UDC 343.53:336.7
DOI: 10.63341/naia-chasopis/4.2025.75

Application of AI to detect anomalous transactions as a new direction in combating money laundering

Dmytro Ovsianiuk*
Analytical Department (Criminal Analysis Center)
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0000-0002-1846-4167

Andriy Okushko
PhD in Law
Cyber Police Department of the National Police of Ukraine
02093, 19 Boryspilska Str., Kyiv, Ukraine
https://orcid.org/0009-0003-3627-2489

Yevhenii Panchenko
International Police Cooperation Department of the
National Police of Ukraine
01024, 1 Akademika Bogomoltsya Str., Kyiv, Ukraine
https://orcid.org/0000-0001-5755-7457

Abstract
The aim of the study was to examine the effectiveness of applying artificial-intelligence algorithms in the financial-monitoring system. The methodology included a comparative analysis of the practices of the United States, the European Union and Ukraine, a case analysis of international financial incidents (United States, European Union, Ukraine), and an assessment of the regulatory framework. It was established that the regulatory basis for a rule-based system is enshrined in the international standards of the Financial Action Task Force and implemented in the legislation of the European Union, the United States and Ukraine, which ensures transparency of control while simultaneously reducing adaptability to new schemes. In the United States, legal norms ensure strict reporting and sanctions, yet these norms demonstrated critical gaps in rule-based monitoring. In the European Union, multi-level directives strengthened centralised supervision while preserving the problem of bureaucratic inertia. In Ukraine, cryptocurrency Anti-Money Laundering still remained limited. It was identified that in the 2024 judgments of the High Anti-Corruption Court there were recorded cases of using fractional land deals totalling more than 3.1 million dollars, as well as large-scale organised schemes that rule-based systems did not detect. The 2024 statistics (1.75 million financial reports, UAH 12.1 billion of seized

Article's History:
Received: 01.07.2025
Revised: 11.10.2025
Accepted: 25.11.2025

Suggest Citation:
Ovsianiuk, D., Okushko, A., & Panchenko, Ye. (2025). Application of AI to detect anomalous transactions as a new direction in combating money laundering. *Law Journal of the National Academy of Internal Affairs*, 15(4), 75-87. doi: 10.63341/naia-chasopis/4.2025.75.

*Corresponding author

assets) demonstrated the scale of Ukraine's Anti-Money Laundering system but revealed the need to reduce false positives and strengthen analytics. Alignment with international practice showed that the effectiveness of future anti-money-laundering solutions for Ukraine is possible only if the regulatory framework is combined with AI models that meet the requirements of the Financial Action Task Force and the European Union. The practical significance lay in applying the results by banks, regulators and law-enforcement bodies of Ukraine to reduce false positives, detect complex schemes and adapt monitoring systems to international standards

Keywords:
model explainability; federated learning; graph neural networks; graph autoencoders; reduction of false positives; cryptocurrency operations; privacy of transactional data

Introduction

Money laundering presents a significant threat to global financial stability. According to the United Nations Conference on Trade and Development (UNCTAD) (2023), significant volumes of illicit financial flows were identified in Namibia, including through customs-value manipulation and misinvoicing in external trade. Preliminary estimates cover the period 2010-2020 and show that such practices lead to substantial losses of state revenues and distort trade statistics. This underscores the need to increase the transparency of financial operations and international cooperation in countering illicit financial flows (2023). In traditional approaches, rule-based systems dominated, operating on the basis of static rules and threshold values; however, the inefficiency became evident – these systems generate large numbers of false alerts and are unable to respond in a timely manner to new and complex money-laundering schemes (Bakry *et al*., 2024). This overloads compliance units and reduces the effectiveness of monitoring, which creates the need to introduce innovative solutions based on Artificial Intelligence (AI) (Singh, 2025).

The state of scientific research shows growing interest in the application of machine-learning and deep-learning algorithms in the field of Anti-Money Laundering (AML). B. Dumitrescu *et al*. (2022) proved that anomaly-detection methods in transaction graphs provide a higher level of identification of suspicious operations in banking networks. Graph representation of data specifically makes it possible to capture hidden links between clients and transactions that remain invisible to tabular models. This confirmed a significant advantage of anomaly detection in complex multi-level schemes. The study by R.I.T. Jensen & A. Iosifidis (2023) found that the use of deep-learning algorithms can substantially reduce the number of false alarms in AML systems. The authors demonstrated that the model increases precision without a loss of recall, i.e., ensures a more balanced approach to compliance. This indicated a real possibility of optimising monitoring processes.

The integration of AI into banking analytics and regulatory compliance was also detailed in the work of S. Rana *et al*. (2025). The authors found that the use of AI systems makes it possible to increase the accuracy of identifying suspicious transactions and ensures compliance with modern regulatory requirements. The study also emphasised the economic value of introducing such technologies, as these technologies reduce the workload on financial-monitoring units and optimise banks' resources. The application of big-data analytics in the forensics of financial crimes was developed in the study by M. Purohit & H. Barot (2024). The authors showed that a data-driven-forensics approach opens new possibilities for detecting hidden patterns in financial flows. Using large data sets makes it possible to identify complex criminal structures that remain unnoticed by classical rule-based methods, thereby creating additional tools for more effective counteraction to money laundering. In the field of digital assets, protecting cryptocurrency networks is key. S. Balusamy *et al*. (2025) concluded that combining AI with blockchain technologies can significantly enhance the security of financial operations. The authors emphasised that such an approach ensures transparency of transactions while simultaneously creating an additional layer of protection in a high-risk environment.

The evolution of the Ukrainian AML framework makes a significant contribution to understanding the adaptation of the national system to European standards. In the study by A. Fortunenko *et al*. (2025), it was shown that expanding the liability of legal entities helps increase financial transparency and strengthen institutional mechanisms for countering money laundering. This has direct relevance for the integration of innovative approaches, including AI, because effective application of technologies is only possible with a robust legal foundation. The work of S. Kalabukhova (2025) emphasised that systematic collection and processing of information is a key factor in the effectiveness of analytical activity in the field of financial intelligence, enabling the timely detection of hidden schemes and minimising errors in law enforcement. This conclusion has universal significance, as it demonstrates that effective implementation of technologies (including AI) is possible only under conditions of a clearly structured analytical process.

A similar position is held by D. Ovsianiuk (2024), who noted that the clear structuring of stages – from the collection and verification of information to its interpretation and use in decision-making – is a key factor in the effectiveness of analytics. Such an approach

allows hidden schemes to be detected in a timely manner, reduces the risk of errors in law enforcement, and increases the overall effectiveness of combating financial crimes. The opportunities and challenges of implementing AI in Ukraine's banking sector became the subject of analysis in the work of N. Horobets *et al*. (2025). The authors showed that the use of AI can significantly reduce the level of false alerts in transaction-monitoring processes while simultaneously requiring compliance with the General Data Protection Regulation (GDPR)[1] and the AI Act[2], which defined the conditions for effective integration of technologies into the national AML system. However, a significant part of the research focused on the technical aspects of anomaly detection, while less attention was paid to issues of model explainability and the legal legitimacy in judicial and regulatory processes.

