Список використаних джерел:

1. RFC 7230: hypertext transfer protocol (HTTP/1.1): message syntax and routing. IETF Datatracker. URL: https://datatracker.ietf.org/doc/html/rfc7230 (дата звернення: 24.03.2026).
2. MQTT version 3.1.1. OASIS standard. URL: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/mqtt-v3.1.1.html (дата звернення: 24.03.2026).
3. IoT fundamentals: networking technologies, protocols, and use cases for the internet of things. Cisco Press: Source for Cisco Technology. URL: https://www.ciscopress.com/store/iot-fundamentals-networking-technologies-protocols-9781587144561 (дата звернення: 24.03.2026).

УДК 004.8:336.7

ВИЯВЛЕННЯ ФІНАНСОВОГО ШАХРАЙСТВА У ЦИФРОВИХ ПЛАТІЖНИХ СИСТЕМАХ ІЗ ВИКОРИСТАННЯМ СУЧАСНИХ МЕТОДІВ МАШИННОГО НАВЧАННЯ

Печерський Є.В.
yegor.141231@gmail.com
Черкаський державний фаховий бізнес-коледж
Марченко С. В.
м.Черкаси, Україна

Інтенсивна цифровізація фінансових сервісів, розвиток електронної комерції та мобільних платіжних платформ спричинили суттєве збільшення обсягів транзакційних потоків і водночас ускладнення шахрайських схем. Сучасні фінансові екосистеми характеризуються високою динамікою поведінкових патернів користувачів, мережевою природою взаємодій та значною нерівномірністю розподілу класів. За таких умов традиційні підходи на основі правил та класичні статистичні методи демонструють обмежену здатність до адаптації й своєчасного виявлення нових типів фінансових загроз.

Останні дослідження показують, що ефективність протидії шахрайству визначається не лише точністю класифікації транзакцій, але й здатністю систем аналізувати часову еволюцію фінансових взаємодій, враховувати мережеву

структуру даних і підтримувати стабільність роботи моделей у production-середовищі [1; 2]. У цьому контексті особливої актуальності набуває використання сучасних методів машинного навчання та штучного інтелекту, орієнтованих на обробку потокових і високо взаємопов'язаних даних.

Аналіз сучасних підходів машинного навчання до виявлення фінансового шахрайства, визначення їхніх функціональних переваг і практичних обмежень, а також обґрунтування архітектурних принципів побудови інтелектуальних систем аналізу транзакційних потоків у реальному часі.

Ранні системи виявлення фінансового шахрайства базувалися на алгоритмах класифікації із ручною інженерією ознак. Методи логістичної регресії, дерев рішень і ансамблеві алгоритми забезпечували прийнятні результати в умовах відносно стабільних даних. Однак такі моделі виявилися недостатньо ефективними у задачах, де шахрайські операції маскуються під легітимну активність або формують складні багаторівневі залежності.

Критичний аналіз сучасних досліджень свідчить, що класичні алгоритми мають обмежену здатність до узагальнення у випадках зміни концепції (concept drift) – зміни статистичних закономірностей у транзакційних потоках [3]. У результаті виникає необхідність регулярного оновлення моделей і використання більш адаптивних підходів до навчання.

Подальший розвиток пов'язаний із впровадженням підходів репрезентативного навчання (representation learning), що забезпечують автоматичне формування ознак із великих масивів транзакційних даних. Глибинні нейронні мережі дозволяють моделювати складні нелінійні залежності між характеристиками транзакцій і підвищують здатність систем виявляти слабко виражені ризикові патерни.

Значну увагу в сучасних роботах приділяють послідовним моделям, зокрема трансформерним архітектурам і темпоральним згортковим мережам, які враховують часову структуру фінансової активності клієнтів. Такі підходи демонструють покращення показників виявлення шахрайства порівняно з традиційними алгоритмами, особливо у задачах прогнозування ризикових дій

користувачів [2]. Разом із тим підвищення складності моделей призводить до зростання вимог до обчислювальних ресурсів і ускладнює їх інтеграцію у реальні фінансові системи. Це актуалізує проблему пошуку компромісу між точністю та продуктивністю.

Одним із найбільш перспективних напрямів є застосування графових нейронних мереж, які дозволяють враховувати мережеву природу фінансових взаємодій. У транзакційних графах вузли можуть відповідати рахункам, користувачам або пристроям, а ребра – фінансовим операціям. Дослідження показують, що графові моделі здатні виявляти організовані шахрайські схеми, які залишаються непомітними для моделей, що аналізують транзакції ізольовано [1]. Подальший розвиток пов’язаний із використанням динамічних графових архітектур, які враховують еволюцію фінансових мереж у часі та підвищують адаптивність систем до нових стратегій шахрайства [4].

У задачах фінансового шахрайства актуальною залишається проблема значної нерівномірності розподілу класів. У зв’язку з цим активно досліджуються підходи виявлення аномалій, що дозволяють моделювати нормальну поведінку транзакційних потоків і фіксувати відхилення від неї.

Крім того, перспективним напрямом є використання федеративного навчання (federated learning), яке дозволяє кільком фінансовим установам спільно навчати моделі без обміну конфіденційними даними. Такий підхід сприяє формуванню більш узагальнених моделей і підвищує рівень інформаційної безпеки [5].

Сучасні системи виявлення шахрайства будуються як потокові аналітичні платформи, інтегровані у фінансові сервіси. Їхня архітектура передбачає використання модулів генерації ознак у реальному часі, сервісів прогнозування та підсистем моніторингу якості моделей.

Одним із ключових викликів є забезпечення стабільності роботи моделей у production-середовищі в умовах зміни концепції. Це потребує впровадження адаптивних стратегій навчання, автоматичного донавчання моделей і

використання гібридних рішень, що поєднують механізми на основі правил з методами машинного навчання.

Сучасні методи машинного навчання суттєво розширюють можливості виявлення фінансового шахрайства, забезпечуючи аналіз великих потоків транзакційних даних і підвищуючи здатність систем адаптуватися до нових типів загроз. Найбільш перспективними напрямами розвитку є використання графових нейронних мереж, темпоральних моделей і підходів федеративного навчання. Водночас практична ефективність таких рішень визначається не лише якістю алгоритмів, а й їх здатністю функціонувати у реальних фінансових системах із жорсткими вимогами до швидкодії, інтерпретованості та стабільності метрик.

Список використаних джерел:

1. Dou Y., Liu Z., Sun L., Deng Y., Peng H., Yu P. S. Enhancing Graph Neural Network-based Fraud Detectors against Camouflaged Fraudsters // *Proceedings of the 29th ACM International Conference on Information and Knowledge Management (CIKM '20)*. New York : ACM, 2020. P. 3158–3162. DOI: 10.1145/3340531.3411903.
2. Chen Y., Zhao C., Xu Y., Nie C., Zhang Y. Deep Learning in Financial Fraud Detection: Innovations, Challenges, and Applications // *Data Science and Management*. 2025. DOI: 10.1016/j.dsm.2025.08.002.
3. Gama J., Žliobaitė I., Bifet A., Pechenizkiy M., Bouchachia A. A Survey on Concept Drift Adaptation // *ACM Computing Surveys*. 2014. Vol. 46, No. 4. Article 44. DOI:10.1145/2523813.
4. Ren L., Hu R., Li D., Liu Y., Wu J., Zang Y., Hu W. Dynamic graph neural network-based fraud detectors against collaborative fraudsters // *Knowledge-Based Systems*. 2023. Vol. 278. Article 110888. DOI: 10.1016/j.knosys.2023.110888.
5. Yang Q., Liu Y., Chen T., Tong Y. Federated Machine Learning: Concept and Applications // *ACM Transactions on Intelligent Systems and Technology*. 2019. Vol. 10, No. 2. Article 12. P. 1–19. DOI: 10.1145/3298981.