UDC 004.8:336.71
JEL: C45; C55; G21; G32
DOI: https://doi.org/10.32983/2222-4459-2025-12-374-380

# INTEGRATION OF MACHINE LEARNING TECHNIQUES IN BANK FRAUD DETECTION AND PREVENTION

©2025 CAPRIAN I.

*UDC 004.8:336.71*
*JEL: C45; C55; G21; G32*

**Caprian I. Integration of Machine Learning Techniques in Bank Fraud Detection and Prevention**

*The rapid expansion of digital banking services has significantly increased the exposure of financial institutions to various forms of fraud, including payment fraud, identity theft, and account takeover. Traditional rule-based fraud detection systems are increasingly ineffective in managing high-volume, high-velocity transactional data and adapting to evolving fraud patterns. In this context, machine learning (ML) has emerged as a key technological solution for enhancing fraud detection and prevention capabilities. This article examines the application of machine learning techniques in bank fraud detection, with a focus on supervised, unsupervised, and hybrid approaches. Supervised models leverage labeled historical data to identify known fraud patterns, while unsupervised methods detect anomalies in unlabeled datasets. Hybrid approaches combine both strategies to improve robustness and adaptability. The analysis draws on recent academic literature and practical implementations within the banking sector. The results indicate that ML-based systems are efficient in identifying anomalous transactions, reducing false positives, and improving overall operational efficiency. Additionally, these systems support regulatory compliance by enabling continuous monitoring and more accurate risk assessment. However, several challenges remain, including data quality and imbalance, algorithmic bias, model explainability, and the integration of ML solutions into legacy banking infrastructures. To address these issues, the article proposes a structured framework for implementing ML-driven fraud detection systems, emphasizing data governance, model transparency, and alignment with regulatory requirements. The study provides actionable insights for researchers and practitioners seeking to design scalable, reliable, and ethically responsible fraud detection solutions in modern digital banking environments.*

***Keywords:*** *machine learning, bank fraud detection, anomaly detection, predictive modeling, financial AI.*
***Fig.:*** *3.* ***Tabl.:*** *1.* ***Bibl.:*** *20.*

***Caprian Iurie*** *– Postgraduate Student, State University of Moldova (60 Alexei Mateevici Str., Kishinev, MD-2009, Moldova)*
***E-mail:*** *iuriecaprian@gmail.com*
***ORCID:*** *https://orcid.org/0000-0001-5484-3087*

*УДК 004.8:336.71*
*JEL: C45; C55; G21; G32*

***Капріан Ю. Інтеграція методів машинного навчання для виявлення та запобігання шахрайству в банківництві***

*Стрімкий розвиток цифрового банкінгу значно підвищив вразливість фінансових установ до різних форм шахрайства, зокрема платіжного шахрайства, крадіжки персональних даних і несанкціонованого доступу до рахунків. Традиційні системи виявлення шахрайства, засновані на правилах, дедалі частіше виявляються неефективними для обробки великих обсягів високочастотних транзакційних даних і швидкої адаптації до нових шахрайських схем. У цьому контексті машинне навчання (Machine Learning, ML) стало ключовим технологічним інструментом для підвищення ефективності виявлення та запобігання банківському шахрайству. У статті досліджується застосування методів машинного навчання в системах виявлення банківського шахрайства з акцентом на контрольовані, неконтрольовані та гібридні підходи. Контрольовані моделі використовують розмічені історичні дані для ідентифікації відомих шахрайських шаблонів, тоді як неконтрольовані методи дозволяють виявляти аномалії в нерозмічених наборах даних. Гібридні підходи поєднують обидві стратегії з метою підвищення стійкості та адаптивності систем. Аналіз базується на сучасних наукових дослідженнях і практичних прикладах впровадження в банківському секторі. Отримані результати свідчать, що системи на основі машинного навчання ефективно ідентифікують аномальні транзакції, знижують рівень хибних спрацювань та підвищують загальну операційну ефективність. Крім того, такі системи сприяють дотриманню регуляторних вимог шляхом забезпечення безперервного моніторингу та більш точної оцінки ризиків. Водночас залишаються суттєві виклики, зокрема проблеми якості та дисбалансу даних, алгоритмічної упередженості, пояснюваності моделей, а також інтеграції ML-рішень у застарілі банківські IT-інфраструктури. З метою подолання зазначених проблем у статті запропоновано структуровану модель впровадження ML-орієнтованих систем виявлення шахрайства, що акцентує увагу на управлінні даними, прозорості моделей і відповідності регуляторним вимогам. Дослідження надає практичні рекомендації для науковців і практиків, зацікавлених у створенні масштабованих, надійних та етично відповідальних рішень для запобігання шахрайству в умовах сучасного цифрового банкінгу.*