Secondly, existing studies were mainly focused on the international context, whereas the Ukrainian experience was covered fragmentarily and required systematic analysis. The issue of integrating innovative approaches into already existing rule-based systems, which still dominate financial institutions, also remained insufficiently developed. Therefore, the aim of the study was the theoretical assessment of the effectiveness of artificial-intelligence algorithms for improving the accuracy and adaptability of the detection of financial offences. The research hypothesis was that artificial-intelligence algorithms, in particular anomaly-detection methods of machine learning, allow the detection of suspicious financial transactions with higher accuracy than rule-based systems, especially in the presence of complex patterns or atypical behaviour.

Materials and Methods

The study covered an analysis of traditional rule-based systems and international practices and outlined areas for adapting the Ukrainian system to international practices. The choice of countries was determined by the fact that the United States had leading experience in applying rule-based and AI approaches, the EU formed supranational standards and ethical requirements, and Ukraine was adapting these practices in the process of European integration. This made it possible to identify both common features and challenges relevant for the further harmonisation of Ukrainian practice with international approaches.

Traditional rule-based systems were presented in order to assess the advantages of static rules for regulators and auditors (simplicity, transparency) and to identify the limitations. Rule-based systems were chosen as the baseline because these systems were enshrined in laws and standards and were simple to apply. To confirm the limitations, the method of case analysis of international – COVID-19 relief fraud and AML Bitcoin fraud (United States) (U.S. Department of Justice, Office of Public Affairs, 2025a; U.S. Department of Justice, Office of Public Affairs, 2025b), TD Bank money laundering (United States) (FinCEN, 2024), fake-art money laundering (EU) (Eurojust, 2024) – and Ukrainian examples of money-laundering and fraud schemes (National Police of Ukraine, 2023; 2024; National Police of Ukraine – Zaporizhzhia Region, 2025) was applied to demonstrate practical incidents of rule-based approaches (the sources used were official publications of U.S. state bodies reflecting court judgments and plea agreements with fines (TD Bank). Full court decisions were available only via the PACER system, therefore open official releases were used. The fake-art money-laundering case (EU) was at the indictment stage; final court decisions were not publicly available, therefore an official Eurojust (2024) press release was used).

The method of systematisation and comparison of practices of using AI methods based on academic research was also applied; Explainable AI was analysed for decision transparency, graph and generative models were analysed for detecting hidden schemes and reducing false positives, and simulation environments were used for testing algorithms. The task of this stage was to show the limitations of traditional rules and to prove the feasibility of integrating AI solutions into national AML frameworks.

A method of comparative analysis of the AML systems of the EU, the United States and Ukraine was applied, which provided for a structured comparison of key aspects: legislation, supervisory authorities, reporting mechanisms, regulation of cryptocurrencies, sanctions, ethical dimensions and international cooperation. This made it possible to assess the degree of harmonisation with the standards of the Financial Action Task Force (FATF) and to identify the strengths and weaknesses of each jurisdiction: EU regulatory framework, European Banking Authority, United States, Ukraine, international legal standard.

Results and Discussion

Limitations of traditional rule-based systems and the potential of AI in the AML. Traditional rule-based systems in the sphere of combating money laundering are financial-monitoring algorithms that function on the basis of predefined rules and threshold values, for example limits on the amount or frequency of transactions. The advantage lies in the simplicity of implementation and comprehensibility for regulators and auditors. Such approaches are expressly enshrined in international and national standards, in the

[1] General Data Protection Regulation. (2016, April). Retrieved from https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en?utm_source=.
[2] Regulation of the European Parliament and of the Council No. 2024/1689 "On Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)". (2024, August). Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1689/oj.

Law of Ukraine No. 361-IX[1], in the United States – the Bank Secrecy Act[2], the USA Patriot Act[3], the Anti-Money Laundering Act of 2020[4], and in the EU –Directive No. 2015/849[5], and No. 2018/843[6].

Directive No. 2018/1673[7], as well as in the FATF (2025) recommendations. The advantage is the simplicity of implementation and interpretation, which makes rule-based solutions convenient for regulators and auditors. At the same time, the limitation of such an approach is manifested in weak sensitivity to new and complex patterns. An example is the TD Bank case in the United States, where the system missed about 92% of transactions amounting to $18.3 trillion, which became the basis for regulatory measures. In October 2024, TD Bank N.A., together with its parent company TD Bank US Holding Company, was subjected to investigation due to violations of the Bank Secrecy Act[8] and systemic shortcomings in combating money laundering. Between 2018 and 2024, a bank client carried out more than $470 million in illegal transactions through bank branches, using large cash deposits and wire transfers that were not properly identified by employees.

In addition, five bank employees conspired with criminal organisations to open accounts used to launder $39 million to Colombia, including proceeds from drug trafficking. As a result of the incident, TD Bank agreed to multibillion-dollar fines, asset restrictions, the appointment of an independent monitor, and the strengthening of internal controls and anti-money-laundering staff. This case underscores the critical need to comply with anti-money-laundering standards and effective internal controls, since the violation leads to financial and reputational risks (FinCEn, 2024). This indicates that the static nature of rule-based systems creates critical gaps in adapting to new schemes.

In contrast to static rules, AI methods are based on machine learning and are capable of detecting complex multi-level patterns in financial data. The use of Explainable AI in the AML sphere is necessary to ensure the legitimacy of such systems in courts and to build public trust. Regulators emphasise that automated decisions must be justified; otherwise, there is a risk of legal challenges. The processing of transactional data simultaneously creates privacy risks, particularly in the EU, where the GDPR applies. One promising approach is federated learning, which makes it possible to train models without transferring raw data, preserving clients' privacy (Konstantinidis & Gegov, 2024). AI tools significantly outperform traditional rule-based systems in accuracy and adaptability, particularly in detecting complex money-laundering schemes through cryptocurrencies. Algorithms are capable not only of detecting anomalous transactional flows, but also of recognising hidden schemes that remain invisible to classical methods. This increases the effectiveness of AML systems, reduces the risk of erroneous decisions, and ensures greater sensitivity to new types of financial abuse (Altman *et al*., 2023). Algorithms based on graph neural networks demonstrate significant effectiveness in detecting complex transactional links that remain unnoticed by traditional rule-based systems. These models have shown the ability to identify hidden relationships between different participants in financial networks and to detect potential beneficiaries. This underscores the promise of applying graph methods in the development of hybrid AML systems that combine technological accuracy with requirements for legal substantiation (Wójcik, 2024).

To evaluate the effectiveness of anti-money-laundering algorithms, studies use a specialised multi-agent simulator that models the full laundering cycle: from the placement of funds obtained from various types of criminal activity to the layering and integration into the legal economy. The environment reproduces transactions between different participants (banks, companies, private individuals) and allows algorithms to be tested on controlled examples. Its value lies in the ability to reproduce typical laundering schemes (for example, cycles or branching) while preserving the full confidentiality of real client data. This contributes to the development of more accurate and adaptive AI systems in the AML sphere, particularly in terms of cross-border transactions and scenarios that are difficult to trace by classical methods (Johannessen & Jullum, 2023). Indicative is the example of using graph-based generative models, which have demonstrated the ability

[1] Law of Ukraine No. 361-IX "On Prevention and Counteraction to Legalisation (Laundering) of the Proceeds of Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction". (2019, December). Retrieved from https://zakon.rada.gov.ua/laws/show/361-20?utm_source= #Text.

[2] Bank Secrecy Act of USA. (1970, October). Retrieved from https://www.govinfo.gov/content/pkg/USCODE-2022-title31/pdf/USCODE-2022-title31-subtitleIV-chap53-subchapII.pdf?utm_source=.

[3] USA Patriot Act. (2001, October). Retrieved from https://www.congress.gov/bill/107th-congress/house-bill/3162/text?utm_source=.

[4] Anti-Money Laundering Act of USA. (2020, April). Retrieved from https://www.congress.gov/bill/116th-congress/house-bill/6395/text?utm_source=.

[5] Directive of the European Parliament and of the Council No. 2015/849 "On the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing". (2015, May). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L0849&utm_source=.

[6] Directive of the European Parliament and of the Council No. 2018/843 Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing. (2018, May). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843&utm_source=.

[7] Directive of the European Parliament and of the Council No. 2018/1673 "On Combating Money Laundering by Criminal Law". (2018, October). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L1673&utm_source=.

[8] Bank Secrecy Act of USA. (1970, October). Retrieved from https://www.govinfo.gov/content/pkg/USCODE-2022-title31/pdf/USCODE-2022-title31-subtitleIV-chap53-subchapII.pdf?utm_source=.

simultaneously to reduce the number of false positives and to maintain high sensitivity to truly suspicious operations. This conceptually confirms the advantage of intelligent methods over exclusively rule-based monitoring, especially in scenarios with multistep and complex transactional schemes (Karthikeyan & Bhowmik, 2025).

Although AI methods require high-quality data and create challenges in terms of explainability and privacy, such methods form the foundation of modern AML systems. These methods outperform rule-based solutions in accuracy, adaptability, and the ability to detect new and complex schemes. Rule-based systems may remain a basic filter for obvious anomalies (for example, large cash transfers), but the static nature and narrow range make these systems insufficient as the primary tool. In contrast, AI approaches are capable of working with large and heterogeneous data, considering the dynamics of transactional flows and increasing the reliability of law-enforcement practice in the sphere of combating money laundering. Although rule-based systems for combating money laundering formally comply with international standards, the practical application demonstrates a number of significant limitations. Such systems are capable mainly of identifying obvious anomalies; however, the static nature makes timely responses to complex, multi-level and cross-border schemes impossible. This is confirmed by examples from international practice, where significant financial crimes remained without proper control, summarised in Table 1.

Table 1. Empirical analysis of cases of limitations of rule-based approaches in AML and the imperative to use AI

Case	Description	Failure of rule-based approaches	Need for AI analytics
COVID-19 relief fraud (USA)	More than $11 million illegally obtained as loans under the Paycheck Protection Program (PPP). Funds were laundered through real estate (25 properties), gambling and other assets. Sentence: 15+ years' imprisonment, confiscation	Rule-based document checks did not detect forgeries and inflated indicators; these checks did not track anomalous behaviour after receiving funds	AI is able to analyse large data sets, detect falsified documents and hidden transactional networks, reducing the risks of abuse in state programmes
AML Bitcoin fraud (USA)	The fraudulent cryptocurrency scheme caused $10 million in losses to investors, $2 million of which were laundered through real estate and personal expenses. Sentence: 7 years' imprisonment	Rule-based systems did not recognise false statements and did not detect patterns of transactions in cryptocurrency	AI can identify anomalous crypto-transactions and fraudulent networks, strengthening legal mechanisms for protecting investors in digital assets
Fake art money laundering (EU)	More than 2,000 counterfeit works of art seized, 38 persons arrested. Potential losses – €200 million. The scheme covered Belgium, France, Italy, and Spain	Rule-based approaches failed to detect cross-border schemes and to verify the authenticity of works	AI enables the tracking of cross-border networks and anomalies in the art market, ensuring more effective legal oversight and reducing the risks of trade in forgeries.
TD Bank money laundering (USA)	TD Bank found guilty of large-scale AML violations: $3 billion in fines, $470 million laundered through branches. 92% of transactions (totalling $18.3 trillion) remained outside monitoring	Use of outdated systems (10 years without updates), lack of control of large deposits and transfers, systemic deficits in financial monitoring	AI is able to monitor large volumes of transactions in real time and detect complex schemes, reducing legal risks for banks and increasing trust in the financial system
Money laundering through resale of securities (Ukraine) (National Police of Ukraine, 2024)	Activities of an organised group that legalised more than UAH 1 billion through fictitious operations with the resale of securities on the stock exchange	Traditional systems perceived transactions as lawful because documents formally met the requirements, and did not detect cyclical resales between the same participants	AI can analyse the intensity of transactions and hidden links between companies, detecting anomalous cycles of resale
Money laundering via VAT-refund schemes (Ukraine) (National Police of Ukraine – Zaporizhzhia Region, 2025)	Criminal activity of enterprises which, through fictitious employment of persons with disabilities, illegally obtained tax benefits and formed an inflated tax credit. This made it possible to file declarations with unlawful VAT-refund amounts of more than UAH 200 million	Rule-based approaches did not detect systematic features in tax declarations and fictitious use of benefits, which allowed abuse of the VAT-refund mechanism	AI for early detection of suspicious flows and building risk profiles
Cryptocurrency fraud totalling more than UAH 3.5 million (Ukraine)[1]	Illegal misappropriation of cryptocurrency in the amount of more than UAH 3.5 million. The obtained digital assets were transferred to personal wallets on the blockchain and then partially converted into cash. The scheme was built using online platforms for trading virtual assets and subsequent "laundering" through exchangers	Traditional banking and tax systems did not track transactions on the blockchain, which made timely response to fraudulent actions impossible	AI algorithms of graph analysis make it possible to identify suspicious wallets, trace chains of cryptocurrency transactions and form an evidentiary base for criminal proceedings

Sources: compiled by the authors based on the FinCEN (2024), Eurojust (2024), U.S. Department of Justice, Office of Public Affairs (2025a; 2025b)

[1] Directive of the European Parliament and of the Council No. 2015/849 "On the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing". (2015, May). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L0849&utm_source=.

Rule-based approaches, despite the formal compliance with international standards, demonstrate serious limitations in practical application. These approaches do not ensure an adequate response to complex, multi-level and cross-border money-laundering schemes, which creates risks for both public finances and private investors. In this context, the use of AI is not only a technological innovation but also a necessary condition for strengthening the legal system of combating money laundering. AI algorithms are capable of forming an evidentiary base for judicial processes, increasing the transparency of the financial sector, reducing the risks of appeals against decisions and strengthening trust in regulatory institutions. The expediency of implementing AI in AML systems is determined not so much by technological advantages as by legal, practical and economic necessity: to ensure compliance with legislative requirements, to increase the effectiveness of law enforcement and to protect the financial stability of the state.

The results of the study demonstrated that rule-based systems generate a significant volume of false-positive alerts, which leads to the blocking of legitimate clients. This correlated with the work of A.N. Bakry *et al*. (2024), who proved that automated ML solutions are capable of reducing the number of false positives due to adaptive signal suppression. The comparison revealed similarity in detecting multi-level money-laundering schemes that remained unnoticed by traditional rule-based systems. The comparison of results shows a common trend: rule-based systems are limited in detecting complex and multi-level money-laundering schemes, whereas AI algorithms have a significantly higher potential for the identification. The results of the study also revealed that AI approaches significantly outperform rule-based systems in detecting multi-level money-laundering schemes. At the same time, such approaches do not completely eliminate the problem of false positives, which creates a risk of blocking legitimate clients and legal consequences for banks. This corresponded to the conclusions of the study by Y. Chen *et al*. (2025), which confirmed the effectiveness of AI in the sphere of cryptocurrency transactions. The authors emphasised that combining different methods ensures higher accuracy and legal reliability, which meant that rule-based approaches are insufficient, whereas AI forms the foundation of modern 21st-century AML systems.

The study by E.J. Reite *et al*. (2025) showed that the application of AI in classifying clients by risk level makes it possible to reduce the number of false positives while simultaneously increasing the detection of suspicious transactions. Such an approach makes monitoring more effective and directs resources to truly dangerous categories of clients. The obtained results correlate with the conclusions of the current study that AI approaches outperform rule-based systems in accuracy and adaptability, as well as the ability of AI to work with large data sets and to detect hidden financial networks. This confirms that risk-oriented classification is a key tool for increasing the effectiveness of AML systems.

The results of the study confirmed that rule-based systems can be used only as a basic filter, since the low sensitivity makes these sytems insufficient in the fight against complex money-laundering schemes. In contrast, AI approaches demonstrated the ability to reduce false positives, adapt to the dynamics of transactions and meet the requirements of regulators. Similar conclusions are presented in the work of V. Singh (2025), where machine learning is considered as a tool for optimising AML policies, capable of combining technological efficiency and legal compliance with regulatory requirements. The study by H. Gandhi *et al*. (2024) also confirmed these trends, drawing attention to the advantages of AI/ML in combating complex schemes, particularly in the sphere of cryptocurrency transactions. At the same time, the authors emphasised the challenges of explainability and privacy protection, which remain critical for the legal legitimacy of such solutions. Taken together, this confirms that the development of AML systems is inseparable from the implementation of AI, since it is AI that ensures the balance between detection accuracy, protection of clients' rights and compliance with standards. Thus, despite regulatory embeddedness and ease of use, rule-based systems remain overly static and are characterised by a high level of false-positive alerts. In contrast, AI approaches provide significant accuracy, the ability to detect multi-level schemes and a reduction in erroneous signals.

International standards of the Financial Action Task Force (FATF) and the features of implementation in Ukrainian legislation. The FATF (2025) recommendations are the global standard for combating money laundering and terrorist financing. These Recommendations do not have direct legal force, but each jurisdiction implements the recommendations in its own laws and regulations. These standards are focused on cryptocurrencies and VASPs, as well as on the control of anonymous wallets and rapid transactions. The FATF carries out peer reviews and applies the tools of "grey" and "black lists", which forces countries to improve the AML legislation. The FATF acts as a "matrix", and the EU, the United States and Ukraine implement these standards in the own laws, supervisory bodies and practical cases.

Cryptocurrency transactions combine publicity and anonymity: all operations are stored in an open register, yet wallet owners remain pseudo-anonymous. This creates conditions for the legalisation of proceeds, since large transfers can be hidden among millions of small transactions. The FATF separately emphasised the risks associated with anonymous wallets and high-speed transactions and obliged countries to strengthen the regulation of VASPs. The EU, the United States and Ukraine form three different approaches to

AML/CTF regulation that combine the FATF international standards with national specificities. The study of these models makes it possible to evaluate the effectiveness of centralised and decentralised supervision, the scale of sanctions and the readiness to respond to new challenges, particularly in the sphere of cryptocurrencies.

In the EU, the key act is Directive No. 2015/849[1], which establishes the foundations for combating money laundering and terrorist financing. Article 30 provides for the creation of registers of beneficial owners; however, practice has shown fragmentation of approaches in different Member States, which complicates cross-border access to data. Amendments introduced by Directive No. 2018/843[2] expanded the list of obliged entities, including providers of services for virtual assets (VASPs), but at the same time created a risk of bureaucratisation and excessive burden on small businesses. In addition, Directive (EU) 2018/1673[3] criminalised money laundering at the Union level but left room for divergent interpretations of sanctions among Member States. The European Banking Authority (2025), noted that the lack of harmonisation in supervision creates "regulatory arbitrage".

In the United States, the main problem is the archaic nature of certain provisions of the Bank Secrecy Act of USA[4]. In particular, section 5313 requires mandatory reports on transactions over $10,000, which, in the modern conditions of the 21st century, leads to an excessive volume of reports without increasing the effectiveness of the fight against ML. The amendments of Money Laundering Control Act[5] and the Patriot Act[6], Title III significantly expanded FinCEN's powers, but the broad interpretation became the subject of criticism due to the risk of excessive interference with privacy. Even the Anti-Money Laundering Act[7], which introduced requirements for beneficial-ownership reporting, was partially revised by FinCEN (2025), raising doubts about compliance with FATF Recommendation 24 (FinCEN, 2025). As a result, the system is characterised by an overload of SAR reports and inconsistent approaches to the regulation of cryptocurrencies.

In Ukraine, the basis is the Law No. 361-IX[8], which implemented the FATF standards. At the same time, Article 209 of the Criminal Code of Ukraine[9] contains wording that allows the avoidance of criminal liability when intent is not proven, and the 2025 amendments only partially eliminated this gap. Cabinet of Ministers Resolutions No. 692[10] and No. 800[11] detailed the reporting procedure, but in practice led to excessive regulation and a conflict between state and banking procedures. The State Financial Monitoring Service of Ukraine (2023), in methodological recommendations, focused on new threats (in particular modern forms of slavery), yet the sphere of cryptocurrencies remains under insufficient control, which contradicts FATF (2025) Recommendation 15. Even positive steps, such as the introduction of corporate criminal liability provided for in legislative initiatives formed on the basis of the analytical conclusions of the State Financial Monitoring Service of Ukraine (2025), indicate the gradual evolution of the national system of combating money laundering towards alignment with FATF standards.

Although the FATF Recommendations set a unified international standard, the implementation demonstrates significant legal challenges. In the EU, the problem remains fragmentation and the lack of full harmonisation, which creates room for "regulatory arbitrage". In the United States, the system suffers from outdated

[1] Directive of the European Parliament and of the Council No. 2015/849 "On the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing". (2015, May). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L0849&utm_source=.

[2] Directive of the European Parliament and of the Council No. 2018/843 Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing. (2018, May). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843&utm_source=.

[3] Directive of the European Parliament and of the Council No. 2018/1673 "On Combating Money Laundering by Criminal Law". (2018, October). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L1673&utm_source=.

[4] Bank Secrecy Act of USA. (1970, October). Retrieved from https://www.govinfo.gov/content/pkg/USCODE-2022-title31/pdf/USCODE-2022-title31-subtitleIV-chap53-subchapII.pdf?utm_source=.

[5] Money Laundering Control Act of USA. (1986, October). Retrieved from https://www.govinfo.gov/content/pkg/STATUTE-100/pdf/STATUTE-100-Pg3207.pdf?utm_source=.

[6] USA Patriot Act. (2001, October). Retrieved from https://www.congress.gov/bill/107th-congress/house-bill/3162/text?utm_source=.

[7] Anti-Money Laundering Act of USA. (2020, April). Retrieved from https://www.congress.gov/bill/116th-congress/house-bill/6395/text?utm_source=.

[8] Law of Ukraine No. 361-IX "On Prevention and Counteraction to Legalisation (Laundering) of the Proceeds of Crime, Financing of Terrorism and Financing of Proliferation of Weapons of Mass Destruction". (2019, December). Retrieved from https://zakon.rada.gov.ua/laws/show/361-20?utm_source= #Text.

[9] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14?utm_source=#Text.

[10] Resolution of the Cabinet of Ministers of Ukraine No. 692 "On the Approving the Procedure for the Preparation and Publication of the Comprehensive Administrative Reporting in the Field of Prevention and Counteraction to Legalisation (Laundering) of Proceeds from Crime, Financing of Terrorism, and Financing of Proliferation of Weapons of Mass Destruction". (2020, August). Retrieved from https://www.kmu.gov.ua/npas/pro-zatverdzhennya-poryadku-formuvannya-ta-oprilyudnennya-kompleksnoyi-administrativnoyi-zvitnosti-u-t50820?utm_source=.

[11] Resolution of the Cabinet of Ministers of Ukraine No. 800 "On Amendments to the Methodology for Determining the Amount of Damage Resulting from Unauthorized Occupation of Land Plots, use of Land Not for its Intended Purpose, and Removal of the Fertile Soil Layer". (2020, September). Retrieved from https://surl.li/susukg.

norms and an overload of SAR reports, which reduces the effectiveness of monitoring and increases the risks of excessive interference with privacy. In Ukraine, the key challenge is combining the requirements of the FATF and EU directives with the realities of national financial supervision and the level of development of the virtual-assets market. This indicates that formal compliance with international standards does not guarantee practical effectiveness without taking into account legal and technological constraints. In addition, in Ukraine there is no holistic regulation in the sphere of financial monitoring of digital assets – most current norms are scattered among various laws and by-laws, which complicates the application and creates gaps in law enforcement. There was an attempt to adopt an appropriate law that would regulate this sphere, but the issue has not yet been resolved.

Cryptocurrency has become one of the key risk zones for AML systems. Its specificity lies in the combination of the publicity of the blockchain and the pseudo-anonymity of wallet owners, which complicates the identification of ultimate beneficiaries. Traditional rule-based methods have proved insufficient, as these methods do not take into account complex transactional structures, in particular layering and smurfing. Instead, modern 21st century approaches have proved effective in detecting hidden links and atypical flows of assets. In the EU, the main challenge remains the fragmentation of law and uneven supervision, which creates "regulatory arbitrage" and complicates cross-border interaction. In the United States, the problem lies in the overload of SAR reports and the archaic nature of norms, which generates large volumes of formal reporting without real improvement in effectiveness and increases the risk of legal challenges. In Ukraine, despite active cooperation with the FATF and the conclusion of new international memoranda, there are resource constraints and the complexity of harmonising the national system with European requirements, which exacerbates risks in the cryptocurrency segment. Under these conditions, the integration of AI solutions appears not so much as a technological innovation as a legal and practical necessity: algorithms make it possible to reduce the number of false alerts, ensure the transparency of decisions (critical for courts and regulators), strengthen trust in the financial sector and reduce economic costs of monitoring. It is precisely the combination of regulatory clarity and intelligent technologies that is the key factor in increasing AML effectiveness on a global scale. Table 2 presents a comparative analysis of key AML/FT reporting indicators for 2024. The data presented included statistical indicators, the results of analytical work, international areas of cooperation and the ethical challenges of using AI.

Table 2. AML/FT reporting and ethical requirements for AI in the EU, USA, and Ukraine

Indicator	EU	USA	Ukraine
Statistics (number of Suspicious Transaction/ Activity Reports (STR/ SAR)	70% of competent authorities record high/increasing ML/TF risks in FinTech, 2.5× growth in the number of authorised CASP (2022-2024), 61% of violations are related to CDD shortcomings	4.7 million SARs, 20.5 million CTRs, 152,100 CMIRs, 1.7 million FBARs (daily averages: SAR ~12,870, CTR ~56,160)	In 2024, 1,754,604 reports were received, of which 1,750,940 were registered. From banks, 1,736,196 reports were registered; from non-bank institutions 14,467 electronic and 277 paper reports. Distribution of registered reports: threshold – 82.26% (1,440,319), suspicious (activity) – 17.58% (307,828), tracking requests – 0.14% (2,648). Case reports on suspicious transactions (activity) for 2024 – 208,852, the share of banks among reports that were registered – 99.2% (State Financial Monitoring Service of Ukraine, 2025)
Analytical materials/ proceedings	2,666 active investigations (+38% y/y) with an estimated harm of €24.8 billion; 1,504 newly opened, 205 indictments (+47%), €849 million of assets frozen	818 requests; ~58,628 positive responses, ~13,660 participating institutions; 6,503 subjects. 314(b): 6,100+ registered institutions; 48,223 SARs with a reference to 314(b); 1,693 institutions mentioned 314(b) in SARs; 62 SARs on terrorism. Access to BSA: 2.3 million searches, 432 agencies; 12,000+ users	1,053 generalised materials prepared and sent (amount of suspicions UAH 62.6 billion). Use of GM by law enforcement: 69 criminal proceedings initiated, GM used in 336 CP (346 GM), 90 CP completed; 39 cases considered by the court. Value of seized and frozen assets – UAH 12.1 billion
International programmes/exchanges	The EBA notes increased supervisory actions (off-site / on-site) in most sectors; improvement of residual risk in banking/market sectors; but weak controls in payment institutions and among new CASP	Rapid Response Program (RRP) FY24: 518 requests, $82.6 million returned to victims; $126.4 million (46%) frozen in FY24 (over $1.5 billion since 2015). Egmont exchanges: 972 incoming requests, 863 responses, 452 outgoing requests; 1,028 incoming and 212 outgoing spontaneous disclosures	4 Memoranda of Understanding (MoU) in 2024 with Norway, Germany, Gibraltar, Jersey; a total of 85 MoU since 2003

Table 2, Continued

Indicator	EU	USA	Ukraine
Ethical aspects of AI application	False positives: possible false alerts in FinTech, explainability: algorithms must be transparent to regulators, privacy: compliance with the GDPR when processing personal data	False positives: daily SARs (~12,870) may create false suspicions, explainability: the need for explanations of decisions for regulators and courts, privacy: compliance with the BSA and national privacy laws	False positives: 17.58% of suspicious transactions out of 1.75 million reports may be false, explainability: AI decisions must be understandable to law enforcement and the court, privacy: compliance with Ukrainian legislation on the protection of personal data

Note: the 314(b) programme is a voluntary mechanism in the USA that allows banks and financial institutions to exchange information about suspicious transactions to combat money laundering and terrorism
Sources: compiled by the authors on the basis of the European Banking Authority (2025), Financial Action Task Force (2025), State Financial Monitoring Service of Ukraine (2025), Financial Crimes Enforcement Network (FinCEN) (2025)

Effective combat against transnational crimes, particularly in the sphere of drug trafficking, largely depends on international information exchange and the harmonisation of legal frameworks between jurisdictions, which corresponds to approaches to AML/FT regulation where interaction between national financial intelligences and international partners is a determining factor of effectiveness (Ovsianiuk & Ustymenko, 2024). The combination of international practice and FATF standards outlines the key directions for improving the national system of combating money laundering and terrorist financing in Ukraine. First and foremost, it is essential to update the regulatory and legal framework and the methodological recommendations of the State Financial Monitoring Service to include provisions on the use of artificial intelligence for real-time transaction monitoring. The experience of the USA and the EU shows that the introduction of hybrid systems (rule-based + AI) makes it possible to reduce the level of false positives, which directly improves the legal quality of financial supervision. A separate legal direction is the development of public-private partnerships in the sphere of crypto-AML, where the NBU, the SFMS and banks can use AI tools to analyse blockchain transactions, following the example of US practice. This complies with FATF requirements regarding the regulation of VASP and helps to eliminate gaps in the control of anonymous wallets.

No less important is the integration of ethical and legal standards: the adaptation of GDPR[1] principles into the national legislation of Ukraine, the development of federated-learning practice to minimise the risks of personal-data leakage, as well as the enshrining of explainable-AI requirements for the legitimacy of the evidentiary base in judicial proceedings. Institutional development also acquires strategic significance: investment in digital infrastructure, the creation of regulatory frameworks for grant funding of technologies and staff training at the NBU. This will ensure legal certainty in the AML sphere, remove Ukraine from the "grey zones" of international rankings and accelerate its integration into the European financial-legal area.

The results of the study showed that rule-based solutions can be applied only as a basic level of control, whereas AI methods should become the core of AML systems, capable of ensuring higher accuracy and adaptability. This corresponded to the conclusions of N. Pocher *et al*. (2023), who investigated the detection of anomalous cryptocurrency transactions in the context of AML/CFT. The authors emphasised that static rule-based approaches cannot ensure adequate legal protection in the field of cryptocurrencies, as such approaches do not detect hidden schemes in blockchain networks. Instead, the application of AI creates new opportunities for forming the evidentiary base in criminal proceedings, improves the effectiveness of law enforcement and strengthens trust in financial supervision. This underlined that AI in crypto-AML has not only technological, but also key legal significance for compliance with international standards and the protection of the financial system.

S. Wang *et al*. (2024) proposed the application of graph methods in combination with structural criteria (minimisation of structural entropy) to detect hidden links in large transactional networks. The authors showed that such an approach makes it possible to reduce the level of "noise" in data and to increase the accuracy of identifying complex money-laundering schemes, including multi-level and high-speed transactional flows.

This correlated with the results of the current study regarding the effectiveness of AI analysis in the field of financial supervision, especially where traditional rule-based approaches are insensitive. At the same time, the current study emphasised that the practical implementation of such solutions must take into account not only the technical characteristics of the algorithms, but also legal requirements. This is of key importance for the legitimacy in judicial processes and compliance practice, as well as for the protection of the rights of subjects of financial transactions.

[1] General Data Protection Regulation. (2016, April). Retrieved from https://commission.europa.eu/law/law-topic/data-protection/legal-framework-eu-data-protection_en?utm_source=.

From a legal point of view, the main challenge for AML is to find a balance between the effectiveness of monitoring and the protection of the rights of subjects, since excessive false positives lead to unlawful blockings and legal disputes, whereas low sensitivity leaves room for the avoidance of liability, as emphasised by the FATF and EU/US regulators. T. Pousette & A. Rosenda (2024) stressed that for EU and US regulators, reason codes and model traceability – which ensure transparency and the possibility of appealing decisions – are a critical condition for the acceptability of AI. This directly aligned with the results of the current study regarding FATF requirements for the accountability of financial institutions and the principles of the GDPR, which prohibit completely opaque automated decisions. This means that explainable AI becomes not only a technological, but also a legal standard in the AML sphere.

The results showed that the rule-based approach in AML generates millions of reports that overload the system and conceal real risks. This correlated with C.-H. Poon *et al.* (2025), who proved that traditional rules are unable to account for complex multi-level schemes. The authors found that LineMVGNN (a model that applies multi-graph neural networks (MVGNN) to detect money laundering by analysing several graphs to improve transaction-detection accuracy) reveals hidden transactional links that rule-based methods miss. This meant that formal threshold criteria create noise rather than effective supervision. In the legal dimension, this threatens to turn norms into "dead law" and creates a risk of legal challenges due to disproportionate monitoring. Rule-based monitoring, despite its technical limitations, ensures a proportionate approach – thanks to the predictability of rules and the clarity of legal control. By contrast, the use of AI can create risks of disproportionality, as it forms unique indicators for different monitoring contexts, which complicates the regulatory verification and potentially expands the boundaries of interference with privacy. Therefore, the integration of AI into financial-monitoring systems must be accompanied by the development of transparent explainability criteria and legal limits on use, in order to avoid criticism, legal challenges and non-compliance with FATF standards.

S.A. Ajagbe *et al*. (2025) carried out a comprehensive comparison of machine-learning algorithms for detecting money laundering in transactional data. The authors demonstrated that ensemble models significantly outperform both classical ML approaches and simple rule-based methods in terms of accuracy and stability of results. This corresponded to the current study on the problem of false positives in AML systems, which overload supervision and reduce effectiveness. The correct choice of algorithm directly affects the reduction of false positives and improves the quality of financial monitoring. This means that, in the legal sphere, the application of optimal ML models makes it possible to avoid blocking legitimate transactions and reduces the risks of legal challenges. Such an approach opens up the possibility of reducing SAR/STR overload and moving to more accurate, proportionate monitoring that complies with FATF international standards.

M. Di Gennaro *et al*. (2025) showed that temporal graph neural networks (Temporal GNN) make it possible effectively to track suspicious laundering schemes that were manifested through rapid and multi-level transactions. The researchers found that Temporal GNN can take into account the temporal dynamics of flows and detect atypical transactional patterns that remain unnoticed by static models. This was consistent with the results of the study that the main challenge in the sphere of cryptocurrencies is the risks of high-speed transfers and anonymous wallets, to which the FATF draws attention. This meant that AML solutions without the integration of temporal characteristics remain formal and are not capable of genuinely counteracting the risks of cryptocurrency markets. In the legal dimension, such an approach directly complies with the FATF Recommendation on new technologies and proves the readiness of countries to ensure not only formal, but also practical compliance with standards.

Thus, the integration of AI into regulatory frameworks, the development of public-private partnerships, compliance with ethical standards and investment in technologies form the basis for the modernisation of Ukraine's AML system. This will reduce false positives, increase monitoring effectiveness, improve the results of combating money-laundering crimes and ensure full compliance with FATF standards, contributing to European integration.

Conclusions

The results of the study confirmed the research hypothesis, proving that artificial-intelligence algorithms outperform rule-oriented systems in terms of accuracy and the ability to detect complex and atypical transactions. Traditional rule-based systems, despite compliance with FATF standards, miss significant volumes of suspicious transactions due to the static nature. In the TD Bank case (USA), 92% of transactions amounting to $18.3 trillion were not detected, including $470 million in illegal operations through cash deposits and transfers; in Ukraine in 2024, 1,754,604 reports were recorded, of which 1,730,000+ were from banking institutions, with 82.26% being threshold and only 17.58% suspicious. The implementation of AI in AML systems requires ensuring explainability for legitimacy in judicial processes and compliance with privacy standards (the GDPR, Ukrainian data-protection legislation). Rule-based systems may remain a basic filter for obvious anomalies, but these systems should be combined with AI algorithms to increase monitoring effectiveness. The introduction of such an approach will

stimulate the training or retraining of existing specialists, or the replacement with those more advanced in AI-based AML approaches.

The experience of the USA and the EU shows that hybrid systems reduce false positives and improve the legal quality of supervision. Special legislation sets the global standard, but its implementation in the EU, the USA, and Ukraine has differences. The EU suffers from fragmented supervision, the USA – from outdated norms and SAR-report overload, Ukraine – from resource constraints and insufficient control of cryptocurrencies. This underlines the need to harmonise legislation and to implement AI to increase effectiveness. At the same time, the application of AI in AML is accompanied by risks and limitations. The main ones are the problem of decision explainability, which may complicate the use as evidence in courts, and privacy risks in connection with GDPR requirements. The effectiveness of models depends on data quality, and residual false positives, although reduced, still create a burden for banks. A challenge is also the high computational cost and the risk of concentration of control among a few technology providers. To improve the AML system, Ukraine should update the regulatory framework with AI in mind, develop partnerships for blockchain analysis, adapt GDPR principles and invest in infrastructure and personnel. This will reduce risks, strengthen trust and promote the European integration of the financial sector.

A limitation of the study was the dependence of model effectiveness on the volume and quality of input data, as well as the complexity of practical implementation in financial institutions due to high cost and the need for specialised personnel. Further research should focus on combining different types of AI algorithms in hybrid architectures, on testing the operation under concept drift conditions, and on integration with FATF regulatory requirements.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of Interest

None.

References

[1] Ajagbe, S.A., Majola, S., & Mudali, P. (2025). Comparative analysis of machine learning algorithms for money laundering detection. *Discover Artificial Intelligence*, 5, article number 144. doi: 10.1007/s44163-025-00397-4.

[2] Altman, E., Blanuša, J., von Niederhäusern, L., Egressy, B., Anghel, A., & Atasu, K. (2023). Realistic synthetic financial transactions for antimoney laundering models. In A. Oh, T. Naumann, A., Globerson, K., Saenko, M., Hardt & S., Levine (Eds.), *Advances in neural information processing systems*. Red Hook: Curran Associates, Inc.

[3] Bakry, A.N., Alsharkawy, A.S., Farag, M.S., & Raslan, K.R. (2024). Automatic suppression of false positive alerts in anti-money laundering systems using machine learning. *The Journal of Supercomputing*, 80, 6264-6284.

[4] Balusamy, S., Rengasamy, R., & Aravind, J. (2025). Protecting financial transactions and cryptocurrency networks from fraud using AI-powered blockchain technology. In *Proceedings of the 2025 global conference in emerging technologies* (pp. 1-6). Pune: IEEE.

[5] Chen, Y., Chen, Z., & Amin, H.U. (2025). LG-VGAE: A local and global collaborative variational graph autoencoder for detecting crypto money laundering. *Knowledge and Information Systems*, 6, article number 586.

[6] Di Gennaro, M., Panebianco, F., Pianta, M., Zanero, S., & Carminati, M. (2025). Amatriciana: Exploiting temporal GNNs for robust and efficient money laundering detection. *arXiv*. doi: 10.48550/arXiv.2506.00654.

[7] Dumitrescu, B., Baltoiu, A., & Budulan, S. (2022). Anomaly detection in graphs of bank transactions for anti money laundering applications. *IEEE Access*, 10(96). doi: 10.1109/ACCESS.2022.3170467.

[8] Eurojust. (2024). *International operation leads to seizure of 2 000 fake works of art with potential losses of EUR 200 million*. Retrieved from https://surl.li/vvgdgf.

[9] European Banking Authority. (2025). *Opinion and report on money laundering and terrorist financing risks affecting the EU's financial sector*. Retrieved from https://surl.lt/mprhoo.

[10] Financial Action Task Force (FATF). (2025). *International standards on combating money laundering and the financing of terrorism & proliferation. The FATF Recommendations*. Paris: FATF.

[11] FinCEN. (2024). *FinCEN assesses record $1.3 billion penalty against TD Bank, N.A. and TD Bank USA, N.A. U.S. Department of the Treasury*. Retrieved from https://surl.lu/uhpaml.

[12] FinCEN. (2025). *FinCEN year in review FY 2024 [Infographic]*. Retrieved from https://www.fincen.gov/system/files/shared/FinCEN-Infographic-Public-2025-508.pdf?utm_source=.

[13] Fortunenko, A., Shkondin, O., Stadnyk, O., & Hontaruk, I. (2025). *Ukraine: Evolving antimoney laundering framework expands corporate criminal liability*. Retrieved from https://surl.li/mjofyb

[14] Gandhi, H., Tandon, K., Gite, S., Pradhan, B., & Alamri, A. (2024). Navigating the complexity of money laundering: Anti–money laundering advancements with AI/ML insights. *International Journal on Smart Sensing and Intelligent Systems*, 17(1).

