ЖУРНАЛ
ЄВРОПЕЙСЬКОЇ ЕКОНОМІКИ
Том 24. № 4 (95). Жовтень–грудень 2025
Видання Західноукраїнського національного університету

Спиридон Д. ЛАМПРОПУЛОС,
Георгіос Л. ТАНАСАС,
Георгія Н. КОНТОГЕОРГА

ВИЯВЛЕННЯ ШАХРАЙСТВА В БАНКІВСЬКИХ ТРАНЗАКЦІЯХ З ВИКОРИСТАННЯМ ШТУЧНОГО ІНТЕЛЕКТУ ТА АНОНІМІЗОВАНИХ ДАНИХ

Резюме

У статті розглянуто здатність класифікаторів машинного навчання на основі штучного інтелекту, навчених на анонімних даних банківських транзакцій, ефективно виявляти шахрайські операції. У дослідженні перевірено гіпотезу H1: щонайменше один класифікатор має площу під кривою ROC-кривою (AUC) > 0,50 противагу нульовій гіпотезі H0, згідно з якою AUC найкращої моделі ≤ 0,50. Використовуючи анонімний набір даних, наданий комерційним банком зі США, оцінено широкий спектр класифікаторів, зокрема ансамблеві методи на основі дерев рішень, ймовірнісні, методи на основі відстані, лінійні та маржинальні алгоритми навчання, а також нейронну ме-

Лампропулос Спиридон Д., PhD, позаштатний доцент, кафедра управління туризмом, Патрський університет, Патри, Греція. ORCID: 0009-0003-6701-9427 Email: spyridonlampropoulos@upatras.gr
Танасас Георгіос Л., PhD, доцент, кафедра менеджменту і технологій, Патрський університет, Патри, Греція. ORCID: 0000-0002-7893-9363 Email: thanasasgeo@upatras.gr
Контогеорга Георгія Н., PhD, аудитор, Рахункова палата Греції, Афіни, Греція; афілійований дослідник, Університет Париж I Пантеон-Сорбонна, Париж, Франція. ORCID: 0000-0002-9830-324X Email: kont_georgia@yahoo.gr

режу із застосуванням програмного забезпечення Orange Data Mining. Оцінювання моделей здійснювалося за допомогою стратифікованої 10-кратної перехресної перевірки. Кілька моделей досягли значень AUC > 0,50, а методи деревного бустингу забезпечили найкращий баланс між виявленням шахрайства та обмеженням кількості хибнопозитивних спрацьовувань. Лінійні базові моделі та методи на основі відстані продемонстрували низьку ефективність, тоді як SVM забезпечив високий рівень повноти, попри операційно дорогий рівень хибнопозитивних спрацьовувань. Загалом отримані результати підтверджують H1 і не узгоджуються з H0. Дослідження пропонує прозорий, готовий до практичного використання в банківському секторі еталон на основі анонімних, реалістичних для виробничого середовища ознак, а запропонований підхід легко відтворюється для налаштування порогів прийняття рішень та систем управління у фінансових установах.

Ключові слова:

аналітика фінансових транзакцій, банківське шахрайство, банківські транзакції, класифікація машинного навчання, штучний інтелект, CatBoost, XGBoost.

Класифікація за JEL: G21, C45, C52, C55, M42.

1 таблиця, 1 рисунок, 32 джерела літератури.

Вступ

Штучний інтелект (ШІ) суттєво вплинув на фінансову та бухгалтерську сферу, трансформувавши процеси збору, перевірки, аналізу та виявлення аномалій у великих масивах даних. У середовищах фінансової звітності та процедур підтвердження, що базуються на штучному інтелекті, вилучення, аналіз і валідація даних можуть бути ефективно скоординовані на всіх етапах, що зменшує кількість ручних помилок, підвищує точність і рівень прозорості аудиту. Класифікатори машинного навчання (МН) широко застосовуються в банківському секторі для виявлення шахрайства на рівні транзакцій,

Том 24. № 4 (95). Жовтень–грудень 2025
ISSN 1684-906X

де патерни шахрайської поведінки є нелінійними, розрідженими та такими, що швидко змінюються (Bolton & Hand, 2002; Ngai et al., 2011).

Мета дослідження – дослідити системи ШІ, навчені на анонімному наборі даних, наданому комерційним банком із США (установа анонімізована); оцінити, чи можуть класифікатори ШІ/МН виявляти шахрайські транзакції. Для операціоналізації дослідницької мети використано розширений набір моделей (Random Forest, XGBoost, CatBoost, SVM, Neural Networks), оцінених із застосуванням стратифікованої перехресної перевірки, а також показників дискримінації й балансу помилок (AUC, F1, MCC), які є найбільш придатними для задач виявлення шахрайства з незбалансованими класами (Chicco & Jurman, 2020; Breiman, 2001; Chen & Guestrin, 2016; Cortes & Vapnik, 1995; Heaton, 2018).

Метою дослідження також є оцінка ефективності класифікаторів штучного інтелекту й машинного навчання (ШІ/МН) у виявленні шахрайських банківських операцій в умовах, наближених до реального виробничого середовища, з використанням винятково анонімних ознак.

Отже, основні гіпотези сформульовано так:

H1 (основна гіпотеза): класифікатори машинного навчання на основі штучного інтелекту, навчені на анонімних даних банківських транзакцій, здатні ефективно передбачати, чи є транзакція шахрайською (AUC > 0,50).

H0 (нульова гіпотеза): класифікатори машинного навчання на основі штучного інтелекту, навчені на анонімних даних банківських транзакцій, не забезпечують ефективного прогнозування шахрайства, оскільки показник AUC найкращої моделі не перевищує 0,50 (AUC ≤ 0,50).

Ця стаття: а) прозорий еталон оцінювання для порівняльного аналізу взаємодоповнювальних типів моделей, б) аналізує порогозалежну операційну поведінку моделей (AUC, точність прогнозу/повнота (precision / recall), MCC, матриці невідповідностей) та в) контекстуалізує емпіричні результати в контексті літератури з аналізу шахрайства для з'ясування, коли й чому окремі моделі штучного інтелекту перевершують лінійні або базові моделі на основі відстані у процесі використання банківських даних (Bolton & Hand, 2002; Ngai et al., 2011; Chen & Guestrin, 2016).

Решта статті організована таким чином: у розділі 2 представлено огляд літератури; у розділі 3 описано набір даних і змінні (усі анонімізовані), а також методологію та дизайн оцінювання; у розділі 4 наведено результати; у розділі 5 – практичні аспекти впровадження; у розділі 6 обговорено результати, їхні наслідки для моніторингу банківського шахрайства та напрямки подальших досліджень; у розділі 7 сформульовано висновки.

Огляд літератури та постановка проблеми

У фінансовій та бухгалтерській сферах штучний інтелект широко застосовується для підвищення ефективності й точності, проте результати залежать від організаційної готовності, якості даних та системи врядування. Згідно з оглядами впровадження штучного інтелекту, компанії отримують відчутні переваги за наявності надійних конвеєрів обробки даних і чіткого нагляду, тоді як відсутність цих чинників призводить до низької ефективності та дефіциту довіри (Cubric, 2020; Petkov, 2020). Цей контекст є принципово важливим для задач виявлення банківського шахрайства: навіть потужні алгоритми демонструватимуть низьку результативність за низької якості даних, слабкого контролю або моніторингу. Організація та готовність даних не є другорядними аспектами, оскільки саме вони визначають верхню межу ефективності будь-якої моделі, що навчається на банківських транзакціях.

Десятиліття досліджень показали, що шахрайство з транзакціями має три властивості, які ускладнюють прогнозування, а саме: а) суттєвий дисбаланс класів (шахрайських транзакцій значно менше, ніж легітимних платежів), б) зміна поведінкових патернів з часом у міру адаптації злочинців та в) асиметричність витрат (пропущений випадок шахрайства є дороговартісним, однак надмірна кількість хибнопозитивних спрацьовувань також призводить до значних витрат) (Bolton & Hand, 2002; Ngai et al., 2011). У зв'язку з цим виявлення шахрайства традиційно формулюється як задача навчання з учителем (класифікація кожної транзакції) у поєднанні з підходами виявлення аномалій (ідентифікація нетипової поведінки) (Bolton & Hand, 2002; Ngai et al., 2011; Bulatova et al., 2019; Kuryliak et al., 2025).

Нелінійні ансамблі дерев рішень особливо ефективні у процесі використання структурованих банківських даних. Random forest (англ. випадковий ліс) (Breiman, 2001) моделює взаємодії без складного конструювання ознак, а методи градієнтного бустингу (наприклад, XGBoost) ітеративно коригують помилки (Chen & Guestrin, 2016). У CatBoost категоріальні змінні обробляються нативно, а перенавчання зменшується завдяки упорядкованому бустингу (ordered boosting), що є особливо корисним, коли ознаки включають тип пристрою, канал та тип транзакції. Емпіричні дослідження, що додають часові або реляційні сигнали (послідовності або мережі між картками й торговцями), також показують, що гнучкі нелінійні алгоритми перевершують прості лінійні моделі або базові алгоритми на основі відстані (van Vlasselaer et al., 2015; Jurgovsky et al., 2018).

Через низьку частоту випадків шахрайства та асиметрію витрат використання лише показника точності прогнозу може бути оманливим. У науковій літературі зазначено такі рекомендації: а) використовувати показники дискримінації, що не залежать від порогових значень (AUC), б) аналізувати

точність прогнозу / повноту, зосереджену на міноритарному класі (шахрайстві), та в) використовувати збалансовані метрики, що враховують усі чотири комірки матриці невідповідностей, зокрема MCC (Fawcett, 2006; Saito & Rehmsmeier, 2015; Chicco & Jurman, 2020). Також заохочується очевидне врахування витрат під час навчання моделей (навчання з урахуванням витрат) та під час встановлення порогів прийняття рішень (Bahnsen et al., 2013; Bahnsen et al., 2015). Крім того, Pozzolo et al. (2018) наголошують, що оцінювання не повинно ґрунтуватися тільки на статичних випадкових невідповідностях, а має враховувати умови реального середовища (наприклад, часові розриви, концептуальний дрейф, затримки верифікації).

Разом ці висновки забезпечують чітку теоретичну основу для нашого дослідження. Ми навчили різноманітний набір класифікаторів ШІ/МН на анонімізованих даних банківських транзакцій та оцінили їх за допомогою AUC (дискримінація, нечутлива до порогових значень), точності прогнозу / повноти (фокус на міноритарному класі) та MCC (збалансована коректність класифікації) в межах стратифікованої перехресної перевірки.

Штучний інтелект сприяє виявленню шахрайства та аномальної фінансової активності, що підвищує достовірність і точність фінансової звітності, зменшуючи ризики її спотворення внаслідок шахрайських транзакцій, порушення цілісності аудиту та значних викривлень фінансової інформації (Wells, 2020). Системи виявлення шахрайства на основі машинного навчання здатні ідентифікувати аномалії швидше й точніше, ніж використання лише ручних процедур перевірки (Ngai et al., 2011). Моделі виявлення та прогнозування шахрайства, керовані штучним інтелектом, зокрема Random Forest, Gradient Boosting і Neural Networks, довели свою ефективність у виявленні поведінки з високим рівнем ризику в банківському середовищі, посилюючи системи внутрішнього контролю та забезпечуючи надійність фінансової звітності (Ryman-Tubb et al., 2018). Відтак оцінювання алгоритмів виявлення шахрайства безпосередньо сприяє глибшому розумінню того, як штучний інтелект може підвищити надійність і достовірність фінансових процесів.

Методологія та теоретичні засади

У дослідженні використано анонімізований набір даних про транзакції, наданий комерційним банком із США, який побажав бути невідомим. Базу даних надано на умовах дотримання конфіденційності, у зв'язку з чим необроблені транзакційні дані не можуть бути оприлюднені. Перед наданням доступу з набору даних вилучено всю інформацію, що могла б дозволити ідентифікацію фізичних осіб. Дослідження зосереджене тільки на виявленні шахрайства на рівні банківських транзакцій і призначене лише для дослідницьких цілей.

Цільова змінна (бінарна): *Is_Fraud (клас «1» розглядається як позитивний / цільовий клас у середовищі Orange)* (з англ.: Наявність_Шахрайства).

Особливості предиктора: *Transaction_Amount, Transaction_Type, Transaction_Time, Device_Used, Account_Age, Credit_Score, Previous_Fraud* (з англ.: Сума_транзакції, Тип_транзакції, Час_транзакції, Використаний_пристрій, Вік_рахунка, Кредитний_скоринг, Попереднє_шахрайство).

Типові банківські дані містять суму транзакції, часову мітку (дата й час), пристрій або канал здійснення операції, тип транзакції, тривалість існування й активності рахунка, а також бінарний індикатор попередніх випадків шахрайства.

За допомогою дескрипторів транзакцій, індикаторів каналів, інформації про клієнта / його рахунок та простої історії поведінки набір ознак відповідає усталеній практиці аналізу шахрайства на рівні транзакцій. Ознаки Transaction_Amount та Transaction_Time відображають величину та часові закономірності покупок, які часто відрізняють шахрайські операції від легітимних (Whitrow et al., 2009; Jurgovsky et al., 2018). Різні платіжні канали та вектори доступу (наприклад, операції з фізичною присутністю картки проти віддалених транзакцій, банкомат проти онлайн-каналу) неодноразово демонстрували відмінні профілі ризику (Bolton & Hand, 2002; Ngai et al., 2011). Ознака Account_Age відображає ефекти життєвого циклу рахунка (нові рахунки, як правило, мають вищий ризик), а Credit_Score надає узагальнену оцінку кредитного ризику, пов'язаного зі схильністю до шахрайства в операційних умовах (Ngai et al., 2011; Bhattacharyya et al., 2001). Ознака Previous_Fraud кодує мінімальну історію поведінки: попередньо підтверджені випадки шахрайства, як показано в літературі, є сильним операційним сигналом і широко використовуються в банківських правилах та моделях.

Цей перелік змінних є виробничо-придатним (не містить персональних даних), відповідає законодавчим обмеженням на використання банками та відображає ключові виміри, які в літературі пов'язуються з шахрайством: динаміку сум і часу транзакцій, канали та пристрої, зрілість і якість рахунків, а

Том 24. № 4 (95). Жовтень–грудень 2025
ISSN 1684-906X

також наявність негативних подій у минулому (Bolton & Hand, 2002; Ngai et al., 2011).

У статистиці ознак середовища Orange відсутні пропущені значення. Часові мітки транзакцій охоплюють вісім тижнів, починаючи з січня, а клас «1» відповідає шахрайству. Це дозволяє навчати моделі без імпутації даних і застосовувати коректні схеми оцінювання за умов дисбалансу класів.

Усі експерименти проведені в середовищі Orange Data Mining, візуальному аналітичному інструменті для побудови та оцінювання моделей машинного навчання (Demšar et al., 2013). Панель навчання охоплювала:

- **Лінійні базові моделі:** Ridge Regression та Lasso Regression (навмисно збережені як лінійні орієнтири для перевірки лінійної роздільності та формування консервативних базових моделей).
- **Методи на основі відстані:** k-Nearest Neighbors (kNN).
- **Методи на основі маржі:** Support Vector Machine (SVM).
- **Ймовірнісні моделі:** Naive Bayes.
- **Ансамблеві методи:** Random Forest, AdaBoost.
- **Методи градієнтного бустингу:** XGBoost, CatBoost.
- **Нейронна модель:** нейронна мережа.
- **Онлайн-лінійна модель:** Stochastic Gradient Descent (SGD).

Кілька попередніх досліджень показали, що ансамблі дерев рішень і методи бустингу добре працюють зі структурованими банківськими даними (Breiman, 2001; Chen & Guestrin, 2016), а лінійні моделі слугують інтерпретованими, консервативними базовими орієнтирами (Hoerl & Kennard, 1970; Tibshirani, 1996). Використання SVM, kNN, Naive Bayes і нейронних мереж доповнює відповідно маржинальні (margin-based), прикладо-орієнтовані (instance-based), ймовірнісні (probabilistic) та глибинні (deep learning) підходи до навчання (Cortes & Vapnik, 1995; Cover & Hart, 1967; Mitchell, 1997; Heaton, 2018).

У цьому дослідженні проведено оцінювання ефективності різних моделей машинного навчання. Обрані моделі представляють чотири основні категорії методів прогнозного навчання, що зазвичай застосовуються в аналітиці шахрайства: а) навчання на основі відстані (kNN), б) деревні ансамблеві методи (Random Forest, XGBoost, CatBoost, AdaBoost), в) ймовірнісні моделі (Naive Bayes) й г) лінійні та нелінійні дискримінаційні моделі навчання (SVM, Logistic / Ridge / Lasso Regression, Stochastic Gradient Descent, Neural Networks).

Згідно з попередніми науковими дослідженнями, шахрайські патерни часто є нелінійними, розрідженими та динамічними, що зумовлює необхідність порівняння простих інтерпретованих моделей із більш складними ансамблевими моделями на основі штучного інтелекту (Ngai et al., 2011). Зокрема, методи градієнтного бустингу на основі дерев рішень демонструють високу ефективність у роботі із структурованими фінансовими даними, завдяки здатності моделювати складні взаємодії між характеристиками та формувати нелінійні межі класів (Chen & Guestrin, 2016).

Передові моделі штучного інтелекту також порівнювалися з класичними моделями, зокрема Logistic Regression, Naive Bayes і kNN, що дало змогу безпосередньо пов'язати будь-яке спостережуване покращення саме з використанням передових моделей ШІ, а не з упередженістю набору даних. Відповідно до цього підходу, основною метою дослідження є демонстрація цінності штучного інтелекту в сучасних системах виявлення шахрайства шляхом порівняння прогнозних алгоритмів на основі ШІ з традиційними статистичними і правило-орієнтованими методами.

Для оцінювання використано віджет «Test & Score» (з англ.: «Тест і оцінка») у програмному середовищі Orange з такими налаштуваннями:

- **Протокол оцінювання:** застосовано стратифіковану 10-кратну перехресну перевірку, за якої параметр stratified забезпечує збереження пропорцій класів у кожному фолді за можливості, що дозволяє отримати надійні оцінки з низькою дисперсією в умовах дисбалансу класів.
- **Цільовий клас:** як позитивний визначено клас «1», що є принципово важливим для коректного обчислення покласових метрик і подальшого PR- та ROC-аналізу.
- **Вихідні дані для діагностики:** для кожної моделі сформовано показники ефективності та матриці невідповідностей (за допомогою віджета Confusion Matrix) з метою детального аналізу характеру класифікаційних помилок, зокрема співвідношення хибних-позитивних і хибних-негативних результатів.

Ефективність оцінювалася на рівні дискримінаційної здатності з використанням перехресної перевірки, при цьому основним критерієм був показник AUC.

В операційному сенсі ефективність інтерпретувалася як перевищення середнього значення AUC, отриманого за результатами перехресної перевірки, порогового рівня 0,50 принаймні для однієї моделі. Оцінювання здійснювалося у поєднанні з додатковими діагностичними показниками (точність прогнозу / повнота, F1, MCC та матриці невідповідностей) з метою виключення дегенеративних режимів роботи моделей. Це правило було визначене

заздалегідь і не передбачало апріорного виділення будь-якої конкретної моделі.

Віджет Test & Score у середовищі Orange надає стандартний набір показників якості класифікації. Нижче наведено метрики, використані в дослідженні, та їхні офіційні визначення:

- **AUC (Area Under the ROC Curve, площа під ROC-кривою):** імовірність того, що класифікатор присвоїть випадково вибраному позитивному прикладу вищий ранг, ніж випадково вибраному негативному; обчислюється у віджеті Test & Score та додатково аналізується за допомогою віджета ROC Analysis.
- **CA (Classification Accuracy), точність класифікації:** частка правильно класифікованих прикладів серед усіх класів.
- **Precision (точність прогнозу):** частка істинно позитивних випадків серед усіх прикладів, передбачених як позитивні.
- **Recall (Sensitivity), повнота / чутливість:** частка істинно позитивних випадків серед усіх фактичних позитивних прикладів.
- **F1-score (F1-міра):** гармонійне середнє показників precision (точності прогнозу) та recall (повноти).
- **MCC (Matthews Correlation Coefficient, коефіцієнт кореляції Метьюза):** збалансований кореляційний індекс, що враховує всі чотири комірки матриці невідповідностей.
- **Матриця невідповідностей (Confusion Matrix, діагностична):** таблиця співвідношення передбачених і фактичних класів для візуалізації хибно позитивних та хибно негативних результатів, а також помилок за класами.

Оскільки шахрайство є рідкісним явищем, а витрати класифікаційних помилок – асиметричними, використання лише показника точності класифікації може бути оманливим. Застосування AUC, precision / recall і F1, а також коефіцієнта MCC відповідає усталеним, найкращим практикам оцінювання моделей у задачах із незбалансованими класами (Fawcett, 2006; Saito & Rehmsmeier, 2015; Chicco & Jurman, 2020).

Результати дослідження

Для оцінювання прогностичної ефективності кількох моделей машинного навчання з цільовою змінною Is_Fraud застосовано стратифіковану 10-кратну перехресну перевірку. Серед показників оцінювання використовувалися AUC (Fawcett, 2006), точність класифікації, точність прогнозу, повнота (Saito & Rehmsmeier, 2015), F1-score та коефіцієнт кореляції Метьюза (MCC), який, враховуючи всі компоненти матриці невідповідностей, забезпечує надійну оцінку ефективності класифікації в умовах дисбалансу класів (Chicco & Jurman, 2020).

Таблиця 1

Підсумок оцінювання моделей

Model	AUC	Accuracy	F1	Precision	Recall	MCC
CatBoost	*0,737*	*0,733*	*0,345*	*0,566*	*0,248*	*0,236*
Naive Bayes	0,740	0,729	0,283	0,567	0,188	0,202
Ridge Regression	0,567	0,716	0,000	0,000	0,000	0,000
Lasso Regression	0,516	0,716	0,000	0,000	0,000	0,000
XGBoost	0,703	0,704	0,368	0,467	0,303	0,193
Random Forest	0,642	0,690	0,338	0,428	0,279	0,152
kNN	0,510	0,657	0,198	0,294	0,149	0,010
AdaBoost	0,572	0,646	0,391	0,382	0,401	0,142
Neural Network	0,500	0,543	0,332	0,284	0,400	0,000
Stochastic Gradient Descent	0,500	0,500	0,362	0,284	0,500	0,000
SVM	0,499	0,329	0,431	0,284	0,897	0,001

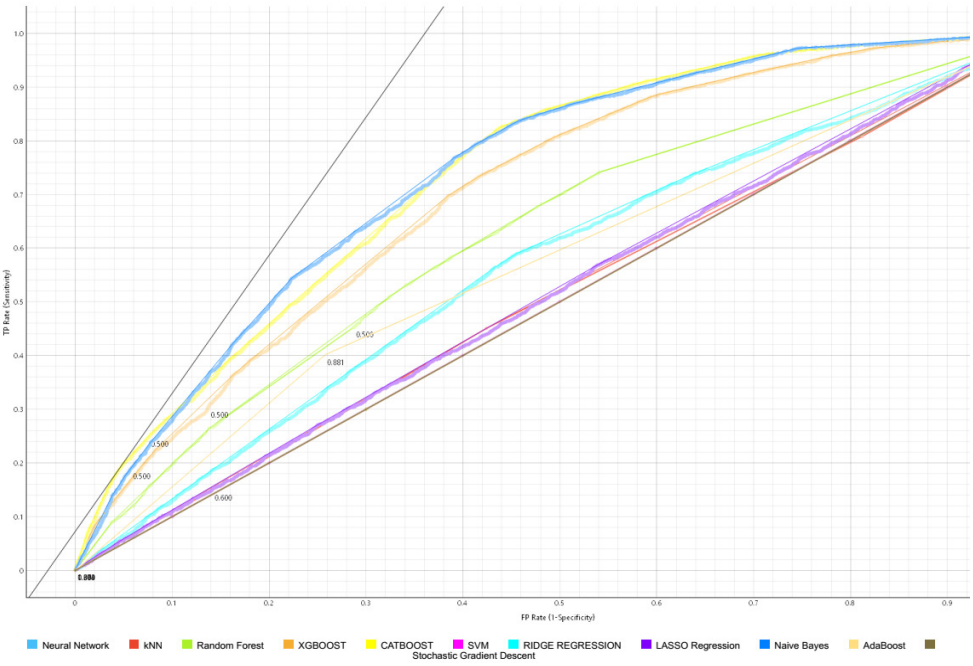
Джерело: розраховано авторами.
Примітка. AUC – площа під ROC-кривою; Accuracy – точність класифікації; F1; Precision – точність прогнозу; Recall – повнота; MCC – коефіцієнт кореляції Метьюза. Оцінювання виконано за допомогою стратифікованої 10-кратної перехресної перевірки.

На рис. 1 наведено ROC-криві для всіх класифікаторів, де шахрайство визначено як позитивний клас. Naive Bayes і CatBoost формують верхню огинаючу криву; за ними з незначним відставанням слідує XGBoost, водночас Random Forest демонструє слабші результати, що узгоджується з ранжуванням за AUC у зведенні оцінювання моделей. kNN та AdaBoost, базові моделі,

розташовані ближче до діагоналі 45°, а лінійні моделі та неналаштована нейронна мережа фактично слідують цій діагоналі. Це відповідає значенням AUC, близьким до 0,50. Хоча Naive Bayes має дещо вищий AUC порівняно з CatBoost, показник MCC є нижчим через меншу повноту та менш сприятливий операційний баланс, що відображається у формі ROC-кривої та підтверджується матрицями невідповідностей. Отримані ROC-профілі узгоджуються з попередніми результатами та підтверджують доцільність поєднання ROC-аналізу з показниками precision–recall і MCC у задачах із незбалансованими класами (Fawcett, 2006; Saito & Rehmsmeier, 2015).

Рисунок 1

ROC-криві моделей класифікаторів



Джерело: розроблено авторами.

CatBoost (модель з найкращими показниками)

CatBoost продемонстрував найбільш збалансовану ефективність (AUC = 0,737; MCC = 0,236). Матриця невідповідностей засвідчила, що модель правильно виявила 704 випадки шахрайства (істинно позитивні), пропустила 2134 випадки (хибнонегативні) та помилково класифікувала 540 транзакцій як шахрайські (хибнопозитивні). Модель ефективно ідентифікувала шахрайські операції, водночас утримуючи кількість хибнопозитивних результатів на контрольованому рівні, що робить її найбільш надійною та операційно придатною серед розглянутих моделей. Упорядкований бустинг (ordered boosting) та нативна підтримка категоріальних ознак у CatBoost сприяють зниженню перенавчання під час роботи зі структурованими фінансовими даними та покращують здатність моделі до узагальнення.

Naive Bayes

Naive Bayes продемонстрував високу точність прогнозу (0,567), проте дуже низьку повноту (0,188). Матриця невідповідностей показала 534 виявлені випадки шахрайства (TP), 2 304 пропущені (FN) та 408 хибнопозитивних спрацювань (FP), що вказує на обережний характер виявлення шахрайства. Така поведінка зумовлена сильним припущенням умовної незалежності ознак, яке рідко відповідає динаміці фінансового шахрайства (Mitchell, 1997).

Ridge Regression та Lasso Regression

Ridge Regression і Lasso Regression класифікували всі транзакції як нешахрайські, що призвело до значень F1 = 0 та MCC = 0. Матриці невідповідностей містили 0 TP, 2838 FN, 0 FP та 7162 TN. Ці лінійні моделі не здатні виявляти нелінійні патерни шахрайства, характерні для даних фінансової поведінки (Hoerl & Kennard, 1970; Tibshirani, 1996).

XGBoost

Баланс між виявленням шахрайства та кількістю хибних спрацювань був кращим у XGBoost (AUC = 0,703; MCC = 0,193). Матриця невідповідностей показала 861 виявлений випадок шахрайства (TP), 1977 пропущених (FN) та 982 хибнопозитивні спрацювання (FP), що є кращим компромісом, ніж Random Forest. Це узгоджується зі здатністю градієнтного бустингу поступово усувати помилки (Chen & Guestrin, 2016).

Random Forest

Помірну ефективність продемонстрував Random Forest (AUC = 0,642; MCC = 0,152). Матриця невідповідностей показала 779 виявлених випадків шахрайства (TP), 2059 пропущених (FN) та 1061 хибнопозитивне спрацювання щодо легітимних транзакцій (FP). Це узгоджується з консервативним характером моделі, тобто кількість хибнопозитивних результатів нижча за рахунок пропуску частини шахрайських операцій (Breiman, 2001).

k-Nearest Neighbors (kNN)

kNN продемонстрував дуже низьку повноту (0,149) та слабку загальну дискримінаційну здатність (MCC = 0,010). Матриця невідповідностей засвідчила 422 правильно виявлені випадки шахрайства (TP), 2416 шахрайських транзакцій, помилково класифікованих як легітимні (FN), та 1011 легітимних транзакцій, хибно позначених як шахрайські (FP). Це свідчить про сильну упередженість моделі до домінантного нешахрайського класу, що є очікуваним, коли подібність на основі відстані не відображає поведінкові патерни шахрайства (Cover & Hart, 1967).

AdaBoost

AdaBoost продемонстрував середній рівень ефективності (F1 = 0,391). Матриця невідповідностей показала 1138 виявлених випадків шахрайства (TP), 1 700 пропущених (FN) та 1843 хибнопозитивні спрацювання (FP), що вказує на підвищену чутливість до виявлення шахрайства за рахунок зростання кількості хибнопозитивних результатів і, відповідно, нижчу точність прогнозу (Freund & Schapire, 1997).

Neural Network (Нейронна мережа)

Дискримінаційна здатність нейронної мережі виявилась слабкою (AUC = 0,500; MCC = 0,000). Матриця невідповідностей показала 1136 правильно виявлених випадків шахрайства (TP), 1702 пропущені (FN) та 2864 легітимні транзакції, помилково позначені як шахрайські (FP), що підтверджує низьку ефективність моделі. Це узгоджується з відомими обмеженнями недостатньо налаштованих нейронних моделей на табличних даних (Heaton, 2018).

Stochastic Gradient Descent (SGD)

SGD продемонстрував нестабільну та слабку класифікаційну здатність (AUC = 0,500; MCC = 0,000). Це свідчить про труднощі у формуванні розділювальних меж у цьому наборі даних (Bottou, 2010).

Support Vector Machine (SVM)

Модель SVM досягла високої повноти (0,897), правильно виявивши 2 545 випадків шахрайства (TP), однак супроводжувалася 6418 хибнопозитивними спрацюваннями (FP) та 293 пропущеними випадками (FN). Точність прогнозу залишалася низькою (0,284) (Saito & Rehmsmeier, 2015). Такий дисбаланс робить SVM непридатною для практичного використання в реальних системах скринінгу шахрайства, де вартість хибних тривог є високою (Cortes & Vapnik, 1995).

CatBoost визначено як найсильнішу модель, що забезпечує найкращий баланс між здатністю виявляти шахрайство та контролювати хибнопозитивні спрацьовування, що робить її найбільш придатним кандидатом для реальних

систем моніторингу та втручання у випадках фінансового шахрайства. Оскільки кілька моделей досягли значень AUC (Fawcett, 2006), що суттєво перевищують 0,50 (зокрема, Naive Bayes = 0,740; CatBoost = 0,737), отримані результати підтверджують H1 і не узгоджуються з H0 для цього набору даних. CatBoost ідентифіковано як «найкращу загалом» модель на основі збалансованої ефективності (найвище значення MCC = 0,236) у поєднанні з конкурентоспроможним AUC. Таким чином, основну гіпотезу H1 прийнято, а нульову гіпотезу H0 відхилено.

Практичне застосування

Емпіричні результати можуть бути інтерпретовані як основа робочого процесу комерційної системи скринінгу шахрайства в банківських установах. По-перше, моделі, що демонструють надійну дискримінаційну здатність і збалансовану поведінку в разі виявлення помилок (відображену показниками AUC у поєднанні з precision/recall та MCC), є придатними для використання як первинний рівень оцінювання транзакцій і формування показника ризику шахрайства для кожної транзакції. По-друге, банки можуть встановлювати та періодично переглядати порогові значення прийняття рішень з урахуванням операційних можливостей і асиметричних витрат (зокрема, вартості пропущеного випадку шахрайства порівняно з вартістю розслідування хибного спрацювання) (He & Garcia, 2009; Bahnsen et al., 2015). По-третє, модель має бути інтегрована в систему управлінського контролю (governance), що передбачає:

- регулярний моніторинг показників ефективності для виявлення їхньої деградації в міру еволюції шахрайських патернів (Pozzolo et al., 2018);
- планове перенавчання моделі з використанням нещодавно отриманих маркованих результатів за їх наявності;
- чітко визначені протоколи ескалації, які забезпечують своєчасний розгляд випадків з високим рівнем ризику, а транзакції з низьким рівнем ризику обробляються у штатному режимі.

Незважаючи на те, що дані є анонімізованими, практичне впровадження таких моделей у банківському середовищі все одно потребує належної документації, перевірки, постійного моніторингу та забезпечення аудиту відповідно до вимог управління модельними ризиками (Division of Banking Supervision and Regulation, 2011), що має підтримуватися ефективною системою управління ризиковими даними та практиками звітності (Basel Committee on Banking Supervision, 2013).

Обговорення

У дослідженні проаналізовано чотири сімейства загальних класифікаторів, які широко застосовуються в аналітиці шахрайства: а) методи на основі відстані (k-nearest neighbors), б) ансамблеві методи на основі дерев рішень (Random Forest, XGBoost, CatBoost, AdaBoost), в) ймовірнісні моделі (Naive Bayes) та г) лінійні та маржинальні дискримінаційні моделі (Ridge/Lasso, Stochastic Gradient Descent, Support Vector Machines), а також ґ) нейронну мережу. Попередні дослідження свідчать, що патерни шахрайства в транзакційних даних є нелінійними та змінюються з часом, що зумовлює доцільність порівняння гнучких ансамблевих методів із простими базовими моделями (Ngai et al., 2011). Дерева градієнтного бустингу часто демонструють високу ефективність на структурованих банківських даних, оскільки здатні моделювати взаємодію ознак та складні межі прийняття рішень (Chen & Guestrin, 2016).

Отримані результати узгоджуються з H1 і не узгоджуються з H0, оскільки декілька класифікаторів демонструють рівень дискримінації, суттєво вищий за 0,5 за показником AUC на цьому наборі даних.

Серед сімейств моделей деревні методи градієнтного бустингу забезпечили найвищий рівень дискримінаційної здатності та збалансованості помилок на анонімних даних банківських транзакцій. Найвищі значення AUC отримано для Naive Bayes та CatBoost (AUC ≈ 0,74 для обох моделей), водночас CatBoost продемонстрував найвищий показник MCC (≈ 0,24) і найбільш збалансоване представлення помилок. Матриця невідповідностей CatBoost засвідчила 704 істинно позитивні результати (TP), 2134 хибнонегативні (FN) та 540 хибнопозитивні (FP), що вказує на обережний підхід до маркування шахрайства за умови стриманої кількості хибних спрацьовувань (Chicco & Jurman, 2020).

Хоча Naive Bayes демонструє дещо вищий AUC, ніж CatBoost, його недостатня повнота зумовлює суттєво нижче значення MCC, що свідчить про нестабільний загальний баланс помилок на незбалансованих даних (Chicco & Jurman, 2020). З огляду на це CatBoost визначено як найкращу модель за сукупною ефективністю.

XGBoost (AUC ≈ 0,70; MCC ≈ 0,19) продемонстрував подібні результати з 861 TP, 1977 FN та 982 FP, що узгоджується з очікуваною ефективністю градієнтного бустингу на структурованих фінансових даних (Chen & Guestrin, 2016). Random Forest (AUC ≈ 0,64; MCC ≈ 0,15) показав помірну ефективність із 779 TP, 2059 FN та 1061 FP і був здатний враховувати взаємодію ознак, хоча й у консервативніших рамках (Breiman, 2001).

Naive Bayes, незважаючи на високий показник AUC, продемонстрував високу точність прогнозу, але низьку повноту (precision ≈ 0,57; recall ≈ 0,19) з 534 істинно позитивними результатами (TP), 2304 хибнонегативними (FN) та 408 хибнопозитивними (FP). Це є типовим проявом припущення умовної незалежності ознак у присутності складних і взаємозалежних патернів фінансового шахрайства (Mitchell, 1997).

Порівняно з базовими моделями з відмінними характеристиками, SVM досяг високої повноти (≈ 0,90), однак за операційно неприйнятного рівня хибнопозитивних спрацювань (2545 TP, 293 FN та 6418 FP), що відображає відому чутливість цієї моделі до дисбалансу класів і вибору порогових значень (Cortes & Vapnik, 1995). kNN продемонстрував низьку повноту (≈ 0,15) з 422 TP, 2416 FN та 1011 FP, що є очікуваним у випадках, коли відстань між спостережуваними значеннями не відображає подібності поведінкових патернів (Cover & Hart, 1967). Нейронна мережа та SGD продемонстрували ефективність на рівні випадкового вгадування (AUC = 0,50) (Hoerl & Kennard, 1970; Tibshirani, 1996; Heaton, 2018; Bottou, 2010), тоді як Ridge та Lasso деградували до класифікації класу більшості (0 TP, 2838 FN, 0 FP), що додатково вказує на нелінійний характер патернів шахрайства.

У випадку категоріальних каналів, типів пристроїв і гетерогенних поведінкових патернів банківських транзакцій регульований деревний бустинг продемонстрував найнадійніші операційні результати, а лінійні чи методи на основі відстані або недостатньо виявляли шахрайство, або генерували надмірну кількість хибнопозитивних спрацьовувань.

Оскільки шахрайство є рідкісним явищем, а витрати класифікаційних помилок – асиметричними, використання тільки одного показника точності класифікації може виявитись оманливим. У цьому контексті доцільно застосовувати показники AUC, точності прогнозу / повноти, F1 та MCC (Fawcett, 2006; Saito & Rehmsmeier, 2015; Chicco & Jurman, 2020). Зазначені закономірності є типовими для задач виявлення шахрайства: Naive Bayes забезпечує високу точність прогнозу (тобто невелику кількість хибних тривог), однак залишає непоміченими значну кількість шахрайських операцій; SVM досягає високої повноти, існує надзвичайно висока частка хибнопозитивних спрацьовувань. Натомість моделі деревного бустингу демонструють збалансовану поведінку помилок, яку можна додатково налаштовувати шляхом зміни порогів прийняття рішень щодо структури витрат, відповідно до вимог банку (Chen & Guestrin, 2016). Порогові значення спрацювання в банківських системах узгоджуються з асиметрією витрат. Водночас налаштування порогів або навчання з урахуванням витрат дозволяють балансувати між точністю прогнозу та його повнотою (He & Garcia, 2009; Bahnsen et al., 2015).

Висновки

У дослідженні оцінено широкий спектр класифікаторів AI/ML на анонімному наборі даних банківських транзакцій, використовуючи стратифіковану 10-кратну перехресну перевірку та метрики оцінювання, оптимальні для виявлення шахрайства за умов дисбалансу класів (AUC, точність прогнозу / повнота, F1, MCC). Регульовані деревні методи бустингу продемонстрували найкращі операційні профілі: CatBoost досяг AUC = 0,737 і MCC = 0,236 за помірного рівня хибнопозитивних спрацьовувань (TP = 704, FN = 2134, FP = 540). XGBoost також проявив хорошу ефективність (AUC = 0,703, MCC = 0,193, TP = 861, FN = 1977, FP = 982). Naive Bayes отримав найвище значення AUC (0,740) за мінімальної повноти (0,188) (TP = 534, FN = 2304, FP = 408), що відповідає його консервативній природі з пропуском значної частини шахрайських операцій. Лінійні базові моделі Ridge/Lasso деградували до класифікації класу більшості (TP = 0, FN = 2838, FP = 0), а SVM досяг дуже високої повноти (0,897) ціною 6418 хибнопозитивних спрацьовувань.

Такі результати підтверджують H1 («класифікатори машинного навчання, навчені на анонімних даних банківських транзакцій, здатні ефективно передбачати шахрайство, AUC > 0,50») та не узгоджуються з H0 («ефективність найкращої моделі не перевищує AUC ≤ 0,50»). Отримані результати узгоджуються з попередніми дослідженнями, які свідчать, що дерева градієнтного бустингу доволі ефективно працюють зі структурованими фінансовими даними, а коефіцієнт MCC є інформативним узагальнювальним показником за наявності дисбалансу класів (Breiman, 2001; Chen & Guestrin, 2016; Chicco & Jurman, 2020).

На цьому наборі даних дерева градієнтного бустингу (CatBoost / XGBoost) забезпечують достатній баланс між виявленням шахрайства та контролем обсягу хибних спрацьовувань. Зокрема, структура помилок у матриці невідповідностей CatBoost (TP = 704; FP = 540) свідчить про меншу кількість необґрунтованих ескалацій порівняно з моделлю SVM, яка, попри високу повноту, характеризується надмірною кількістю хибнопозитивних спрацьовувань (FP = 6418). Банки можуть обирати моделі деревного бустингу як детектори першої лінії та налаштовувати порогові значення відповідно до власних співвідношень витрат (відносної вартості кожного хибного спрацьовування та вартості пропущеного випадку шахрайства). Такий підхід узгоджується з найкращими практиками у сфері незбалансованої класифікації, де порогові значення або навчання з урахуванням витрат адаптуються до обмежень бізнесу (He & Garcia, 2009; Bahnsen et al., 2015).

Водночас вибір моделі є лише одним із чинників. Для успішного впровадження критично важливими є якісні конвеєри обробки даних, постійний моніторинг та належний нагляд, які малоефективні для продуктивного банківського застосування (Cubric, 2020). Фінансовим установам рекомендується

впроваджувати: а) періодичне калібрування порогових значень відповідно до поточного рівня шахрайської активності, б) моніторинг змін у даних та цикли перенавчання для реагування на нові патерни шахрайської поведінки, а також в) чітко визначені шляхи ескалації, що забезпечать зосередження уваги аналітиків на найбільш значущих сигналах про ризик (Bolton & Hand, 2002; Pozzolo et al., 2018).

З огляду на це сучасні моделі деревного бустингу з постфактумним налаштуванням порогів є одними з найпереконливіших емпіричних обґрунтувань для їх практичного використання як високоефективної базової моделі в банках. Подібний підхід дозволяє посилити превентивні механізми контролю і зменшити фінансові втрати, водночас зберігши навантаження на аналітиків на контрольованому рівні (Chen & Guestrin, 2016).

Що стосується обмежень дослідження, транзакційні дані охоплюють лише перші шість тижнів 2025 р. (від початку січня до середини лютого). Отримані результати можуть змінюватися під впливом сезонних факторів чи появи нових схем шахрайства. Набір даних походить з одного банку, розташованого у США, тому зовнішня валідність результатів може підвищитись у разі реплікації дослідження в кількох фінансових установах. У межах обмеженого набору даних були доступні лише транзакційні та базові характеристики рахунків. Мережеві й послідовні ознаки (зокрема «продавець – картка» та динаміка сесій) зазвичай забезпечують додаткове підвищення ефективності виявлення шахрайства (van Vlasselaer et al., 2015; Jurgovsky et al., 2018).

Стійкість моделей є предметом подальших досліджень. Перевірка з урахуванням часової впорядкованості даних і послідовні оновлення моделей дозволили б кількісно оцінити ефективність їхньої адаптації до постійної еволюції патернів шахрайства (Pozzolo et al., 2018). По-друге, навчання та калібрування моделей з урахуванням витрат, залежних від індивідуальних випадків, а також матриць збитків окремих банків дозволило б формувати прогнози, що ґрунтуються не лише на статистичній відповідності, а й на операційній економіці (Bahnsen et al., 2015). Зрештою, зовнішня перевірка на різних часових інтервалах, у різних географічних контекстах і фінансових установах є необхідною для оцінювання можливості узагальнення результатів та виявлення потенційних упереджень, специфічних для окремих наборів даних.

Це дослідження пропонує чіткий, практико-орієнтований підхід до виявлення шахрайства у банківський транзакціях на основі анонімних транзакційних даних. У працях здійснено порівняльну оцінку різних моделей-класифікаторів у межах стратифікованої перехресної перевірки та продемонстровано здатність деревного (градієнтного) бустингу забезпечити ефективну дискримінацію на основі анонімних, реалістичних для виробничого середовища характеристик, а лінійні та методи на основі відстані є недостатньо надійними. Отримані результати створюють чіткий орієнтир як для економістів, так і для менеджерів з ризиків, який можна відтворити, перевірити та розширити під час розробки нових підходів з урахуванням витрат і побудови пояснюваних систем моніторингу банківського шахрайства.

Декларація про доступність даних

Набір даних на рівні транзакцій, проаналізований у цьому дослідженні, отримано від банківської установи з дотриманням обмежень конфіденційності. Хоча дані є анонімізованими та не містять інформації, що дозволяє ідентифікувати особу, первинні записи є власністю надавача даних і не можуть бути розміщені у відкритому репозиторії або включені до додатків статті. Щоб забезпечити прозорість та відтворюваність методології, в роботі наведено повний перелік ознак, протокол оцінювання та результати ефективності моделей. З питань, що стосуються набору даних і дизайну дослідження, читачі можуть звертатися до відповідального автора (д-р. Спиридон Д. Лампропулос, spyridonlampropoulos@upatras.gr) з урахуванням чинних обмежень конфіденційності.

Декларація про етичні міркування

Набір даних надано в анонімізованій формі, проте він не містить прямих ідентифікаторів. Використання цього набору даних обмежується тільки науково-дослідницькими цілями в межах вимог конфіденційності, і жодних спроб повторної ідентифікації окремих осіб або організацій не здійснювалося.

Список використаної літератури

Bahnsen, A. C., Aouada, D., & Ottersten, B. (2015). Example-dependent cost-sensitive decision trees. *Expert Systems with Applications, 42*(19), 6609–6619. https://doi.org/10.1016/j.eswa.2015.04.042

Bahnsen, A. C., Stojanovic, A., Aouada, D., & Ottersten, B. (2013). Cost sensitive credit card fraud detection using Bayes Minimum Risk. In *2013 12th International Conference on Machine Learning and Applications* (pp. 333–338). https://doi.org/10.1109/icmla.2013.68

Basel Committee on Banking Supervision. (2013, January). *Principles for effective risk data aggregation and risk reporting* (BCBS Working paper No. 239). Bank for International Settlements. https://www.bis.org/publ/bcbs239.pdf

Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems, 50*(3), 602–613. https://doi.org/10.1016/j.dss.2010.08.008

Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science, 17*(3), 235–249. http://www.jstor.org/stable/3182781

Bottou, L. (2010). Large-scale machine learning with stochastic gradient descent. In Y. Lechevallier & G. Saporta (Eds.), *Proceedings of COMPSTAT'2010* (pp. 177–186). Physica-Verlag HD. https://doi.org/10.1007/978-3-7908-2604-3_16

Breiman, L. (2001) Random forests. *Machine Learning*, *45*(1), 5–32. https://doi.org/10.1023/a:1010933404324

Bulatova, O., Kuryliak, V., Savelyev, Y., Zakharova, O., & Sachenko, S. (2019, September). Modeling the multi-dimensional indicators of regional integration processes [Conference presentation abstract]. In *2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* (pp. 1024–1029), Metz, France. https://doi.org/10.1109/IDAACS.2019.8924430

Chen, T., & Guestrin, C. (2016, August 13–17). XGBoost: A scalable tree boosting system (pp. 785–794). In *2016 KDD '16: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, San Francisco, USA. Association for Computing Machinery. https://doi.org/10.1145/2939672.2939785

Chicco, D., & Jurman, G. (2020). The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation. *BMC Genomics*, *21*(1), Article 6. https://doi.org/10.1186/s12864-019-6413-7

Cortes, C., & Vapnik, V. (1995). Support-vector networks. *Machine Learning, 20*(3), 273–297. https://dx.doi.org/10.1007/BF00994018

Cover, T. M., & Hart, P. E. (1967). Nearest neighbor pattern classification. *IEEE Transactions on Information Theory, 13*(1), 21–27. https://isl.stanford.edu/~cover/papers/transIT/0021cove.pdf

Cubric, M. (2020). Drivers, barriers and social considerations for AI adoption in business and management: A tertiary study. *Technology in Society, 62*, Article 101257. https://doi.org/10.1016/j.techsoc.2020.101257

Demšar, J., Curk, T., Erjavec, A., Gorup, Č., Hočevar, T., Milutinovič, M., Možina, M., Polajnar, M., Toplak, M., Starič, A., Štajdohar, M., Umek, L., Žagar, L., Žbontar, J., Žitnik, M., & Zupan, B. (2013). Orange: Data mining toolbox in Python. *Journal of Machine Learning Research, 14*, 2349–2353. https://www.jmlr.org/papers/v14/demsar13a.html

Division of Banking Supervision and Regulation. (2011, April 4). *SR 11-7: Guidance on model risk management* [Supervision and Regulation letter].

Board of Governors of the Federal Reserve System, Washington, D.C. https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm

Fawcett, T. (2006). An introduction to ROC analysis. *Pattern Recognition Letters, 27*(8), 861–874. https://doi.org/10.1016/j.patrec.2005.10.010

Freund, Y., & Schapire, R. E. (1997). A decision-theoretic generalization of on-line learning and an application to boosting. *Journal of Computer and System Sciences, 55*(1), 119–139. https://doi.org/10.1006/jcss.1997.1504

He, H., & Garcia, E. A. (2009). Learning from imbalanced data. *IEEE Transactions on Knowledge and Data Engineering, 21*(9), 1263–1284. https://doi.org/10.1109/TKDE.2008.239

Heaton, J. (2018). Ian Goodfellow, Yoshua Bengio, and Aaron Courville: Deep learning. *Genetic Programming and Evolvable Machines, 19*(1–2), 305–307. https://doi.org/10.1007/s10710-017-9314-z

Hoerl, A. E., & Kennard, R. W. (1970). Ridge Regression: Biased estimation for nonorthogonal problems. *Technometrics*, *12*(1), 55–67. https://doi.org/10.1080/00401706.1970.10488634

Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P.-E., He-Guelton, L., & Caelen, O. (2018). Sequence classification for credit-card fraud detection. *Expert Systems with Applications, 100*, 234–245. https://doi.org/10.1016/j.eswa.2018.01.037

Kuryliak, V., Lyzun, M., Hayda, Y., Lishchynskyy, I., & Ukhova, N. (2025). Cross-correlation analysis of dynamic interdependencies between socioeconomic development and the demand for higher education in Ukraine. *Journal of European Economy*, *24*(3), 467–485. https://doi.org/10.35774/jee2025.03.467

Mitchell, T. M. (1997). *Machine Learning*. McGraw-Hill. https://www.cs.cmu.edu/~tom/mlbook.html

Ngai, E. W. T, Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2010). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, *50*(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006

Petkov, R. (2020). Artificial intelligence (AI) and the accounting function – A revisit and a new perspective for developing framework. *Journal of Emerging Technologies in Accounting, 17*(1), 99–105. https://doi.org/10.2308/jeta-52648

Pozzolo, A. D., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2018). Credit card fraud detection: A realistic modeling and a novel learning strategy. *IEEE Transactions on Neural Networks and Learning Systems, 29*(8), 3784–3797. https://doi.org/10.1109/TNNLS.2017.2736643

Ryman-Tubb, N. F., Krause, P., & Garn, W. (2018). How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. *Engineering Applications of Artificial Intelligence, 76*, 130–157. https://doi.org/10.1016/j.engappai.2018.07.008

Saito, T., & Rehmsmeier, M. (2015). The precision-recall plot is more informative than the ROC plot when evaluating binary classifiers on imbalanced datasets. *PLoS ONE, 10*(3), Article e0118432. https://doi.org/10.1371/journal.pone.0118432

Tibshirani, R. (1996). Regression shrinkage and selection via the Lasso. *Journal of the Royal Statistical Society: Series B (Methodological)*, *58*(1), 267–288. https://doi.org/10.1111/j.2517-6161.1996.tb02080.x

Van Vlasselaer, V., Bravo, C., Caelen, O., Eliassi-Rad, T., Akoglu, L., Snoeck, M., & Baesens, B. (2015). APATE: A novel approach for automated credit card transaction fraud detection using network-based extensions. *Decision Support Systems, 75*, 38–48. https://doi.org/10.1016/j.dss.2015.04.013

Wells, J. T. (2020). *Principles of fraud examination* (6th ed.). Wiley.

Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N. (2009). Transaction aggregation as a strategy for credit card fraud detection. *Data Mining and Knowledge Discovery, 18*(1), 30–55. https://doi.org/10.1007/s10618-008-0116-z

Отримано: 18 вересня 2025 р.
Рецензовано: 27 жовтня 2025 р.
Рекомендовано до друку: 3 грудня 2025 р.