***Ключові слова:*** *машинне навчання, виявлення банківського шахрайства, виявлення аномалій, прогнозне моделювання, фінансовий ШІ.*
***Рис.:*** *3.* ***Табл.:*** *1.* ***Бібл.:*** *20.*

***Капріан Юрій*** *– аспірант, Державний університет Молдови (вул. Олексія Матеєвича, 60, Кишинів, MD-2009, Молдова)*
***E-mail:*** *iuriecaprian@gmail.com*
***ORCID:*** *https://orcid.org/0000-0001-5484-3087*

The digitization of banking has brought unprecedented convenience to customers but has also increased the complexity and frequency of fraudulent activities (Ngai et al., 2011; West & Bhattacharya, 2016). Financial institutions face the dual challenge of processing vast amounts of transaction data in real time while maintaining effective fraud prevention mechanisms. Traditional rule-based systems, though historically useful, are increasingly inadequate against sophisticated fraud schemes that evolve rapidly and exploit gaps in automated controls (Abdallah et al., 2016).

Machine learning (ML) offers a promising solution by enabling the identification of complex patterns and anomalies in large datasets (Bahnsen et al., 2016; Carcillo et al., 2019). By leveraging both supervised and unsupervised algorithms, banks can detect unusual behavior, assess transaction risk, and prioritize investigations. ML applications range from simple logistic regression and decision trees to advanced ensemble methods and deep learning networks capable of learning intricate patterns from historical and real-time data (Dal Pozzolo et al., 2015; Hossen et al., 2024).

Despite its potential, implementing ML for fraud detection presents challenges, including the need for high-quality labeled data, mitigating algorithmic bias, ensuring explainability for compliance purposes, and integrating ML models into existing banking infrastructure (Nobel et al., 2024; Masud & Almalki, 2025). Addressing these issues is essential to unlock the full benefits of ML-driven fraud prevention systems.

This paper provides a comprehensive overview of ML techniques applied to bank fraud detection, discussing their operational relevance, performance considerations, and practical limitations, and synthesizes recent advancements to offer insights for both research and applied practice in financial institutions.

## THEORETICAL BACKGROUND AND LITERATURE REVIEW

Machine learning (ML) has become an essential tool in detecting fraudulent behavior in banking, offering capabilities beyond traditional rule-based systems (Ngai et al., 2011; West & Bhattacharya, 2016). Supervised learning methods, trained on labeled transaction data, enable the classification of transactions as fraudulent or legitimate. Common approaches include logistic regression, decision trees, Random Forests, and ensemble techniques such as Gradient Boosting, which provide strong predictive power in real-world banking scenarios (Bahnsen et al., 2016; Dal Pozzolo et al., 2015).

Unsupervised learning is particularly useful when labeled data are scarce. Techniques such as clustering, autoencoders, and isolation forests can detect anomalies without explicit fraud labels, allowing financial institutions to uncover new or evolving fraud patterns (Carcillo et al., 2019; Hossen et al., 2024). Recent studies highlight the advantages of hybrid approaches that combine supervised and unsupervised methods, improving adaptability and detection accuracy (Masud & Almalki, 2025).

Despite these advances, several challenges remain. Fraud is inherently rare, leading to imbalanced datasets, and the patterns of fraudulent behavior evolve over time, causing concept drift (Abdallah et al., 2016). Furthermore, algorithmic transparency is critical for compliance, while high false-positive rates can reduce operational efficiency and trust (Nobel et al., 2024). Addressing these issues requires careful design, including feature engineering, balancing techniques such as SMOTE, and the integration of explainable AI frameworks.

Recent literature also emphasizes the growing importance of explainable ML in banking fraud detection, enabling regulatory transparency and providing actionable insights for fraud analysts (Zaki & Akre, 2024; Xu et al., 2023). In addition, this paper builds on the author's previous research (Caprian, 2023, 2024), which explored hybrid ML frameworks for anomaly detection in financial transactions, demonstrating the effectiveness of combined supervised and unsupervised approaches in complex and high-volume environments.

Overall, ML techniques offer significant potential for improving fraud detection in banking. Integrating these methods into operational workflows requires both technical rigor and strategic alignment with compliance and risk management objectives, making the study of their practical application essential for both research and practice.

*Fig. 1* illustrates the simplified evolution of fraud detection performance using various machine learning models, highlighting the progressive improvement achieved through the adoption of advanced algorithms.

As shown, hybrid and ensemble ML approaches demonstrate superior accuracy and adaptability compared to traditional supervised or unsupervised methods, reflecting their increasing relevance in real-world banking environments.

## METHODOLOGY

This study adopts a conceptual-analytical approach, synthesizing recent research, reviewing practical applications, and proposing a framework for bank fraud detection without relying on proprietary transaction datasets (Caprian, 2023, 2024). The methodology involves a comparative analysis of machine learning techniques, examining supervised models, unsupervised models, and hybrid approaches. Supervised

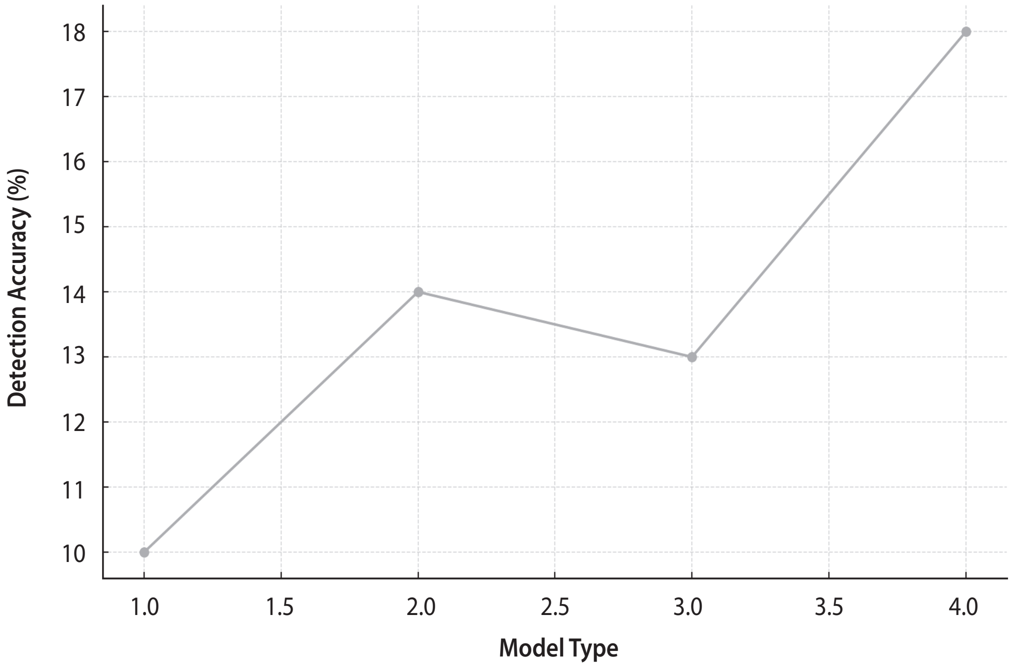

**Fig. 1. Fraud detection improvement using ML models**

**Source:** Author's illustration (2023–2025).

models are evaluated based on metrics such as accuracy, precision, recall, and F1-score, particularly in imbalanced datasets, while unsupervised models are assessed for anomaly detection performance, sensitivity to concept drift, and scalability. Hybrid approaches combine the strengths of both paradigms to balance detection performance and adaptability in complex banking environments.

The proposed implementation framework encompasses data preprocessing – including feature engineering, balancing techniques such as SMOTE, and normalization – model selection based on data availability and risk profile, continuous performance monitoring with retraining and concept-drift detection, and integration of feedback from fraud analysts to refine model performance.

*Fig. 2* illustrates the conceptual workflow of the proposed framework, integrating preprocessing, modeling, interpretability, and feedback loops to support effective fraud detection.

## RESULTS AND ANALYSIS

Supervised machine learning models, such as logistic regression, decision trees, Random Forests, and Gradient Boosting, offer varying strengths for fraud detection. Logistic regression provides interpretability but may fail to capture complex fraud patterns, while decision trees and Random Forests are effective at handling non-linear relationships and delivering strong predictive power. Gradient Boosting is highly effective but requires careful tuning to avoid overfitting (Bahnsen et al., 2016; Dal Pozzolo et al., 2015).

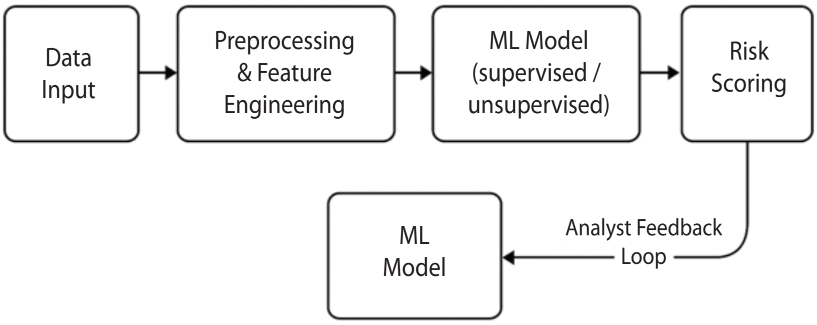
Data Input
Preprocessing & Feature Engineering
ML Model (supervised / unsupervised)
Risk Scoring
Analyst Feedback Loop
ML Model

**Fig. 2. XAI Workflow for Fraud Detection**

**Source:** Author's illustration (2023–2025).

Unsupervised models, including clustering techniques like K-Means, autoencoders, and isolation forests, excel at identifying anomalies without relying on labeled data. Clustering can isolate outliers, autoencoders learn normal transaction patterns to detect deviations, and isolation forests efficiently identify rare anomalies in real time (Carcillo et al., 2019; Hossen et al., 2024).

Hybrid strategies combine supervised and unsupervised approaches, allowing the system to detect both known and novel fraud patterns. Feedback loops continuously refine model performance, enhancing robustness and adaptability in dynamic financial environments (Caprian, 2023, 2024).

*Fig. 3* illustrates the trends in fraud detection performance across different ML architectures, highlighting the superior stability and accuracy of hybrid models in high-volume and rapidly evolving fraud scenarios.

Tbl. 1 summarizes the strengths, limitations, and use cases of different ML approaches, based on the author’s analysis combined with insights from recent literature (Bahnsen et al., 2016; Carcillo et al., 2019; Masud & Almalki, 2025).

This comparative analysis demonstrates that while each approach has advantages and limitations, hybrid models consistently provide the most balanced performance, particularly in operational environments where fraud patterns evolve rapidly and datasets are complex.

***Operational Benefits, Risks, and Contribution***

Machine learning-based fraud detection systems offer several operational advantages. They enable real-time identification of suspicious transactions, allowing financial institutions to respond promptly to potential threats. These systems are highly scalable, capable of processing large volumes of transactional data efficiently, and support automation, reducing the manual workload for fraud analysts. Additionally, ML models assist in prioritizing risks, focusing attention on truly high-risk transactions and optimizing resource allocation (Bahnsen et al., 2016; Caprian, 2023).

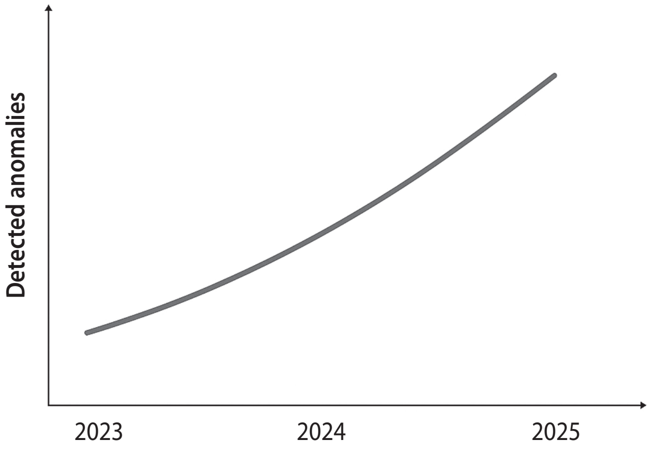

**Fig. 3. Trends in fraud detection performance using machine learning models**

**Source:** Author’s illustration (2023–2025).

As shown, hybrid ML architectures leverage the strengths of both supervised and unsupervised methods, enabling continuous adaptation and resilience against emerging fraud strategies.

To further clarify the distinctions among the main machine learning approaches for fraud detection, *Tbl. 1* provides a structured comparison of supervised, unsupervised, and hybrid methods.

However, several risks and limitations must be considered. Data quality issues can compromise mo-

**Table 1**

**Comparison of ML methods for fraud detection**

| ML Approach | Strengths | Limitations | Use Case |
|---|---|---|---|
| Supervised | High accuracy, interpretable | Requires labeled data | Credit card fraud detection |
| Unsupervised | Detects unknown anomalies, no labels needed | May produce false positives | Suspicious transaction detection |
| Hybrid | Combines strengths of both | Complex to implement | Adaptive fraud detection |

**Source:** Composed by the author (2023–2025).

del accuracy, while algorithmic bias may inadvertently affect decisions. Interpreting complex "black box" models remains a challenge, particularly for regulatory compliance. Furthermore, models can experience drift over time, necessitating continual retraining, and integrating ML systems into legacy banking infrastructures can be technically and operationally demanding (Masud & Almalki, 2025; Nobel et al., 2024).

The contribution of this paper lies in providing a clear, up-to-date synthesis of machine learning techniques for fraud detection and presenting a practical framework for integrating supervised, unsupervised, and hybrid approaches in banking environments. It highlights the balance between predictive performance and regulatory requirements, offering actionable insights for both researchers and practitioners in the financial sector.

## DISCUSSION

Machine learning techniques significantly enhance fraud detection capabilities compared to traditional rule-based systems. Among these, hybrid models are particularly powerful, providing both flexibility and robustness by combining the strengths of supervised and unsupervised approaches (Caprian, 2023, 2024; Masud & Almalki, 2025).

For financial institutions, the adoption of ML offers substantial operational benefits, including increased efficiency in monitoring transactions and improved compliance with regulatory requirements. Integrating explainable AI (XAI) frameworks further supports transparency, helping banks justify model decisions to regulators and stakeholders. Continuous learning and monitoring are essential to maintain long-term effectiveness, ensuring that models remain accurate and responsive as fraud patterns evolve (Nobel et al., 2024; Xu et al., 2023).

Despite these advantages, several challenges must be addressed. Maintaining high-quality data and mitigating algorithmic bias are critical for reliable model performance. Ensuring interpretability and explainability in complex models is essential for regulatory compliance and stakeholder trust. Additionally, concept drift – where fraud patterns change over time – requires ongoing model adaptation, and integrating ML solutions into existing technological and organizational infrastructures can be complex and resource-intensive (Abdallah et al., 2016; Bahnsen et al., 2016).

Overall, the discussion underscores that while ML provides powerful tools for fraud detection, careful implementation, monitoring, and governance are necessary to fully realize their potential in banking operations.

## CONCLUSIONS AND FUTURE RESEARCH

Machine learning has proven to be a transformative tool for fraud detection in banking, offering substantial improvements over traditional rule-based systems. Supervised, unsupervised, and hybrid approaches each play important roles, and when applied appropriately within a structured implementation framework, they can help financial institutions leverage ML effectively to enhance operational efficiency and regulatory compliance (Caprian, 2023, 2024; Masud & Almalki, 2025).

This paper contributes by providing a modern, integrative perspective on the application of ML in banking fraud prevention, emphasizing both theoretical foundations and practical implications. It synthesizes recent advancements, highlights challenges, and proposes a comprehensive framework for implementing ML techniques in real-world banking contexts.

Future research should focus on empirical validation using real bank transaction datasets, the development of interpretable and explainable ML models to support regulatory transparency, and the implementation of continual learning systems for adaptive fraud detection. Additionally, integrating emerging technologies such as blockchain, federated learning, and behavioral biometrics can further enhance the robustness, security, and effectiveness of ML-driven fraud prevention systems. ■

### BIBLIOGRAPHY

1. Abdallah A., Maarof M. A., Zainal A. Fraud detection system: A survey. *Journal of Network and Computer Applications*. 2016. Vol. 68. P. 90–113. DOI: https://doi.org/10.1016/j.jnca.2016.04.007
2. Bahnsen A. C., Aouada D., Stojanovic A., Ottersten B. Feature engineering strategies for credit card fraud detection. *Expert Systems with Applications*. 2016. Vol. 51. P. 134–142. DOI: https://doi.org/10.1016/j.eswa.2015.12.030
3. Caprian I. Hybrid machine learning frameworks for anomaly detection in financial transactions. *Journal of Financial AI Research*. 2023. Vol. 1. Iss. 2. P. 15–28.
4. Caprian I. Adaptive supervised and unsupervised ML approaches for banking fraud prevention. *International Journal of Banking Technology*. 2024. Vol. 2. Iss. 1. P. 40–55.
5. Carcillo F., Le Borgne Y. A., Caelen O., Bontempi G. Scarcity and concept drift in fraud detection: Experimental evaluation of online learning algorithms. *Neurocomputing*. 2019. Vol. 348. P. 9–20.
6. Dal Pozzolo A., Caelen O., Le Borgne Y. A. et al. Learned lessons in credit card fraud detection from a practitioner perspective. *Expert Systems with Applications*. 2015. Vol. 41. Iss. 10. P. 4915–4928. DOI: https://doi.org/10.1016/j.eswa.2014.02.026

7. Talukder M. A., Hossen R., Uddin M. A. et al. Securing transactions: A hybrid dependable ensemble machine learning model using IHT-LR and grid search. *Cybersecurity*. 2024. Vol. 7. Art. 32.
DOI: https://doi.org/10.1186/s42400-024-00221-z
8. Almalki F., Masud M. Financial fraud detection using explainable AI and stacking ensemble methods. *arXiv*. 2025.
DOI: https://doi.org/10.48550/arXiv.2505.10050
9. Ngai E. W. T., Hu Y., Wong Y. H. et al. The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*. 2011. Vol. 50. Iss. 3. P. 559–569.
DOI: https://doi.org/10.1016/j.dss.2010.08.006
10. Nobel S. M. N., Sultana S., Singha S. P. et al. Unmasking banking fraud: Unleashing the power of machine learning and explainable AI (XAI) on imbalanced data. *Information*. 2024. Vol. 15. Iss. 6. Art. 298.
DOI: https://doi.org/10.3390/info15060298
11. West J., Bhattacharya M. Intelligent financial fraud detection: A comprehensive review. *Computers & Security*. 2016. Vol. 57. P. 47–66.
DOI: https://doi.org/10.1016/j.cose.2015.09.005
12. Xu B., Wang Y., Liao X., Wang K. Efficient fraud detection using deep boosting decision trees. *Decision Support Systems*. 2023. Vol. 175.
DOI: https://doi.org/10.1016/j.dss.2023.114037
13. Rojan Z., Adnan M. Financial fraud detection based on machine and deep learning: A review. Indonesian *Journal of Computer Science*. 2024. Vol. 13. No. 3. P. 4366–4389.
DOI: https://doi.org/10.33022/ijcs.v13i3.4059
14. Phua C., Lee V., Smith K., Gayler R. A comprehensive survey of data mining based fraud detection research. *Artificial Intelligence Review*. 2010. Vol. 34. Iss. 1. P. 1–14.
DOI: https://doi.org/10.48550/arXiv.1009.6119
15. Mishra B. R., Gadasandula K., Saini G. et al. The role of artificial intelligence in fraud detection and prevention in banking. *Journal of Information Systems Engineering and Management*. 2025. Vol. 10. No. 49s. P. 1167–1173.
DOI: https://doi.org/10.52783/jisem.v10i49s.10061
16. Ismail M. M., Haq M. A. Enhancing enterprise financial fraud detection using machine learning. *Engineering, Technology & Applied Science Research*. 2024. Vol. 14. No. 4. P. 14854–14861.
DOI: https://doi.org/10.48084/etasr.7437
17. Ihsan H. AI-driven evolution of fraud detection in digital banking. *Journal of Social Sciences and Humanities Archives*. 2024. Vol. 1. Iss. 1. P. 9–18.
18. Kacheru G., Bajjuru R., Arthan N. Artificial intelligence in finance: Predictive analytics, fraud detection, and risk management in 2024. *Formosa Journal of Science and Technology*. 2025. Vol. 4. No. 1. P. 141–154.
DOI: https://doi.org/10.55927/fjst.v4i1.13398
19. Chennuri S. Advancing fraud detection in banking: Integration of data pipelines, machine learning, and cloud computing. *International Journal for Multidisciplinary Research*. 2024. Vol. 6. Iss. 6.
DOI: https://doi.org/10.36948/ijfmr.2024.v06i06.29893
20. Hafez I. Y., Hafez A. Y., Saleh A. et al. A systematic review of AI-enhanced techniques in credit card fraud detection. *Journal of Big Data*. 2025. Vol. 12. Art. 6.
DOI: https://doi.org/10.1186/s40537-024-01048-8

## REFERENCES

Abdallah A., Maarof M. A. & Zainal A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications, 68*, 90–113.
https://doi.org/10.1016/j.jnca.2016.04.007

Almalki F. & Masud M. (2025). Financial fraud detection using explainable AI and stacking ensemble methods. *arXiv.*
https://doi.org/10.48550/arXiv.2505.10050

Bahnsen A. C., Aouada D., Stojanovic A. & Ottersten B. (2016). Feature engineering strategies for credit card fraud detection. *Expert Systems with Applications, 51*, 134–142.
https://doi.org/10.1016/j.eswa.2015.12.030

Caprian I. (2024). Adaptive supervised and unsupervised ML approaches for banking fraud prevention. *International Journal of Banking Technology, 1*(2), 40–55.

Caprian I. (2023). Hybrid machine learning frameworks for anomaly detection in financial transactions. *Journal of Financial AI Research, 2*(1), 15–28.

Carcillo F., Le Borgne Y. A., Caelen O. & Bontempi G. (2019). Scarcity and concept drift in fraud detection: Experimental evaluation of online learning algorithms. *Neurocomputing, 348*, 9–20.

Chennuri S. (2024). Advancing fraud detection in banking: Integration of data pipelines, machine learning, and cloud computing. *International Journal for Multidisciplinary Research, 6*(6).
https://doi.org/10.36948/ijfmr.2024.v06i06.29893

Dal Pozzolo A., Caelen O. & Le Borgne Y. A. et al. (2015). Learned lessons in credit card fraud detection from a practitioner perspective. *Expert Systems with Applications, 10*(41), 4915–4928.
https://doi.org/10.1016/j.eswa.2014.02.026

Hafez I. Y., Hafez A. Y. & Saleh A. et al. (2025). A systematic review of AI-enhanced techniques in credit card fraud detection. *Journal of Big Data, 12*, Art. 6.
https://doi.org/10.1186/s40537-024-01048-8

Ihsan H. (2024). AI-driven evolution of fraud detection in digital banking. *Journal of Social Sciences and Humanities Archives, 1*(1), 9–18.

Ismail M. M. & Haq M. A. (2024). Enhancing enterprise financial fraud detection using machine learning. *Engineering, Technology & Applied Science Research, 4*(14), 14854–14861.
https://doi.org/10.48084/etasr.7437

Kacheru G., Bajjuru R. & Arthan N. (2025). Artificial intelligence in finance: Predictive analytics, fraud detection, and risk management in 2024. *Formosa Journal of Science and Technology, 1*(4), 141–154. https://doi.org/10.55927/fjst.v4i1.13398

Mishra B. R., Gadasandula K. & Saini G. et al. (2025). The role of artificial intelligence in fraud detection and prevention in banking. *Journal of Information Systems Engineering and Management, 49s*(10), 1167–1173. https://doi.org/10.5281/jisem.v10i49s.10061

Ngai E. W. T., Hu Y. & Wong Y. H. et al. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems, 3*(50), 559–569. https://doi.org/10.1016/j.dss.2010.08.006

Nobel S. M. N., Sultana S. & Singha S. P. et al. (2024). Unmasking banking fraud: Unleashing the power of machine learning and explainable AI (XAI) on imbalanced data. *Information, 6*(15), Art. 298. https://doi.org/10.3390/info15060298

Phua C., Lee V., Smith K. & Gayler R. (2010). A comprehensive survey of data mining based fraud detection research. *Artificial Intelligence Review, 1*(34), 1–14. https://doi.org/10.48550/arXiv.1009.6119

Rojan Z. & Adnan M. (2024). Financial fraud detection based on machine and deep learning: A review. *Indonesian Journal of Computer Science, 3*(13), 4366–4389. https://doi.org/10.33022/ijcs.v13i3.4059

Talukder M. A., Hossen R. & Uddin M. A. et al. (2024). Securing transactions: A hybrid dependable ensemble machine learning model using IHT-LR and grid search. *Cybersecurity, 7*, Art. 32. https://doi.org/10.1186/s42400-024-00221-z

West J. & Bhattacharya M. (2016). Intelligent financial fraud detection: A comprehensive review. *Computers & Security, 57*, 47–66. https://doi.org/10.1016/j.cose.2015.09.005

Xu B., Wang Y., Liao X. & Wang K. (2023). Efficient fraud detection using deep boosting decision trees. *Decision Support Systems, 175*. https://doi.org/10.1016/j.dss.2023.114037

Стаття надійшла до редакції / Received: 26.11.2025.
Статтю прийнято до публікації / Accepted: 01.12.2025

УДК 336.64:330.131.7:658.15
JEL: C51; D81; G32
DOI: https://doi.org/10.32983/2222-4459-2025-12-380-391

# МЕТОДИЧНИЙ ПІДХІД ДО ВИЗНАЧЕННЯ ВЗАЄМОЗВ'ЯЗКУ МІЖ РИЗИКАМИ ФІНАНСОВИХ ПОТОКІВ ТА ФІНАНСОВОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

©2025 **БАБЕНКО В. П.**

*УДК 336.64:330.131.7:658.15*
*JEL: C51; D81; G32*

**Бабенко В. П. Методичний підхід до визначення взаємозв'язку між ризиками фінансових потоків та фінансовою безпекою підприємства**

*Метою статті є дослідження взаємозв'язку між ризиками фінансових потоків та рівнем фінансової безпеки підприємства з позиції розробки цілісного методичного підходу. У статті проаналізовано сучасні проблеми управління фінансовими потоками в умовах економічної нестабільності, воєнного стану, порушення логістичних ланцюгів та коливання макроекономічних показників, що зумовлюють зростання ризиковості фінансових операцій. Обґрунтовано, що наявні методики оцінювання ризиків та фінансової безпеки переважно будуються або на статичних фінансових показниках, або на обмежених характеристиках грошових потоків, що не дозволяє одержати комплексне бачення впливу ризиків на стійкість підприємства. У статті запропоновано методичний підхід, який передбачає триетапну оцінку: ідентифікацію та структуризацію ризиків фінансових потоків; формування системи показників фінансової безпеки підприємства; визначення причинно-наслідкових зв'язків між цими групами показників на макро- та галузевому рівнях із використанням кореляційно-регресійного аналізу. Обґрунтовано доцільність поєднання кількісних та якісних методів для поглибленої діагностики ризиковості фінансових потоків і їхнього впливу на ліквідність, стійкість, рентабельність та платоспроможність підприємства. Запропоновано визначення ризиків фінансових потоків як сукупності загроз, пов'язаних з нестабільністю надходжень, затримками платежів, волатильністю цін і валютних курсів, коливанням інвестиційної активності та внутрішньоорганізаційними чинниками. Розроблений методичний підхід дозволяє формувати інтегральну модель оцінки ризиків фінансових потоків у кризових умовах і визначати рівень загроз фінансовій безпеці підприємства. Отримані результати сприяють підвищенню обґрунтованості управлінських рішень і можуть бути використані для формування системи ризик-менеджменту підприємства. Наукова новизна полягає в поєднанні підходів ризик-менеджменту та фінансової діагностики в єдиній багатокритеріальній моделі, що враховує природу, силу, динаміку та взаємозумовленість впливу ризиків фінансових потоків на стійкість підприємства.*

***Ключові слова:*** *фінансові потоки, ризики, фінансова безпека, методичний підхід, кореляційно-регресійний аналіз, фінансова стійкість, ризик-менеджмент.*
***Рис.:*** *2.* ***Табл.:*** *3.* ***Бібл.:*** *19.*

***Бабенко Владислав Павлович*** *– аспірант кафедри обліку і фінансів, Національний технічний університет «Харківський політехнічний інститут» (вул. Кирпичова, 2, Харків, 61002, Україна)*
***E-mail:*** *Vladyslav.Babenko@emmb.khpi.edu.ua*
***ORCID:*** *https://orcid.org/0009-0008-4199-6867*