[15] Horobets, N., Reznik, O., Maliyk, V., Vyhivskyi, I., & Bobrishova, L. (2025). Artificial intelligence technologies in banking: Challenges and opportunities for anti-money laundering in the context of EU regulatory initiatives. *Journal of Money Laundering Control*, 28(4-5), 593-608. doi: 10.1108/JMLC-03-2025-0041.
[16] Jensen, R.I.T., & Iosifidis, A. (2023). Qualifying and raising anti-money laundering alarms with deep learning. *Expert Systems with Applications*, 214, article number 119037. doi: 10.1016/j.eswa.2022.119037.
[17] Johannessen, F., & Jullum, M. (2023). Finding money launderers using heterogeneous graph neural networks. *arXiv*. doi: 10.48550/arXiv.2307.13499.
[18] Kalabukhova, S. (2025). Methods of analysis in the financial intelligence system. *Finance of Ukraine*, 4, 46-57. doi: 10.33763/finukr2025.04.046.
[19] Karthikeyan, G.K., & Bhowmik, B. (2025). Enhancing money laundering detection in bank transactions using GAGAN: A graph-adapted generative adversarial network approach. *International Journal of Data Science and Analytics*, 20, 6301-6331. doi: 10.1007/s41060-025-00823-x.
[20] Konstantinidis, G., & Gegov, A. (2024). Deep neural networks for antimoney laundering using explainable artificial intelligence. In *Proceedings of the 2024 IEEE 12th International Conference on Intelligent Systems* (pp. 430-435). Red Hook: IEEE.
[21] National Police of Ukraine – Zaporizhzhia Region. (2025). *Zaporizhzhia police uncovered a man who misappropriated over UAH 3,500,000 in cryptocurrency*. Retrieved from https://surl.li/ylxqgt.
[22] National Police of Ukraine. (2023). *Over UAH 1 billion laundered through resale of securities on the stock exchange: Law enforcement officers served notices of suspicion to members of a criminal group*. Retrieved from https://surl.li/upjfav.
[23] National Police of Ukraine. (2024). *Over UAH 200 million laundered via VAT schemes: law enforcement exposed organizers using enterprises employing persons with disabilities*. Retrieved from https://surl.li/czvubg .
[24] Ovsianiuk, D. (2024). Intelligence cycle as the basis of analytical activity in combating drug-related crime. *Law Journal of the National Academy of Internal Affairs*, 14(2), 95-104. doi: 10.56215/naia-chasopis/2.2024.95.
[25] Ovsianiuk, D., & Ustymenko, O. (2024). Exchange of information as a form of international cooperation in combating drug trafficking. *Novum Jus*, 18(1), 181-216. doi: 10.14718/NovumJus.2024.18.1.7.
[26] Pocher, N., Zichichi, M., Merizzi, F., Shafiq, M. Z., & Ferretti, S. (2023). Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics. *Electronic Markets*, 33, article number 37. doi: 10.1007/s12525-023-00654-3.
[27] Poon, C.-H., Kwok, J., Chow, C., & Choi, J.-H. (2025). LineMVGNN: Anti-money laundering with line-graph-assisted multi-view graph neural networks. *AI*, 6(4), article number 69. doi: 10.3390/ai6040069.
[28] Pousette, T., & Rosendal, A. (2024). *Explainable anti-money laundering*. (Master's thesis, Chalmers University of Technology, Gothenburg, Sweden).
[29] Purohit, M., & Barot, H. (2024). Data-driven forensics: Unveiling the hidden depths of financial crime. In S.K. Shandilya, D. Sujay & V.B. Gupta (Ed.), *Advancements in cybercrime investigations and modern data analytics*. Boca Raton: CRC Press.
[30] Rana, S., Aggarwal, S., Jagirdar, S.S., & Jain, S. (2025). *Insights in banking analytics and regulatory compliance using AI*. Retrieved from https://www.igi-global.com/gateway/book/358948.
[31] Reite, E.J., Karlsen, J., & Westgaard, E.G. (2025). Improving client risk classification with machine learning to increase anti-money laundering detection efficiency. *Journal of Money Laundering Control*, 28(1), 93-107. doi: 10.1108/JMLC-03-2024-0040.
[32] Singh, V. (2025). Policy optimization for Anti-Money Laundering (AML) compliance using AI techniques: A machine learning approach to enhance banking regulatory compliance. *International Journal of Engineering Research & Technology (IJERT)*, 14(4).
[33] State Financial Monitoring Service of Ukraine. (2023). *Methodological recommendations for analysing money laundering trends related to modern forms of slavery in Ukraine.* Retrieved from https://surl.lt/aglghq.
[34] State Financial Monitoring Service of Ukraine. (2025). *Report of the State Financial Monitoring Service of Ukraine for 2024*. Retrieved from https://fiu.gov.ua/assets/userfiles/0350/2025/REPORT2024.pdf.
[35] U.S. Department of Justice, Office of Public Affairs. (2025a). *Nevada man sentenced for over $11 M COVID-19 relief fraud and money laundering scheme*. Retrieved from https://surl.li/gmfdzu.
[36] U.S. Department of Justice, Office of Public Affairs. (2025b). *Founder and CEO of AML Bitcoin sentenced to seven years in prison for multi-million-dollar fraud scheme*. Retrieved from https://surl.li/dhzpjy.
[37] United Nations Conference on Trade and Development (UNCTAD). (2023). *First-ever official data on illicit financial flows now available*. Retrieved from https://surl.lt/xtcjng.
[38] Wang, S., Wang, P., Wu, B., Zhu, Y., Luo, W., & Pan, Y. (2024). Structural entropy minimization combining graph representation for money laundering identification. *International Journal of Machine Learning and Cybernetics*, 15, 3951-3968. doi: 10.1007/s13042-024-02129-z.
[39] Wójcik, F. (2024). An analysis of novel money laundering data using heterogeneous graph isomorphism networks: FinCEN Files case study. *Econometrics. Ekonometria. Advances in Applied Data Analysis*, 28(2), 32-49.

Застосування штучного інтелекту для виявлення аномальних транзакцій як новий напрям у боротьбі з відмиванням грошей

Дмитро Овсянюк
Аналітичний відділ (Центр кримінальної аналітики)
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0000-0002-1846-4167

Андрій Окушко
Кандидат юридичних наук
Департамент кіберполіції Національної поліції України
02093, вул. Бориспільська, 19, м. Київ, Україна
https://orcid.org/0009-0003-3627-2489

Євгеній Панченко
Департамент міжнародного поліцейського співробітництва
Національної поліції України
01024, вул. Академіка Богомольця, 1, м. Київ, Україна
https://orcid.org/0000-0001-5755-7457

Анотація
Метою дослідження було вивчення ефективності застосування алгоритмів штучного інтелекту в системі фінансового моніторингу. Методологія охоплювала порівняльний аналіз практики США, Європейського Союзу та України, аналіз конкретних випадків міжнародних фінансових інцидентів (США, Європейський Союз, Україна) й оцінювання нормативно-правової бази. Встановлено, що регуляторна база для системи, що ґрунтується на правилах, закріплена в міжнародних стандартах Групи з фінансових заходів проти відмивання грошей та реалізована в законодавстві Європейського Союзу, Сполучених Штатів та України, що забезпечує прозорість контролю та одночасно знижує адаптивність до нових схем. У Сполучених Штатах правові норми забезпечують сувору звітність і санкції, проте ці норми продемонстрували критичні прогалини в моніторингу, що ґрунтується на правилах. У Європейському Союзі багаторівневі директиви посилили централізований нагляд, водночас нерозв'язаною залишилася проблема бюрократичної інерції. В Україні боротьба з відмиванням грошей у сфері криптовалют є недостатньо ефективною. Виявлено, що в рішеннях Вищого антикорупційного суду за 2024 рік було зафіксовано випадки використання дробних земельних угод на суму понад 3,1 млн доларів, а також великомасштабні організовані схеми, які системи, що ґрунтуються на правилах, не виявили. Статистика за 2024 рік (1,75 млн фінансових звітів, 12,1 млрд грн вилучених активів) продемонструвала масштаби системи протидії відмиванню грошей в Україні, а також засвідчила необхідність зменшення кількості помилкових спрацьовувань і посилення аналітики. Узгодження з міжнародною практикою продемонструвало, що ефективності майбутніх рішень щодо протидії відмиванню грошей в Україні можливо досягти лише за умови поєднання нормативно-правової бази з моделями штучного інтелекту, які відповідають вимогам Групи з фінансових заходів проти відмивання грошей та Європейського Союзу. Практичне значення дослідження полягає в застосуванні результатів банками, регуляторними органами та правоохоронними органами України для зменшення кількості помилкових спрацьовувань, виявлення складних схем й адаптації систем моніторингу до міжнародних стандартів

Ключові слова:
пояснюваність моделі; федеративне навчання; графічні нейронні мережі; графічні автокодери; зменшення кількості помилкових спрацьовувань; операції з криптовалютою; конфіденційність транзакційних даних