Облік і оподаткування

УДК 330.3+65:336

Парасій-Вергуненко Ірина Михайлівна
доктор економічних наук,
професор кафедри фінансового аналізу та аудиту
Державний торговельно-економічний університет
Parasii-Verhunenko Iryna
Doctor of Economics, Professor
Department of Financial Analysis and Audit
State University of Trade and Economics
ORCID: 0000-0001-6506-6965

Копотієнко Тетяна Юріївна
кандидат економічних наук,
доцент кафедри фінансового аналізу та аудиту
Державний торговельно-економічний університет
Kopotiienko Tetiana
Candidate of Economic Sciences, Associate Professor
Department of Financial Analysis and Audit
State University of Trade and Economics
ORCID: 0000-0001-6107-9937

ЗАСТОСУВАННЯ МОЖЛИВОСТЕЙ DIGITAL-АНАЛІЗУ У СФЕРІ ФІНАНСІВ ТА БАНКІВСЬКОЇ СПРАВИ
APPLICATION OF DIGITAL-ANALYSIS OPPORTUNITIES IN THE FIELD OF FINANCE AND BANKING

Анотація. *Вступ. Сучасна фінансова система зазнає трансформаційних змін під впливом диджиталізації, глобалізації ринків та зростання вимог до якості управлінських рішень. Digital-аналіз як*

сукупність методів збору, обробки та інтерпретації великих обсягів даних відіграє ключову роль у забезпеченні стійкості, конкурентоспроможності та прибутковості фінансових установ. У зв'язку з цим особливого значення набуває дослідження механізмів впровадження digital-аналізу в управлінські процеси банків, а також її ролі в ідентифікації ризиків, виявленні шахрайства, розробці інвестиційних стратегій та підвищенні клієнтоорієнтованості. Використання інноваційних підходів у сфері обробки даних забезпечує гнучкість адаптації банківських продуктів до потреб споживачів, удосконалення системи внутрішнього контролю та дотримання нормативних вимог.

Мета. Метою статті є дослідження потенціалу digital-аналізу у фінансовому секторі з акцентом на дослідження шахрайству.

Матеріали і методи. Матеріалами дослідження слугували:

1. *нормативно-правові документи, що регламентують діяльність фінансових установ у сфері обробки персональних даних, управління ризиками та запобігання шахрайству;*
2. *статистичні та аналітичні дані щодо використання інструментів машинного навчання та штучного інтелекту в банківській сфері;*
3. *результати прикладних досліджень та кейсів з аналізу шахрайських транзакцій за допомогою методів digital-аналізу.*

У процесі дослідження були застосовані методи: системного аналізу (для визначення місця digital-аналітики у структурі фінансової установи), теоретичного узагальнення (для класифікації напрямів її використання), статистичного аналізу (для інтерпретації кейсів виявлення шахрайства).

Результати. У статті представлено бачення застосування digital-аналізув банківській справі. Визначено ключові напрями її реалізації: управління кредитними, ринковими та операційними ризиками, виявлення шахрайських транзакцій, прогнозування клієнтської поведінки, автоматизація процесів андеррайтингу, персоналізація фінансових продуктів та забезпечення відповідності регуляторним вимогам. Наведено

приклад аналізу реального датасету з транзакцій кредитних карток, що засвідчив ефективність класифікаційних моделей у виявленні аномальних операцій. Підкреслено, що ефективна аналітика потребує високої якості даних, кібербезпеки та злагодженої інтеграції в IT-інфраструктуру установи.

Перспективи. Подальші наукові дослідження варто зосередити на розробці уніфікованих методик застосування digital-аналізу в банківській сфері, зокрема в контексті алгоритмічного трейдингу, гіперавтоматизації, оцінки сталості фінансової поведінки клієнтів, а також у сегментації цільової аудиторії на основі моделювання життєвого циклу клієнта. Особливої уваги потребує етична та регуляторна сторона використання ШІ в обробці персональних фінансових даних, що передбачає необхідність гармонізації алгоритмів з вимогами прозорості, безпеки та недискримінаційного підходу.

Ключові слова: *digital-аналіз, фінансовий сектор, управління ризиками, виявлення шахрайства, машинне навчання, прогностична аналітика, персоналізація, кібербезпека, банківська трансформація.*

Summary. *Introduction. The modern financial system is undergoing transformational changes driven by digitalisation, globalisation of markets and increasing demands on the quality of management decisions. Digital analysis, as a set of methods for collecting, processing and interpreting large amounts of data, plays a key role in ensuring the sustainability, competitiveness and profitability of financial institutions. In this regard, it is of particular importance to study the mechanisms for implementing digital analytics in the management processes of banks, as well as its role in identifying risks, detecting fraud, developing investment strategies and enhancing customer focus. The use of innovative approaches to data processing provides the flexibility to adapt banking products*

to the needs of consumers, improve internal control and compliance with regulatory requirements.

Purpose. The purpose of the article is to study the potential of digital analysis in the financial sector with a focus on fraud research.

Materials and methods. The research materials were:

1. regulatory documents governing the activities of financial institutions in the field of personal data processing, risk management and fraud prevention;

2. statistical and analytical data on the use of machine learning and artificial intelligence tools in the banking sector;

3. results of applied research and case studies on the analysis of fraudulent transactions using digital analysis methods.

In the course of the study, the following methods were applied: system analysis (to determine the place of digital analytics in the structure of a financial institution), theoretical generalisation (to classify the areas of its use), statistical analysis (to interpret fraud detection cases).

Results. The article presents a vision of the application of digital analytics in banking. The key areas of its implementation are identified: credit, market and operational risk management, detection of fraudulent transactions, forecasting customer behaviour, automation of underwriting processes, personalisation of financial products and ensuring compliance with regulatory requirements. An example of analysing a real dataset of credit card transactions is presented, which demonstrates the effectiveness of classification models in detecting anomalous transactions. It is emphasised that effective analytics requires high quality data, cybersecurity and well-coordinated integration into the IT infrastructure of an institution.

Discussion. Further research should focus on the development of unified methods for applying digital analysis in the banking sector, in particular in the context of algorithmic trading, hyper-automation, assessing the sustainability of customers' financial behaviour, and in segmenting the target audience based on

customer lifecycle modelling. Particular attention should be paid to the ethical and regulatory aspects of using AI in the processing of personal financial data, which requires harmonisation of algorithms with the requirements of transparency, security and non-discrimination.

Key words: *digital-analysis, financial sector, risk management, fraud detection, machine learning, predictive analytics, personalisation, cybersecurity, banking transformation.*

Постановка проблеми. Цифрова трансформація фінансового сектору створює нові можливості для підвищення ефективності, прозорості та адаптивності банківських процесів. У той же час, стрімке зростання обсягів даних, посилення вимог регуляторів, ускладнення клієнтських запитів і зростання кіберзагроз формують нові виклики для фінансових установ. Традиційні підходи до аналізу інформації та прийняття рішень більше не відповідають динаміці сучасного ринку та не забезпечують необхідного рівня точності й оперативності. В умовах високої конкуренції та глобалізації ринків саме digital-аналіз стає стратегічним інструментом для досягнення стійкої конкурентної переваги.

Водночас, процес інтеграції digital аналітичних рішень у діяльність фінансових установ супроводжується низкою проблем: недостатня якість вихідних даних, відсутність єдиної архітектури обробки інформації, складність у впровадженні аналітичних моделей у регульованому середовищі, ризики порушення конфіденційності та етичні дилеми використання алгоритмів штучного інтелекту. Особливо актуальними є питання ефективного управління ризиками, виявлення шахрайських транзакцій, розробки прогнозних моделей клієнтської поведінки та дотримання нормативних вимог за допомогою digital технологій.

Таким чином, виникає потреба у поглибленому дослідженні можливостей, викликів і стратегій впровадження digital-аналізу у

фінансовому секторі, з метою формування науково обґрунтованих підходів до побудови ефективних систем аналізу даних у банківській справі.

Аналіз останніх досліджень і публікацій. Питання digital трансформації фінансового сектору, активно досліджуються як вітчизняними, так і зарубіжними науковцями. Значний внесок у розвиток концептуального підґрунтя використання аналізу даних у фінансах зробили такі зарубіжні автори, як Т. Девенпорт (T. Davenport) та Д. Патіл (D. Patil) [1], які окреслили стратегічну роль data science у прийнятті управлінських рішень. Дослідження М. Міллера (M. Miller) [2] акцентують увагу на прогнозній аналітиці як інструменті управління ризиками у фінансовому секторі. Праця Моахаммад Хасан, Юлій Андріянсьях, Лейла Абдель-Рахман Азіз [3] та Олуватоїн Ф. Айоделе [4] висвітлюють значення штучного інтелекту в запобіганні шахрайству та забезпеченні відповідності регуляторним вимогам у банківській сфері.

Вітчизняні дослідники також активно працюють у цьому напрямі. Зокрема, Холявко Н., Садчикова І., Колоток М. [5] аналізує застосування штучного інтелекту у банківських установах, а Коваленко [6] охартеризувала чинники появи фінансових посередників в цифровій трансформації банків. А. В. Жаворонка, Л. В. Кузнєцової, С. В. Науменкової та С. В. Міщенко, О. В. Сидської та ін. [7-10] висвітлювати питання диджиталізації банківської сфери.

Незважаючи на суттєвий прогрес у вивченні окремих аспектів digital трансформації фінансового сектору, низка наукових питань потребує подальшого дослідження. Зокрема, недостатньо систематизовано напрями впровадження digital-аналізу у функціонування банківської установи як цілісної системи, не до кінця визначено критерії інтеграції аналітичних платформ з урахуванням нормативного середовища, а також бракує методичних підходів до оцінки ефективності впливу аналітичних рішень на фінансову стабільність установи. У зв'язку з цим актуальним є формування

науково-практичного підходу до впровадження digital-аналізу як інструменту антикризового управління та стратегічного розвитку банківських структур.

Метою статті є дослідження потенціалу digital-аналізу у фінансовому секторі з акцентом на дослідження шахрайству.

Матеріали і методи. У процесі підготовки статті використано такі джерела:

1. нормативно-правові документи, що регламентують діяльність фінансових установ у сфері обробки персональних даних, управління ризиками та запобігання шахрайству;
2. статистичні та аналітичні дані щодо використання інструментів машинного навчання та штучного інтелекту в банківській сфері;
3. результати прикладних досліджень та кейсів з аналізу шахрайських транзакцій за допомогою методів digital-аналізу.

У процесі дослідження були застосовані методи: системного аналізу (для визначення місця digital-аналізу структурі фінансової установи), теоретичного узагальнення (для класифікації напрямів її використання), статистичного аналізу (для інтерпретації кейсів виявлення шахрайства).

Виклад основного матеріалу. У сучасних умовах digital-трансформації фінансовий сектор зазнає суттєвих змін, зумовлених стрімким розвитком digital-технологій. Ці зміни впливають як на організаційні процеси у банківській сфері, так і на підходи до управління фінансовими ресурсами, аналізу ринкових тенденцій і взаємодії з клієнтами. Впровадження digital-аналізу та digital-аналітики дає змогу фінансовим установам приймати обґрунтовані управлінські рішення, оптимізувати бізнес-процеси, підвищувати ефективність операційної діяльності та знижувати рівень фінансових ризиків.

Зростання обсягів структурованих і неструктурованих даних у поєднанні з високими вимогами до оперативності обробки інформації

стимулює банки впроваджувати передові аналітичні платформи, що базуються на алгоритмах машинного навчання, штучного інтелекту та прогнозного моделювання. Аналітика в банківській сфері трансформується з інструменту звітності в стратегічний засіб управління, що охоплює ключові напрями: управління ризиками, виявлення шахрайства, персоналізацію продуктів, покращення обслуговування клієнтів, маркетингову оптимізацію та регуляторну відповідність.

Разом з тим, впровадження digital аналітичних рішень супроводжується низкою викликів, специфічних для фінансового сектору. Серед основних бар'єрів, що ускладнюють інтеграцію сучасних інструментів digital-аналізу, слід виділити такі:

1. Дотримання нормативних вимог. Банківські установи функціонують у середовищі жорсткого регулювання, де пріоритетом є дотримання численних законодавчих норм, зокрема положень Загального регламенту про захист даних (GDPR) та аналогічних нормативних актів. Ці документи регламентують порядок збору, зберігання, обробки та передачі персональних даних, що вимагає від банків високого рівня відповідності усіх аналітичних інструментів вимогам конфіденційності. Недотримання регуляторних норм не лише загрожує значними штрафними санкціями, а й може завдати суттєвих репутаційних втрат фінансовим установам.

2. Забезпечення інформаційної безпеки та конфіденційності даних. З огляду на те, що банки обробляють великі обсяги персональних і фінансових даних клієнтів, питання їхньої безпеки набуває критичного значення. Фінансові установи є одними з основних мішеней для кіберзлочинності. Застосування зовнішніх аналітичних сервісів, особливо тих, що працюють у хмарному середовищі, підвищує ризики несанкціонованого доступу до чутливої інформації. Тому пріоритет мають аналітичні платформи, що відповідають міжнародним стандартам безпеки

(зокрема ISO/IEC 27001) та здатні забезпечити контроль над усіма етапами обробки даних.

3. Інтеграція розподілених джерел даних. Ефективний digital-аналіз неможливий без консолідації даних, які часто зберігаються у розрізнених інформаційних системах окремих підрозділів установи. Ізольованість даних, що є спадком застарілих IT-архітектур, перешкоджає побудові цілісного уявлення про клієнта чи фінансову операцію. Це, своєю чергою, ускладнює побудову релевантних моделей прогнозування, оцінки ризиків чи клієнтської поведінки. Успішна інтеграція передбачає модернізацію інфраструктури, перехід до мікросервісної архітектури та впровадження засобів ETL (Extract, Transform, Load).

4. Забезпечення високої якості даних. Результативність digital-аналізу безпосередньо залежить від точності, повноти та актуальності даних. Наявність дубльованої, застарілої або нерелевантної інформації може суттєво спотворити аналітичні висновки, що призводить до прийняття неефективних управлінських рішень. Таким чином, банки повинні впроваджувати стратегії управління якістю даних, включно з постійною валідацією, очищенням, нормалізацією та перевіркою джерел їхнього походження. Високоякісні дані є основою успішного впровадження моделей штучного інтелекту, машинного навчання, а також побудови ефективних систем управління взаємовідносинами з клієнтами (CRM) та маркетингових стратегій [11].

У сучасних умовах digital трансформації банківська аналітика виступає ключовим інструментом у прийнятті обґрунтованих управлінських рішень, виявленні фінансових ризиків та підвищенні якості обслуговування клієнтів. Використання інструментів digital-аналізу у банківській сфері забезпечує формування цінної інформації з великих обсягів фінансових та нефінансових даних, що створює підґрунтя для стратегічного управління.

Швидке зростання обсягів інформації, яку генерують банки, потребує впровадження передових digital-рішень, зокрема алгоритмів машинного навчання, інтелектуального аналізу даних і прогнозної аналітики. Це дозволяє фінансовим установам адаптувати бізнес-моделі до динамічного ринкового середовища та забезпечувати підвищення ефективності діяльності.

Digital-аналіз в банках охоплює широкий спектр напрямів: від операційної ефективності до управління ризиками, боротьби з шахрайством, персоналізації послуг, оптимізації внутрішніх процесів та відповідності регуляторним вимогам. Зокрема, оцінка ризиків, пов'язаних із кредитуванням, інвестуванням і щоденною операційною діяльністю, базується на аналізі історичних даних, що дозволяє ідентифікувати закономірності в поведінці позичальників і передбачати ймовірність неповернення кредитних коштів. Це підвищує точність оцінки кредитоспроможності клієнтів і знижує ймовірність фінансових втрат.

Окрему роль у цьому контексті відіграє аналіз транзакцій у режимі реального часу з використанням алгоритмів машинного навчання, який забезпечує виявлення аномальних операцій, таких як несанкціоновані перекази, спроби шахрайства чи крадіжки персональних даних. Автоматизовані аналітичні платформи здатні оперативно реагувати на підозрілі дії, тим самим мінімізуючи ризики втрати коштів клієнтів і зберігаючи фінансову стабільність установи.

Digital-аналіз також сприяє глибшому розумінню клієнтської поведінки, виявленню уподобань та потреб, що є основою для побудови персоналізованих фінансових продуктів. Аналіз транзакційної активності, частоти звернень до послуг та реакцій на маркетингові комунікації дозволяє формувати індивідуальні пропозиції та підвищувати якість взаємодії з клієнтами. Це, своєю чергою, зміцнює довіру споживачів та сприяє зростанню їхньої лояльності.

Застосування аналітичних підходів до оптимізації внутрішніх процесів дозволяє виявляти неефективні елементи операційної діяльності, автоматизувати рутинні завдання та ефективно розподіляти ресурси. Результатом є зниження операційних витрат, підвищення продуктивності праці та загальна прибутковість банківської установи [12].

У контексті дотримання регуляторних вимог, аналітичні інструменти забезпечують автоматизований моніторинг транзакцій відповідно до принципів KYC (Know Your Customer) та AML (Anti-Money Laundering). Завдяки виявленню потенційно підозрілих дій фінансові установи можуть своєчасно реагувати на ризики порушення нормативних актів, запобігаючи фінансовим санкціям і зберігаючи відповідність чинному законодавству.

Використання прогнозної аналітики дозволяє фінансовим установам не лише реагувати на зміни, а й передбачати їх. На основі історичних даних створюються моделі кредитного скорингу, прогнозуються рівні ризиків, визначаються поведінкові патерни клієнтів. Це дає змогу розробляти ефективні стратегії, формувати інноваційні фінансові продукти та здійснювати стратегічне планування з урахуванням майбутніх ринкових тенденцій.

Таким чином, digital-аналіз у банківській справі виступає не лише технічним інструментом, а й невід'ємною складовою сучасного управління, що дозволяє досягати високої конкурентоспроможності, ефективності та стійкості фінансових установ.

Якщо є говорити, про стратегії ефективної диджиталізації у сфері фінансів, то важливим її аспектом є стратегія гіперавтоматизації. Вона поєднує роботизовану автоматизацію процесів (RPA), штучний інтелект, обробку природної мови та керування бізнес-процесами для досягнення високого рівня автоматизації. У банківському секторі це охоплює обслуговування клієнтів, обробку кредитів, виявлення шахрайства та управління ризиками. Так за даними Gartner на кінець 2024 року згідно

прогнозів було визначено, що гіперавтоматізація знизить операційні витрати на 30%, а до 2025 року її ринок досягне 860 мільярдів доларів.

Ефективне впровадження гіперавтоматизації у фінансових установах вимагає послідовного проходження низки етапів, кожен з яких забезпечує поступовий перехід від ручної обробки даних до повністю автоматизованого середовища:

1. Ідентифікація повторюваних і рутинних операцій. На початковому етапі необхідно здійснити аудит бізнес-процесів з метою виявлення операцій, що є найбільш трудомісткими, монотонними та схильними до помилок. До таких завдань, як правило, належать введення даних, обробка рахунків-фактур, щоденні казначейські операції та базове обслуговування клієнтів. Виявлення таких процесів є підґрунтям для подальшої автоматизації.

2. Розгортання рішень роботизованої автоматизації процесів (RPA). На наступному етапі відбувається впровадження програмних роботів, здатних виконувати рутинні операції за заздалегідь визначеними сценаріями. RPA дозволяє мінімізувати участь людини в операційних завданнях, знижуючи кількість помилок, пришвидшуючи обробку інформації та забезпечуючи сталість процесів.

3. Інтеграція інтелектуальних технологій – ШІ та ML. Розширення функціональних можливостей RPA шляхом поєднання з алгоритмами штучного інтелекту (AI) та машинного навчання (ML) забезпечує перехід до інтелектуальної автоматизації. Таке поєднання дозволяє ботам виконувати складні завдання, що потребують контекстного аналізу, адаптивного прийняття рішень та самообучення на основі історичних даних.

4. Оптимізація використання обчислювальних ресурсів. Для досягнення економічної доцільності гіперавтоматизація передбачає гнучке управління інфраструктурою. Це включає динамічне масштабування

обчислювальних потужностей, балансування між хмарними та локальними ресурсами відповідно до поточних і прогнозованих навантажень.

5. Дотримання стандартів безпеки та нормативних вимог. Під час впровадження автоматизованих рішень особлива увага приділяється забезпеченню конфіденційності, цілісності та доступності даних. Використання гіперавтоматизації має узгоджуватись із вимогами GDPR, PSD2 та іншими нормативами, що регулюють захист персональної та фінансової інформації у фінансовому секторі.

6. Постійний моніторинг та оптимізація процесів. Автоматизовані системи потребують регулярного аудиту продуктивності з метою виявлення вузьких місць та оновлення логіки процесів відповідно до змін ринку, нормативного середовища або внутрішніх стратегій компанії.

7. Залучення сторонніх сервісів та технологічних партнерів. Для забезпечення масштабованості та гнучкості автоматизаційних ініціатив доцільним є використання зовнішніх платформ, хмарних сервісів та спеціалізованих програмних рішень. Це дозволяє не лише скоротити час впровадження, а й забезпечити найвищі стандарти технічного супроводу та відповідності [13].

Інтеграція штучного інтелекту (ШІ) та роботизованої автоматизації процесів (RPA) у діяльність фінансових установ відкриває нові можливості для підвищення ефективності, зниження операційних витрат і мінімізації так званих digital відходів. Згідно з даними Economist Intelligence Unit, 86% керівників фінансових установ планують нарощувати інвестиції в ШІ до 2025 року, що свідчить про стрімке зростання значущості цих технологій у банківському секторі.

ШІ забезпечує здатність до обробки великих обсягів структурованих і неструктурованих даних, виявлення закономірностей, аналізу аномалій та надання стратегічно важливої інформації для прийняття рішень. Водночас RPA виконує автоматизацію повторюваних і стандартних операцій, які

базуються на чітко визначених правилах, що дозволяє зменшити частоту людських помилок і пришвидшити виконання операцій [14; 15].

Digital-модернізація та стратегічне впровадження digital-аналізу є ключовими інвестиційними напрямами для забезпечення стійкого зростання, конкурентоспроможності та оперативного реагування на зміни ринку. Використання передових фінансових технологій дозволяє банківським установам впроваджувати:

- Багатоканальний банкінг. Формування інтегрованого клієнтського досвіду в онлайн-, мобільному та фізичному середовищі сприяє підвищенню задоволеності користувачів, зміцненню лояльності клієнтів та зростанню обсягів транзакцій.
- Рефакторинг систем та перехід до мікросервісної архітектури. Модернізація застарілих інформаційних систем забезпечує кращу масштабованість, підвищує гнучкість технологічної інфраструктури та сприяє скороченню часу виведення нових продуктів на ринок.
- Інвестиції в аналіз. Впровадження аналітичних платформ дозволяє організаціям приймати обґрунтовані управлінські рішення на основі даних, здійснювати таргетовану взаємодію з клієнтами та прогнозувати поведінкові патерни.
- Інтеграція блокчейн-технологій. Застосування децентралізованих реєстрів забезпечує підвищення прозорості, незмінності та безпеки фінансових операцій, що особливо актуально для транзакцій з високим рівнем довіри.
- Digital-безпека та регуляторна відповідність.

Digital-аналіз дедалі більше перетворюється на стратегічний ресурс, який забезпечує інсайти для прийняття рішень, щоб повною мірою реалізувати потенціал аналізу даних, фінансові установи мають реалізувати комплексну стратегію масштабування, а саме: розробити аналітичну

дорожню карту, побудувати екосистему, сформувати озеро даних (Data Lakes), змігрувати у хмарне середовище.

Розподілена хмара є сучасною формою організації хмарної інфраструктури, що забезпечує зберігання, обробку та доступ до даних через кілька взаємопов'язаних хмарних середовищ. Такий підхід поєднує гнучкість локального розміщення з централізованим керуванням, що особливо важливо для фінансових установ, які працюють із критично чутливою інформацією.

Переваги розподіленої хмари включають низьку затримку обробки транзакцій, відповідність регуляторним вимогам, а також підвищену захищеність особистих і фінансових даних.

Фінансовий сектор є одним із найбільш уразливих до кіберзагроз через велику кількість оброблюваних конфіденційних даних та інтенсивність транзакційної діяльності. Середня вартість витоку даних у цій галузі перевищує загальний показник для інших секторів, що підтверджує необхідність цілісного та проактивного підходу до кібербезпеки та включати впровадження принципів відкритого банкінгу, системи виявлення шахрайства, KYC та KYB-процедури, наскрізне шифрування (E2E), використання апаратних модулів безпеки (HSM), токенізація.

Для відображення можливостей digital-аналізу в рамках дослідження шахрайства з кредитними картками розглянемо деідентифікований набір даних транзакцій кредитних карток випущених в Європі. Цей набір даних представляє транзакції, де 0, 172% усіх транзакцій є шахрайськими (рис.1). Він містить лише числові вхідні змінні, які є результатом перетворення PCA, де функції V1-V28 є основними компонентами, отриманими за допомогою PCA. Функція «Time» містить секунди, що минули між кожною транзакцією та першою транзакцією в наборі даних. Функція «Amount» – це сума транзакції. Функція «Class» є змінною і приймає значення 1 у разі шахрайства та 0 в іншому випадку.

Рис. 1. Розподіл шахрайських та не шахрайських транзакцій за період дослідження

Джерело: розроблено авторами

Досліджуючи розподіл шахрайських транзакцій в часі, то вони мають більш рівномірний розподіл, включаючи нічні транзакції.

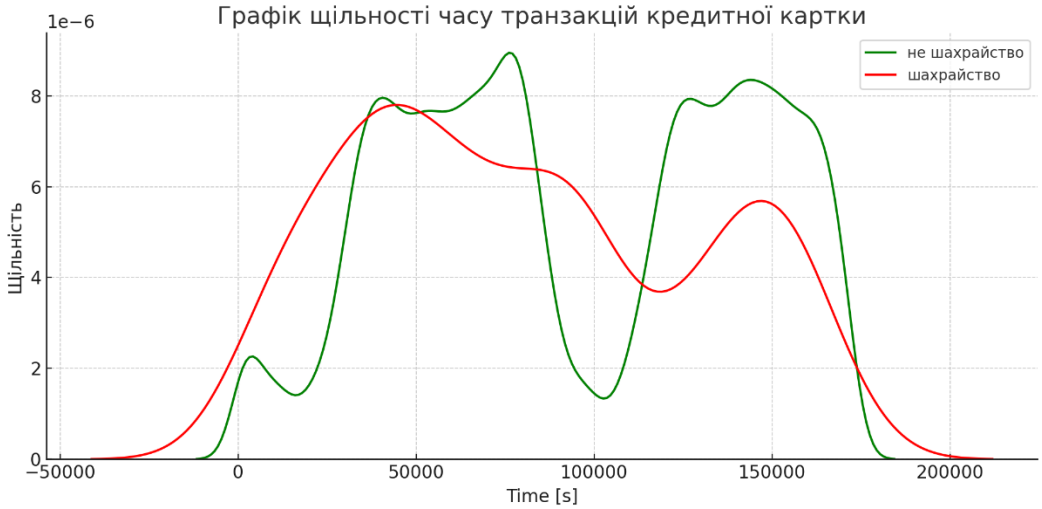


Рис. 2. Графік щільності часу транзакцій кредитних карток

Джерело: розроблено авторами

Не шахрайські транзакції рівномірно розподілені протягом усього проміжку часу, з кількома помітними піками активності. Це свідчить про стандартну поведінку користувачів. Шахрайські транзакції мають інший

розподіл. Видно кілька чітко виражених піків, це потенційно свідчить про скоординовані атаки або використання автоматизованих інструментів для здійснення шахрайських дій у певні моменти.

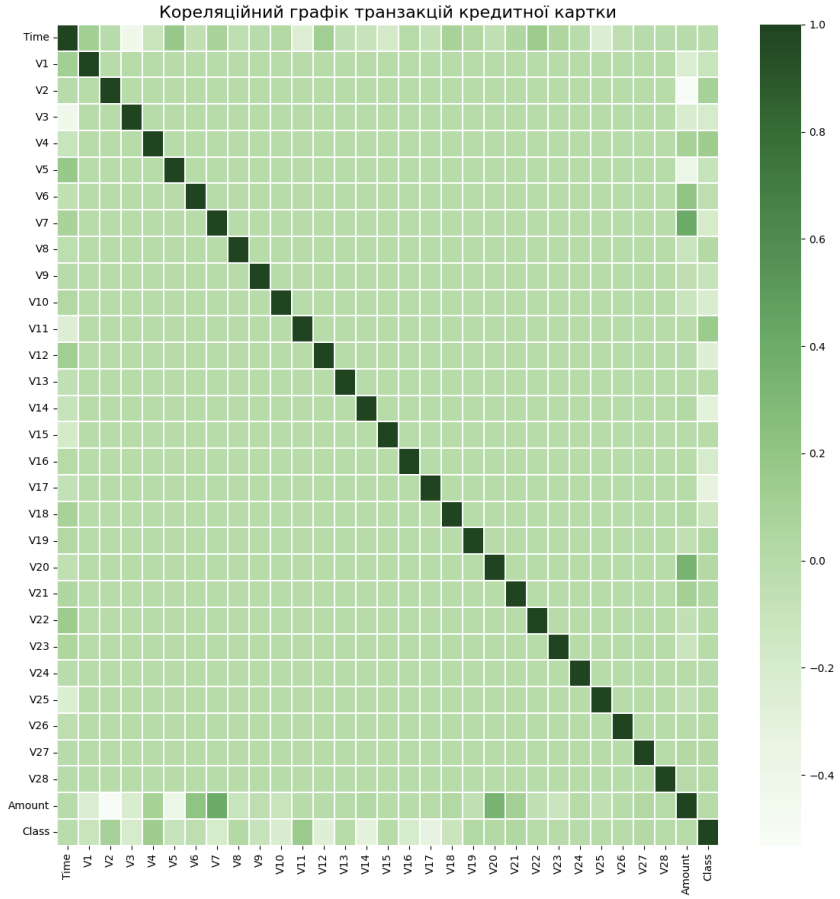


Рис. 3. Кореляційний аналіз транзакцій кредитних карток

Джерело: розроблено авторами

Як і очікувалося, немає значної кореляції між функціями V1-V28. Однак існують певні кореляції між цими функціями та часом (обернена кореляція з V3) і сумою (пряма кореляція з V7 і V20, обернена кореляція з V1 і V5). (рис.3). Діаграма в основному забарвлена в світлі відтінки зеленого, що свідчить про слабку або відсутню лінійну залежність між змінними. Це може означати, що ознаки були спеціально трансформовані для зменшення кореляції. Кореляція між "Amount" та іншими змінними є незначною, що може вказувати на те, що сума транзакції не є ключовим фактором при виявленні аномальних операцій. Є певні місця на графіку, де

кореляція дещо підвищена, що може означати залежність між окремими факторами транзакцій. Відсутність сильної кореляції між змінною "Class" та іншими параметрами свідчить про те, що виявлення шахрайських операцій (Class = 1) не може бути безпосередньо визначене простими кореляційними методами. Це означає, що для ефективного аналізу та виявлення шахрайства можуть знадобитися складніші методи машинного навчання.

Давайте розглянемо розподіл транзакцій у часі для обох класів, а також загальну кількість транзакцій і суми, агреговані за годину (рис.4,5,6,7).

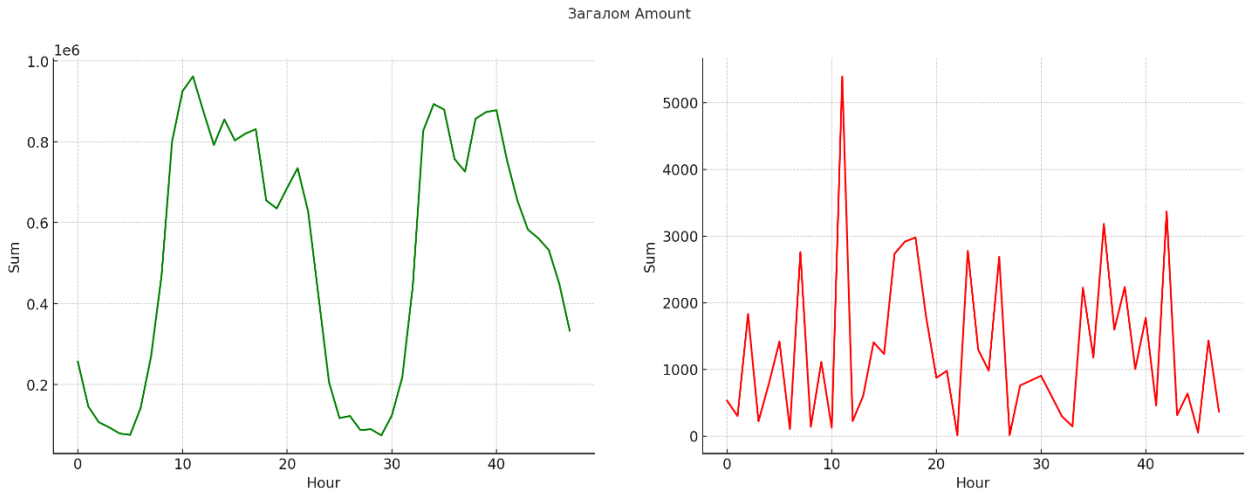


Рис. 4. Зміна загальної суми транзакцій по годинах

Джерело: розроблено авторами

На рисунку 4 дані демонструють виражену циклічну залежність операційної активності за годинами доби. На лівій частині графіку спостерігається чітка циклічність у зміні загальної суми транзакцій, яка повторюється кожні приблизно 24 години. Вищі значення припадають на денний час (орієнтовно з 8 до 18 години), де сума може перевищувати 800 тис. – 1 млн. У нічні години (приблизно 0–6 годин) активність значно знижується, що свідчить про зменшення обсягів операцій. Типовий денний транзакційний ритм – максимальна активність відбувається в робочий час, тоді як уночі активність суттєво знижується.

На правій частині графіку дані виглядають набагато більш розкиданими, із сильними коливаннями і піками (наприклад, різкий сплеск

біля 10-ї години). Загальний тренд менш очевидний, але можна помітити, що сплески часто трапляються у ті самі денні години, що й на лівому графіку. Високі піки свідчать про масові автоматизовані шахрайські транзакції.

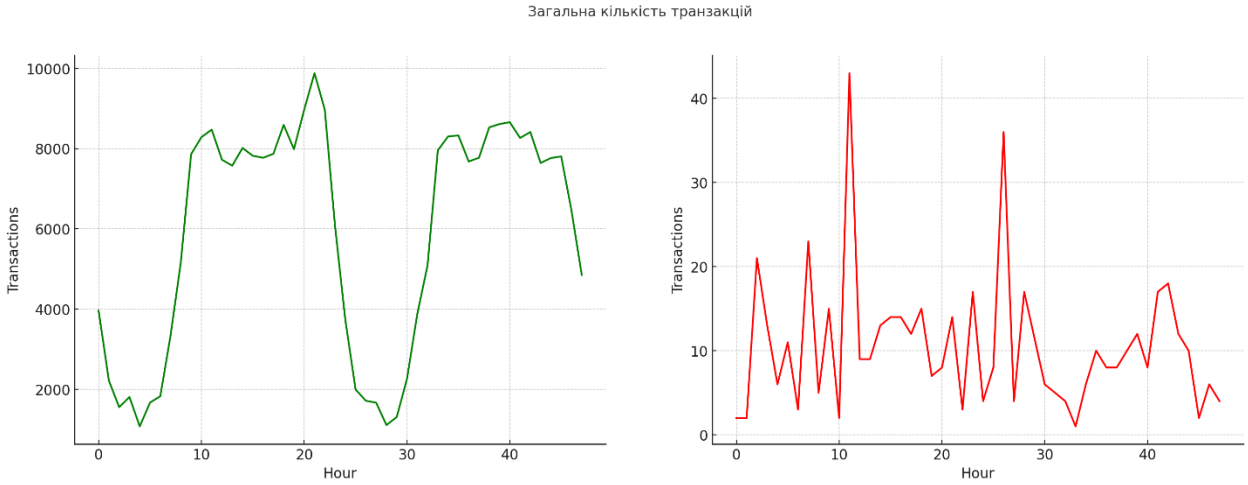


Рис. 5. Зміна загальної кількості транзакцій по годинах

Джерело: розроблено авторами

На рисунку 5 у лівій частині графіку видно чітку циклічність – пік активності припадає на денні години – близько 9:00–20:00, з максимумом близько 19–20 години (~10 тис. транзакцій). Уночі та рано вранці (0:00–6:00) кількість транзакцій зменшується до мінімуму (менше ніж 2 тис.).

Повторюваність свідчить про стабільний щоденний ритм користувацької активності. Права частина рисунку демонструє кількість коливань в межах 0–40 транзакцій на годину, з поодинокими піками (наприклад, о 10-й годині – більше 40). Дані мають сильну дисперсію, без чіткої циклічності – активність нерівномірна.

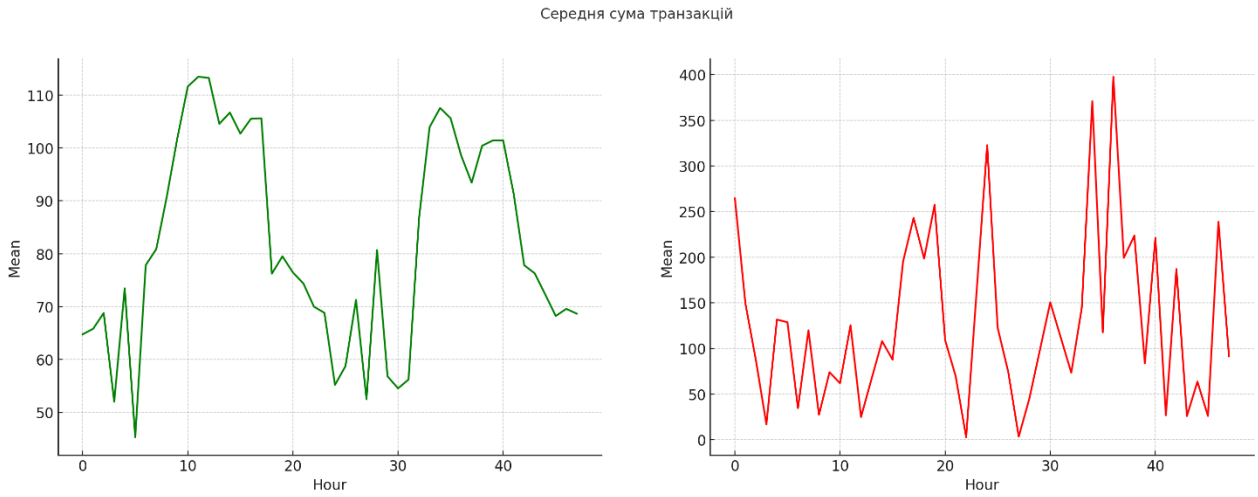


Рис. 6. Зміна середньої суми транзакцій по годинах

Джерело: розроблено авторами

На рисунку 6 спостерігається у лівій частині стабільна динаміка середньої суми транзакцій протягом дня з очевидним підвищенням у робочі години. Середня сума транзакцій коливається у межах ~45 до 115 одиниць.

Правий графік демонструє мінливість та сплески в окремих годинах, характерні для нестандартних фінансових операцій. Середні значення значно вищі – коливаються від 50 до 400 одиниць. Сильна волатильність – немає чітко визначених піків, але є локальні сплески. Ці транзакції – ймовірно, великі індивідуальні платежі, високоризикові операції або транзакції малих обсягів, але з великою сумою.

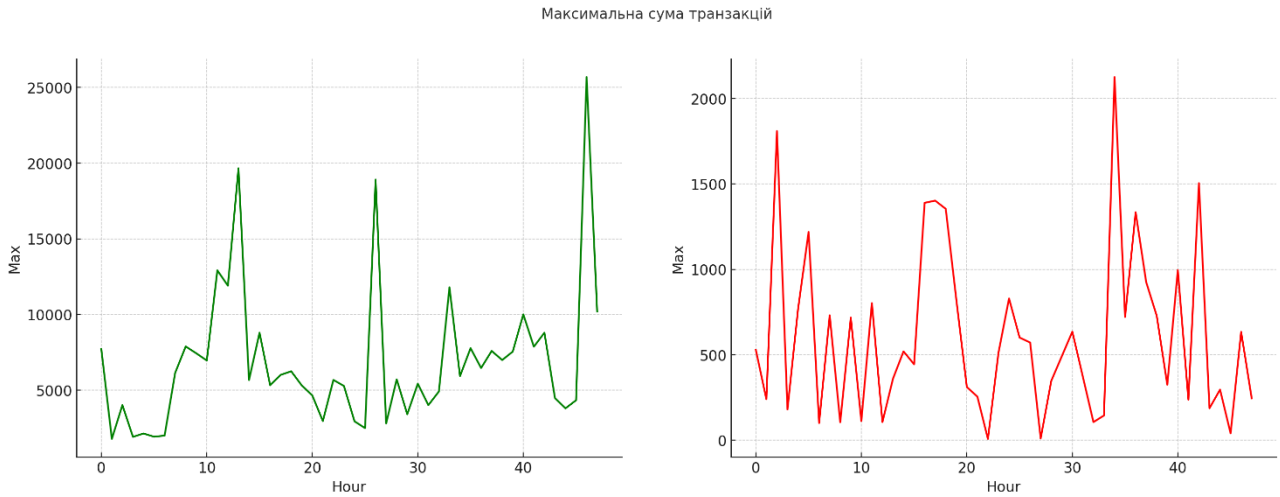


Рис. 7. Зміна максимальної суми транзакцій по годинах

Джерело: розроблено авторами

На рисунку 7 ліва та права частина графіка показує, що максимальні транзакції не мають чіткої повторюваності. Це свідчить про епізодичний характер великих сум, часто не пов'язаний із загальною динамікою кількості чи середньої суми транзакцій. Найвищі піки потребують ретельної перевірки на предмет аномалій або шахрайства, особливо якщо вони не співпадають із загальними періодами активності користувачів.

На лівій частині графіку спостерігаються коливання від ~2000 до понад 25 000 одиниць. На правій частині суми варіюються від ~100 до понад 2000 одиниць. Піки видно в 1-й, 19-й, 31-й, 35-й годинах, де значення перевищують 1500–2000 одиниць.

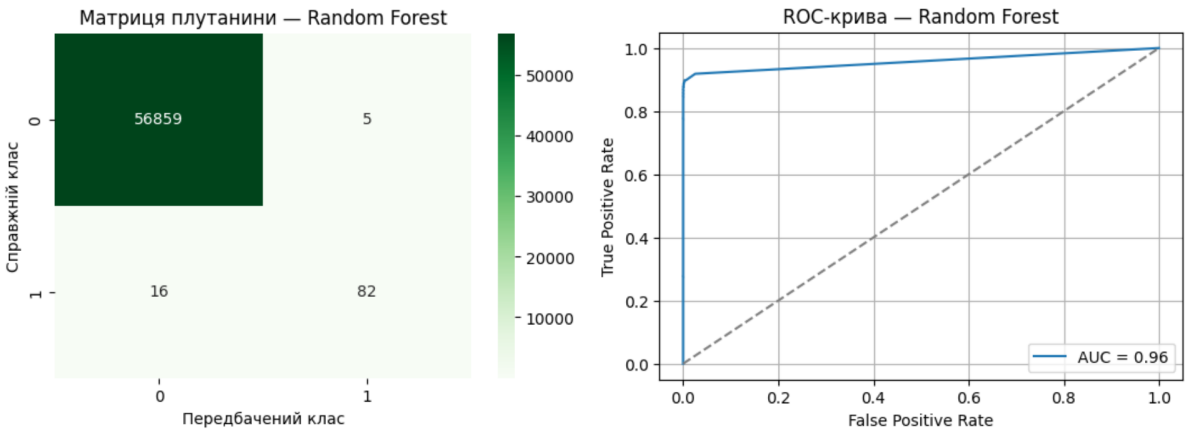
Отже, в рамках зведення вищевикладеної інформації про виконану агрегацію основних метрик транзакцій по годинах (Hour) для кожного класу (Class 0 – звичайні транзакції, Class 1 – шахрайські). В рамках побудованих графіків: для Class 0 (не шахрайство) – суми транзакцій рівномірно розподілені з передбачуваними піками в певні години. Не шахрайські транзакції відбуваються у великій кількості протягом доби, з циклічними піками. У звичайних транзакціях середня сума стабільна та знаходиться в «нормальних» межах. У Class 0 – максимум змінюється плавно, без екстремумів. У Class 1 (шахрайство) – спостерігаються різкі сплески в окремі години, що свідчить про локальні хвилі злочинної активності. поодинокі, але зосереджені в окремих годинах, що потенційно вказує на скоординовані атаки. У шахрайських – є виражені стрибки, що можуть бути ознаками високоризикових операцій. У Class 1 – різко зростає у певні години, вказуючи на спроби провести великі транзакції під час зниженого контролю.

Рис. 8. Суми шахрайських транзакцій протягом доби

Джерело: розроблено авторами

На рисунку 8 зазначена кожна точка – окрема шахрайська транзакція. Видно, що сплески активності в певні часові періоди та на різні рівні суми. Шахрайські дії є продуманими кроками за рахунок концентрації в певний час. Більшість шахрайських транзакцій мають низькі суми (до 200–300 одиниць), що свідчить про маскування або розподілення сум на дрібні платежі. А часті малі суми можуть також свідчити про тактику «тестування системи» – проба транзакцій перед основною атакою або спроби залишитися непоміченими. Маніпуляції зі значними сумами здійснюються у нічні години.

Для виявлення шахрайських транзакцій було проведено навчання чотирьох різних моделей: Random Forest (випадковий ліс), Extra Trees (додаткові дерева) і Logistic Regression (логістична регресія).



Звіт класифікації:

	precision	recall	f1-score	support
0	0.9997	0.9999	0.9998	56864
1	0.9425	0.8367	0.8865	98
accuracy			0.9996	56962
macro avg	0.9711	0.9183	0.9432	56962
weighted avg	0.9996	0.9996	0.9996	56962

Рис. 9. Результати навчання за моделлю Random Forest

Джерело: розроблено авторами

За результатами навчання модель Random Forest (рис.9) продемонструвала високу здатність до розпізнавання шахрайських транзакцій. Значення AUC (Area Under the Curve) становить 0,96, що свідчить про високу ефективність моделі у розділенні класів, навіть за умов незбалансованих даних.

Основні метрики класифікації для класу «шахрайство»:

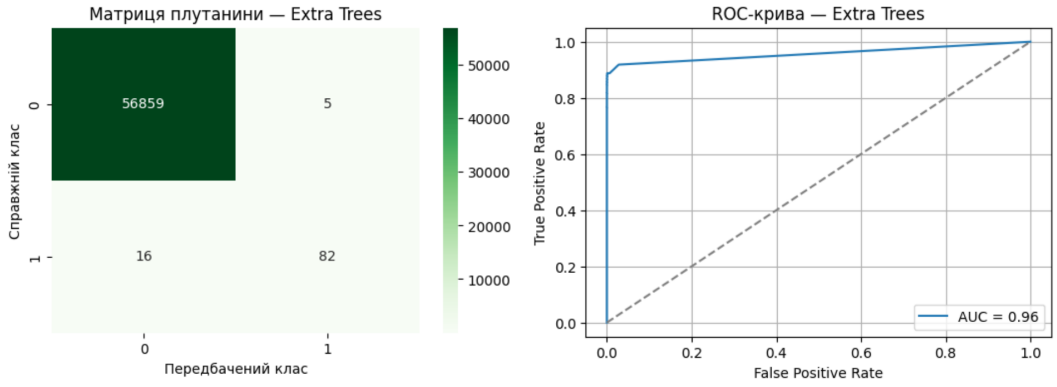
- Точність (precision) – *0.9425* – більшість транзакцій, які модель ідентифікує як шахрайські, справді такими є;
- Повнота (recall) – *0.8367* – модель виявляє приблизно 84% усіх реальних шахрайств;
- F1-міра – *0.8865* – свідчить про збалансовану якість між точністю та повнотою.

Високе значення AUC = 0.96 додатково підтверджує надійність моделі при класифікації, зокрема в умовах класового дисбалансу. Водночас показник повноти (recall) < 1 вказує на наявність випадків пропуску

шахрайських транзакцій, що може мати критичне значення в реальному банківському середовищі.

Зважаючи на це, рекомендується інтегрувати модель із додатковими механізмами контролю, зокрема:

- використання порогового аналізу для налаштування рівня чутливості;
- ручна перевірка або пост-фільтрація підозрілих операцій;
- впровадження інтерпретованих моделей (наприклад, SHAP) для пояснення рішень та підвищення прозорості моделі.




```
Звіт класифікації:
              precision    recall  f1-score   support

           0     0.9997    0.9999    0.9998     56864
           1     0.9425    0.8367    0.8865        98

    accuracy                         0.9996     56962
   macro avg     0.9711    0.9183    0.9432     56962
weighted avg     0.9996    0.9996    0.9996     56962
```

Рис. 10. Результати навчання за моделлю Extra Trees

Джерело: розроблено авторами

Модель Extra Trees Classifier (рис.10) також продемонструвала високу ефективність у виявленні шахрайських транзакцій. Показник AUC = 0.96 свідчить про відмінну здатність моделі розрізняти класи, що підтверджує її придатність до використання в умовах фінансової сфери.

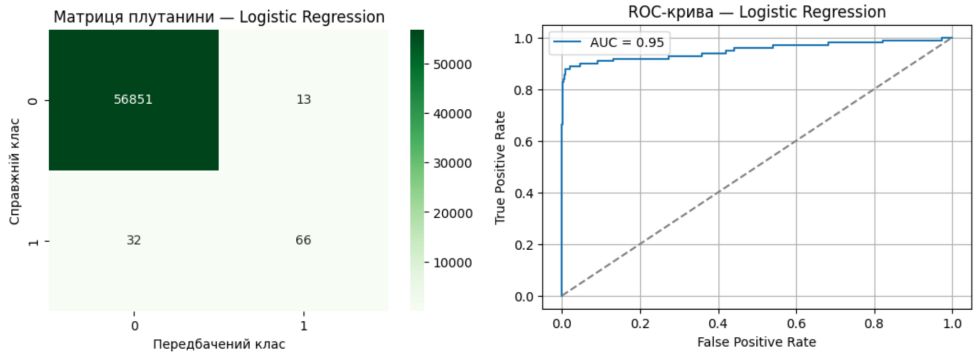
Ключові метрики класифікації для класу «шахрайство»:

- Точність (precision) – 0.9425 – більшість транзакцій, позначених як шахрайські, справді є шахрайськими;

- Повнота (recall) – 0.8367 – модель виявляє понад 83% усіх реальних випадків шахрайства;
- F1-міра – 0.8865 – свідчить про високий баланс між точністю та повнотою.

Поведінка моделі близька до Random Forest, однак Extra Trees може демонструвати покращену швидкість обробки завдяки застосуванню додаткової випадковості при виборі порогів розділення. Як і у випадку з RF, повнота (recall) < 1 означає, що певна частина шахрайських транзакцій залишається не виявленою.

З огляду на ці характеристики, модель є перспективною для використання в реальних умовах як самостійно, так і в рамках ансамблевих підходів – наприклад, у поєднанні з XGBoost або CatBoost. Такий підхід може підвищити загальну точність системи виявлення шахрайства за рахунок об'єднання сильних сторін різних алгоритмів.



Звіт класифікації:

	precision	recall	f1-score	support
0	0.9994	0.9998	0.9996	56864
1	0.8354	0.6735	0.7458	98
accuracy			0.9992	56962
macro avg	0.9174	0.8366	0.8727	56962
weighted avg	0.9992	0.9992	0.9992	56962

Рис. 11. Результати навчання за моделлю Logistic Regression

Джерело: розроблено авторами

Модель Logistic Regression (рис.11) показала достатньо високий рівень якості класифікації, хоча й поступається деревоподібним моделям (Random Forest, Extra Trees). Показник AUC = 0.95 свідчить про здатність моделі

розділяти класи з високою точністю, однак трохи нижчу порівняно з більш складними ансамблевими підходами.

Ключові метрики класифікації для класу «шахрайство»:

- Точність (precision) – *0.835* – близько 16,5% транзакцій, позначених як шахрайські, є хибно позитивними;
- Повнота (recall) – *0.674* – модель виявляє лише близько 67% реальних випадків шахрайства;
- F1-міра – *0.746* – свідчить про помітно нижчий баланс точності та повноти у порівнянні з Random Forest та Extra Trees.

Незважаючи на ці обмеження, модель Logistic Regression має низку важливих переваг:

- Висока швидкість навчання та прогнозування;
- Простота реалізації та інтерпретації результатів;
- Застосовність у задачах, де критично важлива пояснюваність моделі (наприклад, у регуляторній звітності або кредитному скорингу).

Таким чином, Logistic Regression може розглядатися як базовий еталон у задачах класифікації, а також як частина ансамблевих рішень, де вона доповнює більш складні моделі, забезпечуючи прозорість та інтерпретованість прийнятих рішень.

Отже, ансамблеві моделі (Random Forest та Extra Trees) демонструють високу здатність до класифікації – обидві мають однакові значення метрик, що вказує на надійність і стабільність їхніх результатів. Extra Trees має перевагу в швидкості роботи, оскільки використовує випадкові пороги при розбитті вузлів. Logistic Regression показала нижчу повноту та F1-міру, що свідчить про часткову втрату справжніх шахрайських транзакцій. Проте вона залишається цінною через простоту, швидкість навчання і високу інтерпретованість.

Для виявлення шахрайських транзакцій у фінансових системах найкращі результати демонструють ансамблеві моделі (Random Forest та

Extra Trees), які мають високу точність, хорошу повноту та збалансовані F1-метрики. Logistic Regression доцільно використовувати як базову модель, для контролю, пояснення рішень або як частину ансамблю, особливо в умовах обмежених обчислювальних ресурсів або підвищених вимог до прозорості моделі.

Висновки і перспективи подальших досліджень. Таким чином, у процесі digital трансформації фінансової сфери ключового значення набуває впровадження digital-аналізу як основи для прийняття обґрунтованих управлінських рішень. Розглянуто підходи до digital трансформації у фінансовому секторі, включно з гіперавтоматизацією, впровадженням RPA та AI, розвитком багатоканального банкінгу, розгортанням розподіленої хмарної інфраструктури та забезпеченням кібербезпеки на всіх рівнях. Практичні рекомендації щодо масштабування digital-аналізу, дотримання стандартів захисту інформації та впровадження інноваційних технологій створюють основу для підвищення ефективності діяльності фінансових установ і зниження рівня ризиків.

Проведене дослідження аналізу виявлення та машинного навчання для виявлення шахрайських дій з кредитними картами.

Моделі ансамблевого типу (Random Forest і Extra Trees) продемонстрували найвищу точність, повноту та F1-метрику, що свідчить про їхню практичну придатність у задачах кібербезпеки та моніторингу платіжної активності. Logistic Regression, незважаючи на нижчі показники ефективності, може використовуватись як базова модель або частина ансамблю завдяки своїй швидкодії та інтерпретованості. Візуалізація аналітики транзакцій дозволила виявити часові патерни активності, середніх сум, а також пікові періоди для потенційних шахрайських операцій, що додатково підтверджує доцільність інтеграції аналітичних рішень у фінансовий моніторинг.

У подальших дослідженнях доцільно зосередити увагу на розробці методик пояснюваності аналітичних моделей, інтеграції засобів оцінки етичних ризиків та удосконаленні підходів до документального оформлення та обліку витрат, пов'язаних із впровадженням digital-технологій, зокрема для digital-аналізу. Це дозволить сформувати комплексну систему управління digital-ризиками та підвищити прозорість управлінських рішень у фінансових установах.

Література

1. Davenport T.H., Patil D.J. Data Scientist: The Sexiest Job of the 21st Century. URL: http://hbr.org/2012/10/data-scientist-the-sexiest-job-of-the-21st-century/ar/1 (дата звернення: 27.03.2025).

2. Miller M. B. Quantitative financial risk management. Hoboken: Wiley & Sons, Incorporated, John, 2018. 320 p.

3. Hassan M., Abdel-Rahman Aziz L., Andriansyah Y. The role artificial intelligence in modern banking: an exploration of ai-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. *Reviews of contemporary business analytics*. 2023. Vol. 6, no. 1. P. 110–132.

4. Banking fraud identification and prevention / F. Mehdipour, S. Asadi, M. Jalali et al. *27th International Conference on Circuits, Systems, Communications and Computers (CSCC)*, Rhodes (Rodos) Island, Greece, 19–22 July 2023. 2023. https://doi.org/10.1109/cscc58962.2023.00019.

5. Холявко Н., Садчикова І., Колоток М. Напрями використання штучного інтелекту у банківських установах. *Проблеми і перспективи економіки та управління.* 2023. № 2 (34). С. 192–203. https://doi.org/10.25140/2411-5215-2023-2(34)-192-203.

6. Kovalenko V. Digital transformation of the banking sector of the economy of Ukraine. *Фінанси України*. 2021. Vol. 2021, no. 3. P. 84–98. https://doi.org/10.33763/finukr2021.03.084.

7. Zhavoronok A., Kholiavko N. Banking system of Ukraine: trends and prospects of development. *Modern Science*. 2020. No. 10. P. 129–142.

8. Кузнєцова Л. В., Шмуратко Я. А. Регулювання ринку похідних фінансових інструментів в умовах глобальної економічної нестабільності : монографія. Харків : Диса Плюс, 2018. 248 с.

9. Науменкова С., Міщенко С. Цифрова фінансова інклюзія: можливості та обмеження для України. *Науковий вісник ОНЕУ*. 2020. № 1–2 (274–275). С. 133–149.

10. Сидська О. В. Вплив цифрової трансформації на банківську конкуренцію. *Вісник Університету банківської справи*. 2020. № 1 (37). С. 67–74. https://doi.org/10.18371/2221-755x1(37)2020208210.

11. Poddębniak M. Unlocking the potential of digital analytics in finance and banking. *Piwik PRO*. URL: https://piwik.pro/blog/digital-analytics-in-finance-and-banking/ (дата звернення: 27.03.2025).

12. The role of analytics in the banking sector. *iabac.org*. URL: https://iabac.org/blog/the-role-of-analytics-in-the-banking-sector (дата звернення: 27.03.2025).

13. Malashniak M., Lesniak O. 7 strategies for digitalization in the financial sector. *N-iX*. URL: https://www.n-ix.com/digitalization-in-financial-services/ (дата звернення: 27.03.2025).

14. Dunlea J. Unlocking the power of data analytics in finance and banking. *Akkio*. URL: https://www.akkio.com/post/data-analytics-in-banking (дата звернення: 27.03.2025).

15. Як штучний інтелект трансформує банківську індустрію. URL: https://www.consultancy.uk/news/14017/how-artificial-intelligence-is-transforming-the-banking-industry (дата звернення: 27.03.2025).

References

1. Davenport, T. H., & Patil, D. J. (2012). *Data Scientist: The Sexiest Job of the 21st Century*. Retrieved from http://hbr.org/2012/10/data-scientist-the-sexiest-job-of-the-21st-century/ar/1.

2. Miller, M. B. (2018). *Quantitative Financial Risk Management*. Hoboken: John Wiley & Sons, Inc.

3. Hassan, M., Abdel-Rahman Aziz, L., & Andriansyah, Y. (2023). The role of artificial intelligence in modern banking: An exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. *Reviews of Contemporary Business Analytics*, 6(1), 110–132.

4. Mehdipour, F., Asadi, S., Jalali, M., et al. (2023). Banking fraud identification and prevention. In *Proceedings of the 27th International Conference on Circuits, Systems, Communications and Computers (CSCC)*, Rhodes Island, Greece, July 19–22. https://doi.org/10.1109/cscc58962.2023.00019.

5. Kholiavko, N., Sadchykova, I., & Kolotok, M. (2023). Directions of artificial intelligence use in banking institutions. *Problems and Prospects of Economics and Management*, 2(34), 192–203. https://doi.org/10.25140/2411-5215-2023-2(34)-192-203 [in Ukrainian].

6. Kovalenko, V. (2021). Digital transformation of the banking sector of the economy of Ukraine. *Finance of Ukraine*, 2021(3), 84–98. https://doi.org/10.33763/finukr2021.03.084.

7. Zhavoronok, A., & Kholiavko, N. (2020). Banking system of Ukraine: Trends and prospects of development. *Modern Science*, 10, 129–142.

8. Kuznetsova, L. V., & Shmurarko, Ya. A. (2018). *Regulation of the derivatives market under conditions of global economic instability: Monograph*. Kharkiv: Dysa Plus [in Ukrainian].

9. Naumenkova, S., & Mishchenko, S. (2020). Digital financial inclusion: Opportunities and limitations for Ukraine. *Scientific Bulletin of ONEU*, 1–2(274–275), 133–149 [in Ukrainian].

10. Sydska, O. V. (2020). The impact of digital transformation on banking competition. *Bulletin of the University of Banking*, 1(37), 67–74. https://doi.org/10.18371/2221-755x1(37)2020208210 [in Ukrainian].

11. Poddębniak, M. (n.d.). *Unlocking the potential of digital analytics in finance and banking*. Piwik PRO. Retrieved from https://piwik.pro/blog/digital-analytics-in-finance-and-banking/.

12. IABAC. (n.d.). *The role of analytics in the banking sector*. Retrieved from https://iabac.org/blog/the-role-of-analytics-in-the-banking-sector

13. Malashniak, M., & Lesniak, O. (n.d.). *7 strategies for digitalization in the financial sector*. N-iX. Retrieved from https://www.n-ix.com/digitalization-in-financial-services/.

14. Dunlea, J. (n.d.). *Unlocking the power of data analytics in finance and banking*. Akkio. Retrieved from https://www.akkio.com/post/data-analytics-in-banking.

15. *How artificial intelligence is transforming the banking industry* (n.d.). Retrieved from https://www.consultancy.uk/news/14017/how-artificial-intelligence-is-transforming-the-banking-industry.