AI systems, keeping decision-making logs, as well as mechanisms for challenging automated decisions. These aspects are consistent with NIST's recommendations for artificial intelligence risk management. Considering the above, the author proposes a "Pilot system for detecting and blocking cyber threats in the financial sector using AI/ML". The purpose of this project is to deploy and test in production conditions an AI-based system for detecting anomalies and fraud in operations with state payments (contractors, business trips, salaries), with integration into the existing SOC and the "human-in-the-loop" process. Expected result: reduction of risky transactions and financial losses, reduction of response time. For the implementation of the project, it is proposed to consider a rather narrow area of research, namely: monitoring and detection of anomalies in payments to contractors within one division/region (for example, procurement management). The effective application of artificial intelligence technologies reveals not only technical advantages, but also significant challenges related to risk management, compliance with ethical norms and regulatory requirements. To ensure trust and transparency in the functioning of AI-based systems, it is necessary to use internationally recognized methodologies. In particular,

the NIST AI Risk Management Framework (AI RMF) offers a comprehensive approach to risk assessment, decision logging, and model auditability.

The issue of personal data protection is of particular importance. Recommended approaches are anonymization and pseudonymization of data in training sets, which minimizes the risk of unauthorized access to sensitive information. At the same time, it is necessary to adhere to the principles of transparency (explainability), using tools such as SHAP or LIME to explain model solutions. This allows users and auditors to understand the logic of how algorithms work and reduces the risk of bias in decision-making. An important direction is the development of data retention and logging policies that must comply with local legislation on the protection of personal data (PDP). Implementation of such approaches creates a basis for compliance with ethical standards and legal requirements, as well as ensures controllability and accountability of systems.

The use of intelligent systems is of particular importance in the context of the financial security of the Ministry of Internal Affairs, where sensitive data are processed and payments are made, which depend on the stability of the functioning of the units. Artificial intelligence has significant potential to strengthen financial cyber security in the MIA system. Its integration into the processes of monitoring and protection of financial transactions will reduce the risks of fraud, increase the efficiency of response to incidents and create the basis for the formation of reliable digital security in the future.

References

1. Abramov, S., Synytsina, Y., & Manole, A. (2022). Improving the information system of the enterprise through the use of neural networks. *Philosophy, Economics and Law Review*, 2(1), 127-138. https://doi.org/10.31733/2786-491X-2022-1-127-138
2. BusinessInsider. (2025). From fighting fraud to fueling personalization, AI at scale is redefining how commerce works online. https://www.businessinsider.com/sc/how-ai-at-scale-is-shaping-the-future-of-commerce
3. Europol. (2024). *The Internet Organised Crime Threat Assessment (IOCTA) 2024*. https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024
4. Feedzai. (2025). *2025 AI trends in fraud and financial crime prevention*. https://www.feedzai.com/resource/state-of-ai/
5. IBM. (2025). AI fraud detection in banking. https://www.ibm.com/think/topics/ai-fraud-detection-in-banking
6. Milov, O., Kaspersky, O., Yevseiev, S., Milevskyi, S., Pohasii, S., Dmitriev, O., Korol, O., Tkachov, A., Stepanenko, A., Grodskyi, S., Tarasenko, D., & Aleksiyev, V. (2020). Development of the space-time structure of the methodology for modeling the behavior of antagonistic agents of the security system. *Eastern-European Journal of Enterprise Technologies*, 6(2), 30-42. https://doi.org/10.15587/1729-4061.2020.218660
7. National Institute of Standards and Technology. (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. NIST AI 100-1. https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf
8. National Institute of Standards and Technology. (2023). *Overview of the AI RMF*. https://www.nist.gov/itl/ai-risk-management-framework
9. Synytsina, Y., Kaut, O., & Fonareva, T. (2019). Intelligent decision support systems in the enterprise management process. *Infrastruktura Rynku*, 32. http://www.market-infr.od.ua/journals/2019/32_2019_ukr/32.pdf
10. Threatmark. (2025). AI fraud detection in banking: Explore insights from our latest whitepaper on artificial intelligence (AI) and fraud. https://www.threatmark.com/ai-fraud-detection-in-banking/
11. World Economic Forum. (2025). *Global Cybersecurity Outlook 2025*. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf