

**КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА**

**Навчально-науковий інститут
«Інститут інформаційних технологій в економіці»**

Кафедра інформаційних систем в економіці

**ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА
«Системи штучного інтелекту»**

галузь знань	12 Інформаційні технології
спеціальність	122 Комп'ютерні науки

Форма навчання: очна (денна)

КВАЛІФІКАЦІЙНА МАГІСТЕРСЬКА РОБОТА

на тему: «Ідентифікація ризиків онлайн-оплат за допомогою алгоритмів
машинного навчання»

здобувача Оніщенко Діани Сергіївни

Науковий керівник: д. т. н., професор, Шевченко А. І.

**Робота допущена до захисту перед екзаменаційною
комісією з атестації здобувачів вищої освіти (ЕК)**

Завідувач кафедри: к.е.н., доцент Тішков Б.О. _____

Київ 2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА
Навчально-науковий інститут «Інститут інформаційних технологій в економіці»
Кафедра інформаційних систем в економіці

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА

«Системи штучного інтелекту»

галузь знань	12 Інформаційні технології
спеціальність	122 Комп'ютерні науки

ПОГОДЖЕНО:

Керівник проєктної групи (гарант)
освітньо-професійної програми

_____ Васильєва Л.В.
«___» _____ 2025р.

ЗАТВЕРДЖУЮ:

Завідувач кафедри інформаційних
систем в економіці

_____ Тішков Б.О.
«___» _____ 2025 р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувача вищої освіти Онiщенко Діани Сергіївни очної (денної) форми навчання

на підготовку кваліфікаційної магістерської роботи
на тему: «Ідентифікація ризиків онлайн-оплат за допомогою алгоритмів машинного навчання»

Тему затверджено наказом ректора Університету від «07» 03 2025 р. № 464

Кваліфікаційна магістерська робота виконується на матеріалах наукових публікацій та матеріалів з мережі інтернет

План кваліфікаційної магістерської роботи

Розділ I Дослідження предметної області

Розділ II Характеристика та постановка задачі побудови моделі

Розділ III Розроблення проєктних рішень

Об'єкт дослідження: методи машинного навчання для ідентифікації ризиків онлайн-оплат, зокрема шахрайства

Предмет дослідження: підходи до прогнозування, збирання та обробки інформації, що стосується онлайн-оплат, із застосуванням різноманітних технік машинного навчання.

Мета кваліфікаційної магістерської роботи: прийоми логічного аналізу та узагальнення, комплексного системного мислення, інтелектуального аналізу даних, а також алгоритми машинного навчання, зокрема кластеризацію, класифікацію, регресійний аналіз, дерева рішень, ансамблевi методи та оцінку точності моделей

Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети:

У розділі I здійснено аналіз проблеми шахрайства в онлайн-оплатах, а також розглянуто сучасні підходи до виявлення аномальних транзакцій за допомогою методів машинного навчання. Проведено огляд літератури щодо використання моделей класифікації та оцінено їх релевантність у фінансових застосуваннях.

У розділі II описано процес підготовки, очищення та трансформації даних, побудову ознак і методику відбору релевантних змінних. Детально розглянуто реалізацію моделей Random Forest, KNN і CatBoost, а також аргументовано вибір останньої як фінальної.

У розділі III проведено порівняльний аналіз ефективності моделей за основними метриками точності та протестовано рішення в реальному середовищі за допомогою A/B тестування. Узагальнено результати, зроблено висновки щодо практичного впровадження та запропоновано рекомендації для масштабування.

Завдання підготував

науковий керівник _____

_____ А. І. Шевченко

«____» _____ 2025р.

Завдання одержав

здобувач _____

_____ Д. С. Оніщенко

«____» _____ 2025р.

Реферат

Кваліфікаційна магістерська робота містить 95 сторінки, 3 таблиць, 46 рисунки, список використаних джерел з 45 найменувань, 4 додатків.

« Ідентифікація ризиків онлайн-оплат за допомогою алгоритмів машинного навчання »

Об'єктом дослідження виступають методи машинного навчання для ідентифікації ризиків онлайн-оплат, зокрема шахрайства

Предметом дослідження охоплює підходи до прогнозування, збирання та обробки інформації, що стосується онлайн-оплат, із застосуванням різноманітних технік машинного навчання.

Мета і завдання дослідження. прийоми логічного аналізу та узагальнення, комплексного системного мислення, інтелектуального аналізу даних, а також алгоритми машинного навчання, зокрема кластеризацію, класифікацію, регресійний аналіз, дерева рішень, ансамблеві методи та оцінку точності моделей Відповідно до поставленої мети визначені такі *завдання*:

- проаналізувати сучасні методи запобігання фінансовому шахрайству;
- вивчити існуючі підходи до застосування алгоритмів машинного навчання у сфері онлайн-оплат;
- зібрати та підготувати релевантний набір даних;
- побудувати, навчити та протестувати низку моделей класифікації;
- порівняти точність та інтерпретованість моделей;
- запропонувати рекомендації для подальшого впровадження.

Теоретична, методична та практична значущість отриманих результатів. Теоретична значущість роботи полягає у систематизації підходів до виявлення шахрайських транзакцій за допомогою методів машинного навчання, а також у розгляді ефективності різних моделей у контексті обмеженого балансу класів та високих вимог до точності. Окрему увагу приділено аналізу особливостей застосування алгоритму CatBoost, який раніше майже не використовувався для задач виявлення шахрайства, але продемонстрував високу точність і стійкість до переобучення. Методична значущість роботи полягає у формалізації етапів побудови системи виявлення ризиків – від підготовки даних, відбору ознак, навчання моделей до їх інтеграції в бізнес-процеси. Запропонована методика дозволяє відтворити або адаптувати рішення в інших організаціях зі схожою архітектурою даних. Отримані результати мають прикладну цінність і можуть бути використані для впровадження систем виявлення шахрайства в інших високонавантажених онлайн-сервісах. Розроблене рішення протестовано в умовах реального бізнес-середовища за допомогою A/B тестування, що дозволило зафіксувати зниження рівня шахрайських транзакцій без негативного впливу на клієнтський досвід. Це підтверджує ефективність моделі не лише з теоретичної точки зору, а й з позиції практичної доцільності та бізнес-цінності. Впровадження подібних систем може значно покращити якість аналітики ризиків, підвищити безпеку платіжних процесів і зменшити фінансові втрати компанії.

Рік виконання кваліфікаційної магістерської роботи – 2025.

Рік захисту роботи – 2025.

Ключові слова: транзакції, шахрайство, аномалії, fraud rate, машинне навчання.

Summary

Qualification master's thesis contains 95 pages, 3 tables, 46 figures, a list of 45 references, and 4 appendices.

"Identification of Online Payment Risks Using Machine Learning Algorithms"

Object of the Study: Machine learning methods for identifying online payment risks, particularly fraud.

Subject of the Study: Approaches to forecasting, collecting, and processing information related to online payments using various machine learning techniques.

Purpose and Objectives of the Study: The research involves methods of logical analysis and generalization, systems thinking, data mining, and machine learning algorithms such as clustering, classification, regression analysis, decision trees, ensemble methods, and model accuracy evaluation. The following objectives have been defined:

Analyze modern methods of preventing financial fraud;

Study existing approaches to applying machine learning algorithms in the field of online payments;

- collect and prepare a relevant dataset;
- build, train, and test several classification models;
- compare the accuracy and interpretability of the models;
- provide recommendations for further implementation.
- theoretical, Methodological, and Practical Significance of the Results:

The theoretical significance lies in the systematization of approaches to detecting fraudulent transactions using machine learning methods, as well as in evaluating the effectiveness of various models under class imbalance and high accuracy requirements. Particular attention is given to the analysis of CatBoost's application, which had rarely been used for fraud detection tasks but demonstrated high accuracy and resistance to overfitting.

The methodological significance lies in the formalization of the risk detection system development stages—from data preparation and feature selection to model training and integration into business processes. The proposed methodology allows for replication or adaptation in other organizations with similar data architectures.

The results have practical value and can be applied to the implementation of fraud detection systems in other high-load online services. The developed solution was tested in a real business environment using A/B testing, which showed a decrease in fraudulent transactions without negatively affecting customer experience. This confirms the model's effectiveness not only from a theoretical standpoint but also in terms of practical feasibility and business value. The implementation of such systems can significantly improve risk analytics, increase payment process security, and reduce financial losses for the company.

Year of Thesis Completion: 2025

Year of Defense: 2025

Keywords: transactions, fraud, anomalies, fraud rate, machine learning.

В і д г у к

про кваліфікаційну магістерську роботу здобувача навчально-наукового інституту «Інститут інформаційних технологій в економіці» освітньо-професійної програми «Системи штучного інтелекту»

Онiщенко Діани Сергіївни

на тему: «Ідентифікація ризиків онлайн-оплат за допомогою алгоритмів машинного навчання»

Обрана тема є надзвичайно актуальною в контексті зростаючої кількості онлайн-фінансових операцій і водночас – поглиблення проблематики платіжного шахрайства. Використання сучасних методів машинного навчання для виявлення аномалій у транзакціях відповідає сучасним вимогам бізнесу щодо автоматизації процесів ризик-менеджменту та забезпечення кібербезпеки.

Робота вирізняється чіткою структурою, ґрунтовним теоретичним аналізом, логічною послідовністю викладення матеріалу та високим рівнем технічної реалізації. Авторка продемонструвала глибоке розуміння предметної області, вміння працювати з відкритими датасетами, аналітичне мислення та навички програмування.

У роботі реалізовано повний цикл побудови системи виявлення фродових транзакцій – від попередньої обробки даних і вибору релевантних ознак до порівняння моделей (Random Forest, KNN, CatBoost) і проведення А/В тестування. Окрему цінність становить самостійна реалізація прототипу системи в тестовому середовищі.

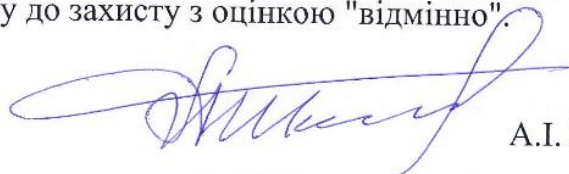
Робота містить як теоретичну новизну (у порівнянні ефективності алгоритмів та формалізації методики побудови моделей), так і практичну цінність. Запропоновані підходи можуть бути адаптовані для використання у платіжних системах і фінансових організаціях, що функціонують у високонавантаженому середовищі. Результати апробовані в умовах, максимально наближених до реальних, що підтверджує доцільність впровадження.

До незначних зауважень можна віднести перевантаженість окремих теоретичних блоків, де опис статистичних методів і алгоритмів іноді виходить за межі основної логіки дослідження. Водночас це не знижує загального наукового та практичного рівня роботи.

Робота Онiщенко Діани Сергіївни відповідає всім вимогам до магістерських досліджень, засвідчує високий рівень професійної підготовки здобувачки та її здатність самостійно вирішувати складні інженерно-наукові завдання. Рекомендую роботу до захисту з оцінкою "відмінно".

Науковий керівник:
Д.т.н., професор,
Чл.-кор. НАН України

«15» травня 2025 р.



А.І. Шевченко

Рецензія
на кваліфікаційну магістерську роботу
здобувача вищої освіти
Оніщенко Діани Сергіївни

Тема « Ідентифікація ризиків онлайн-оплат за допомогою алгоритмів машинного навчання »

Актуальність теми кваліфікаційної магістерської роботи і доцільність її розроблення: тема магістерської роботи є надзвичайно актуальною у контексті стрімкого зростання обсягів онлайн-платежів, що супроводжується еволюцією шахрайських схем і зростанням фінансових ризиків для компаній. Особливої ваги дослідження набуває з огляду на оновлені вимоги міжнародної програми Visa Acquirer Monitoring Program (VAMP), згідно з якими компанії з перевищеним рівнем диспутів зазнають негайних санкцій, що ставить перед бізнесом критичну потребу в надійних системах виявлення та попередження шахрайства. Запропонований підхід із використанням алгоритмів машинного навчання є своєчасним, інноваційним і здатен забезпечити реальний вплив на безпеку цифрових транзакцій.

Якість проведеного дослідження: Оніщенко Діана Сергіївна продемонструвала високий рівень підготовки та професійної зрілості під час виконання дослідження. Вона самостійно опрацювала значний обсяг літератури, нормативних матеріалів і актуальних джерел з тематики управління ризиками онлайн-платежів. У роботі системно застосовано сучасні методи машинного навчання, включно з CatBoost, ансамблевими моделями та підходами до балансування вибірки. Дослідження відзначається глибоким аналізом, високою якістю візуалізації, обґрунтованістю обраної моделі та чітким зв'язком між теоретичними викладками і прикладною реалізацією.

Позитивні риси кваліфікаційної магістерської роботи

- Високий рівень самостійності та ініціативності під час виконання практичних завдань;
- Системність і чітка структура роботи;
- Вдале поєднання теоретичної бази з практичною реалізацією;
- Інтеграція результатів у бізнес-процеси;
- Публічна презентація результатів на науковій конференції.

Практична значимість висновків і рекомендацій запропоноване рішення може бути апробовано в реальному середовищі та частково впроваджене у внутрішні процеси компанії, адже має високу прикладну цінність результатів. Методика може бути адаптована для будь-яких компаній, що працюють із високонавантаженими платіжними сервісами, з метою зниження fraud rate і підвищення якості управління ризиками.

Рецензент:

Андрій ЛУЗАН

Розробник програмного
забезпечення ТОВ «Айті Ленд»

Директор ТОВ «Айті Ленд»

Дрök Аліна



ЗМІСТ

ЗМІСТ	1
ВСТУП.....	3
РОЗДІЛ 1. ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ	7
1.1 Дослідження області цифрових фінансових транзакцій та ризик-менеджменту	7
1.1.1 Нормативно-правове та концептуальне підґрунтя безпеки онлайн-платежів	7
1.1.2 Класифікація та характеристика ризиків цифрових фінансових операцій	10
1.2 Аналіз вже існуючих програмних рішень та досліджень для створення систем штучного інтелекту (СШІ) в онлайн-фінансах.....	19
1.2.1 Огляд готових ІТ-рішень для виявлення транзакційних аномалій	19
1.2.2 Методи машинного навчання для ідентифікації ризиків онлайн-оплат....	23
1.3 Постановка проблеми та формування задач	37
1.4 Обґрунтування вибору підходів	40
Висновки до розділу 1.....	42
РОЗДІЛ 2. Характеристика та постановка задачі побудови моделі	44
2.1 Характеристика об'єкта дослідження	44
2.2 Структура і характеристика СШІ та їх компонентів	45
2.1.1 Алгоритми попередньої обробки даних.....	46
2.1.2 Алгоритм KNN	50
2.1.3 Random Forest	53
2.1.6 Метрики оцінки точності	54

2.1.5 Метрики оцінки точності	55
2.3 Методи, моделі і моделювання систем виявлення ризиків онлайн-оплат	59
2.3.1 Методи побудови та синтезу компонент систем виявлення шахрайства ...	59
2.3.2 Моделі та методи оптимізації систем ідентифікації шахрайських транзакцій	61
2.3.3 Методи та моделі управління поведінкою систем виявлення онлайн-шахрайства.....	62
Висновки до розділу 2.....	63
РОЗДІЛ 3. РОЗРОБЛЕННЯ ПРОЕКТНИХ РІШЕНЬ	64
3.1 Опис бази для системи оцінки ризику транзакцій в онлайн-платежах	64
3.2 Реалізація програмного компоненту	66
3.1 Проектування забезпечувальних підсистем СШ. Реалізація системи.....	72
3.2.1 Формування вибірки та її попередня обробка	72
3.2.2 Використання методу випадкового лісу	80
3.2.3 Використання методу KNN	81
3.2.4 Використання методу Voting model	83
3.2.5 Використання методу CatBoost	84
3.3 Організаційно-економічне забезпечення А/В тестування для перевірки ефективності системи.....	85
Висновки до розділу 3.....	87
ВИСНОВКИ	88
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	90
ДОДАТКИ	95

ВСТУП

Актуальність теми: Останніми роками грошові операції в Інтернеті зростають дуже швидко. З збільшенням обсягів грошових переказів з одного рахунку на інший зростає ризик того, що гроші можуть бути втрачені з банківського рахунку клієнта без його згоди, що також є основним фактором у цій сфері онлайн транзакцій. Попри впровадження новітніх методів автентифікації, таких як 3D-Secure чи біометрія, темпи зростання фінансового шахрайства не зменшуються. Наслідки таких дій виходять за межі лише фінансових втрат. Вони підривають довіру до фінансової системи, гальмують економічний розвиток і шкодять репутації як компаній, так і окремих осіб. Згідно з дослідженням Atlas VPN, проведеним у жовтні 2023 року, щорічні втрати світової економіки від кіберзлочинності та фінансового шахрайства становлять вражаючі \$8 трильйонів. Значна частина цієї суми припадає саме на шахрайські фінансові транзакції. Це на 13% більше, ніж у 2022 році, що вказує на стрімке зростання масштабів цієї проблеми.

Особливого значення в цьому контексті набувають методи машинного навчання, здатні автоматизувати аналіз даних і виявляти аномалії в режимі реального часу [1].

Аналіз останніх досліджень і публікацій: Проблематика боротьби з фінансовим шахрайством вже знайшла своє відображення в роботах [4] оцінили ефективність кількох класифікаторів, зокрема нейронних мереж і дерев рішень, для виявлення шахрайства з кредитними картками, підкреслюючи важливість метрик precision та recall у випадках значного дисбалансу. У ґрунтовному огляді [5] класифікували методи машинного навчання, застосовані до фінансового шахрайства, на п'ять типів: класифікація, кластеризація, прогнозування, виявлення аномалій і візуалізація – причому найвищу ефективність демонстрували моделі класифікації.

Симулятор PaySim, розроблений Lopez-Rojas і Axelsson [6], імітує мобільні фінансові транзакції і часто використовується у сучасних дослідженнях як бенчмарк для виявлення шахрайства. Його наближеність до реальних грошових потоків робить його цікавою альтернативою класичним наборам даних. Adewumi та інші використали PaySim для порівняння нагляданих моделей, таких як SVM, Random Forest і нейронні мережі, зазначивши, що ансамблеві методи демонструють кращу точність і стійкість порівняно з окремими класифікаторами.

Ансамблеві моделі на кшталт Random Forest та AdaBoost отримали широку увагу завдяки здатності ефективно працювати з шумними та незбалансованими даними [7]. Також варто згадати Gradient Boosting Machines, запропоновану Chen, яка з того часу успішно адаптується для задач виявлення шахрайства. Паралельно з цим активно досліджуються моделі глибинного навчання, зокрема прямі нейронні мережі та LSTM-архітектури, які здатні розпізнавати складні тимчасові патерни шахрайства [8]. Водночас ці підходи вимагають значних обсягів даних, ретельного налаштування, а також викликають побоювання серед фінансових регуляторів через "чорну скриньку" внутрішньої логіки моделей.

Водночас значна частина наявних рішень має обмежену здатність до генералізації, є чутливою до дисбалансу класів або недостатньо прозорою для фінансових регуляторів. Це свідчить про наявність нерозв'язаних аспектів у загальній проблемі, зокрема необхідності адаптивних, інтерпретованих і стійких до змін моделей.

Наукова проблема, яка лежить в основі цієї роботи, полягає в розробці системи для ідентифікації ризиків онлайн-оплат, що поєднує точність, адаптивність до нових даних і зрозумілість результатів.

Мета дослідження – розробка системи виявлення ризикованих транзакцій з використанням алгоритмів машинного навчання, здатної працювати в умовах високої мінливості даних і обмеженої частки шахрайських операцій.

Досягнення цієї мети передбачає виконання таких завдань:

- проаналізувати сучасні методи запобігання фінансовому шахрайству;

- вивчити існуючі підходи до застосування алгоритмів машинного навчання у сфері онлайн-оплат;
- зібрати та підготувати релевантний набір даних;
- побудувати, навчити та протестувати низку моделей класифікації;
- порівняти точність та інтерпретованість моделей;
- запропонувати рекомендації для подальшого впровадження.

Об'єктом дослідження виступають методи машинного навчання для ідентифікації ризиків онлайн-оплат, зокрема шахрайства

Предмет дослідження охоплює підходи до прогнозування, збирання та обробки інформації, що стосується онлайн-оплат, із застосуванням різноманітних технік машинного навчання.

Методи дослідження включають: прийоми логічного аналізу та узагальнення, комплексного системного мислення, інтелектуального аналізу даних, а також алгоритми машинного навчання, зокрема кластеризацію, класифікацію, регресійний аналіз, дерева рішень, ансамблеві методи та оцінку точності моделей.

Інформаційну базу складають наукові праці зарубіжних і вітчизняних дослідників, відкриті датасети, аналітика з офіційних сайтів і звіти незалежних агентств.

Наукова новизна роботи полягає в побудові системи ідентифікації ризиків онлайн-оплат за допомогою алгоритмів машинного навчання з урахуванням практичних обмежень і вимог інтерпретованості. Практичне значення дослідження визначається можливістю впровадження результатів у платіжні сервіси або фінансові стартапи, які стикаються з високим рівнем транзакційного ризику.

Результати дослідження були апробовані у вигляді прототипу системи для виявлення підозрілих транзакцій у тестовому середовищі, що дало змогу перевірити застосовність обраних підходів і оцінити їхню ефективність на практиці.

Інформаційна база дослідження складається з наукових публікацій відкритих транзакційних симуляторів, а також галузевої статистики .

Структурно магістерська робота складається з трьох розділів. Перший розділ присвячено теоретичному аналізу проблеми шахрайства в онлайн-оплатах, включаючи огляд сучасних наукових підходів до виявлення аномальних транзакцій та класифікаційних моделей, які застосовуються у фінансовій сфері. У другому розділі висвітлено методологію дослідження: описано джерела та способи збору даних, процес їх попередньої обробки, побудову ознак і обґрунтування вибору моделей машинного навчання. Третій розділ містить експериментальну частину, в якій проведено порівняльний аналіз ефективності обраних алгоритмів та описано впровадження системи в реальні бізнес-процеси.

РОЗДІЛ 1. ДОСЛІДЖЕННЯ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Дослідження області цифрових фінансових транзакцій та ризик-менеджменту

Із розвитком онлайн-оплат зросла потреба у впровадженні чітких стандартів безпеки, яких мали дотримуватись платіжні сервіси. У 2006 році спільними зусиллями американських та європейських платіжних асоціацій було розроблено першу версію стандарту PCI DSS, що визначав ключові вимоги до безпеки транзакцій [4]. Згодом Європейська комісія запровадила директиву PSD, метою якої стало уніфікування та спрощення системи електронних платежів у межах ЄС.

1.1.1 Нормативно-правове та концептуальне підґрунтя безпеки онлайн-платежів

PCI DSS

Із розвитком онлайн-оплат зросла потреба у впровадженні чітких стандартів безпеки, яких мали дотримуватись платіжні сервіси. У 2006 році спільними зусиллями американських та європейських платіжних асоціацій було розроблено першу версію стандарту PCI DSS, що визначав ключові вимоги до безпеки транзакцій [5]. Згодом Європейська комісія запровадила директиву PSD, метою якої стало уніфікування та спрощення системи електронних платежів у межах ЄС.

Стандарт PCI DSS (Payment Card Industry Data Security Standard) було запроваджено з ініціативи провідних міжнародних платіжних систем – Visa, MasterCard, American Express, JCB – та розроблено Радою зі стандартів безпеки індустрії платіжних карток (PCI SSC) як відповідь на зростаючі вимоги до захисту даних у сфері електронних платежів [6].

Цей стандарт представляє собою комплекс із 12 ключових вимог, що регламентують захист конфіденційної інформації власників платіжних карток під час її передачі, обробки та зберігання в інформаційних системах організацій [7].

Основою PCI DSS є принцип комплексного підходу до інформаційної безпеки – стандарт вимагає не лише технічного захисту, а й організаційних заходів, що охоплюють широкий спектр ризиків [8]. До переліку базових вимог входить:

Налаштування безпечного брандмауера для захисту даних карткових власників.

Заборона використання стандартних паролів і налаштувань безпеки, наданих постачальниками.

- забезпечення надійного захисту збережених карткових даних.
- шифрування переданих даних у відкритих і загальнодоступних мережах.
- встановлення та регулярне оновлення антивірусного ПЗ.
- розробка та підтримка захищених додатків і систем.
- обмеження доступу до даних лише для виконання службових обов'язків.
- присвоєння кожному користувачу унікального ідентифікатора для доступу до систем.
- контроль за фізичним доступом до інформаційних ресурсів.
- реєстрація та моніторинг усіх спроб доступу до систем і даних.
- регулярне тестування систем безпеки та процедур.
- формування політики інформаційної безпеки та забезпечення її виконання всім персоналом [9].

PSD

З 1 листопада 2009 року на території Європи набула чинності Директива ЄС про платіжні послуги (PSD), метою якої стало встановлення єдиних правил для електронних платежів у 30 країнах – серед них держави Європейського Союзу, а також Ісландія, Норвегія та Ліхтенштейн [7]. Це дозволило споживачам здійснювати фінансові операції – зокрема перекази коштів чи оплату дебетовими

картками – у межах Європи з такою ж простотою й безпекою, як і в межах власної країни.

У тексті директиви викладено вимоги до інформації, яку користувач повинен надати, аби транзакція була оброблена ефективно та надійно. Важливою новацією PSD стало відкриття ринку для нових гравців – так званих «платіжних установ», серед яких – сервіси грошових переказів, роздрібні компанії та оператори зв'язку. Разом із традиційними банками ці установи формують єдину – аа категорію – постачальники платіжних послуг.

Директива охоплює всі основні види електронних і безготівкових розрахунків, включно з кредитними переказами, прямими дебетами, картковими транзакціями (включно з оплатою кредитними картками), а також мобільними й онлайн-платежами. PSD не поширюється на операції з готівкою або чеками. При цьому захист і регулювання поширюються на платежі в будь-якій європейській валюті, за умови, що і платник, і одержувач послуг перебувають у межах однієї з 30 охоплених країн.

VAMP

У 2022 році загальні втрати, пов'язані з шахрайством в онлайн-платежах, досягли \$41 мільярда, а вже до кінця 2023-го ця сума зросла до \$48 мільярдів. Така динаміка свідчить про суттєву загрозу, що спонукає бізнес активніше фокусуватися на питаннях запобігання платіжному шахрайству. У цьому контексті Visa спільно зі своїми партнерами ставить собі за мету забезпечити захист усіх сторін, залучених у платіжну екосистему [1].

У відповідь на зростання ризиків, із 1 квітня 2025 року компанія запускає оновлену версію програми Visa Acquirer Monitoring Program (VAMP). Нова редакція VAMP передбачає запровадження метрики ризику та встановлення порогових значень, які будуть реалізовані поетапно. Це означає, що продавці в інтернеті мають відповідально ставитися до управління ризиками, аби не перевищити визначені ліміти.

Відповідно до нових правил, починаючи з квітня 2025 року, онлайн-бізнеси, у яких коефіцієнт VAMP перевищуватиме 1,5%, підлягатимуть негайному

моніторингу та фінансовим санкціям у розмірі \$10 за кожен випадок диспуту. З 2026 року поріг стане ще жорсткішим – 0,9%, що вимагатиме від компаній ще більш ефективних рішень у сфері управління ризиками. Таким чином, VAMP стимулює посилення безпеки в цифровому платіжному середовищі.

1.1.2 Класифікація та характеристика ризиків цифрових фінансових операцій

Поява та активне впровадження онлайн-оплат сприяли формуванню широкого спектру способів здійснення безготівкових розрахунків. Серед найпоширеніших – оплата за допомогою банківських карток, цифрових гаманців (таких як Apple Pay або Google Pay), ваучерів та QR-кодів, а також трансакції через SEPA-систему і розрахунки в криптовалюті. рис. 1.1 ілюструє, як розподіляються уподобання щодо платіжних методів у різних країнах – зокрема, у Великій Британії, Німеччині, Франції, Нідерландах, Росії, Іспанії, Швеції, Італії, США, Індії та Китаї. Представлені дані ґрунтуються на дослідженні, ініційованому компанією WayForPay, яке охоплювало інформацію, зібрану від 1820 торгових представництв [8].

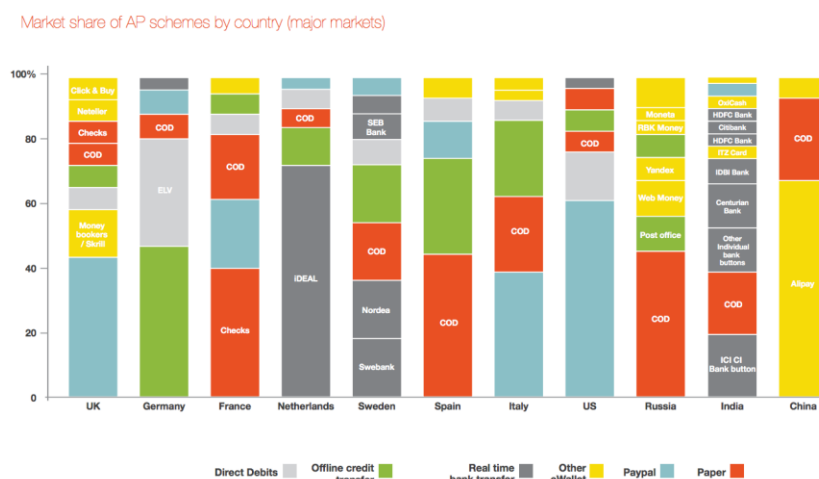


Рисунок 1.1 – Географічне співвідношення популярності альтернативних платіжних рішень

Табл. 1.1 демонструє, як часто використовуються альтернативні платіжні рішення в різних галузях економіки залежно від країни. Проте, згідно з оцінками

компанії WorldPay, через роздрібленість ринку в окремих сферах, статистичні дані можуть мати відхилення до 6% [8].

Серед ключових обмежень, притаманних альтернативним методам оплати, слід виділити відсутність можливості повторного використання платіжної інформації користувача. Це створює труднощі, зокрема, при налаштуванні автоматичних платежів, таких як підписки.

Таблиця 1.1 – Альтернативні платежі

	Велика Британія	Інші країни Європи	США	Азія	Інші країни
Гемблінг, казино	12–18%	63–69%	N/A	N/A	N/A
Контент для дорослих	14–20%	37–43%	26–32%	53–59%	82–86%
Відеоігри	12–18%	45–51%	28–34%	52–58%	78–82%
Цифровий контент	14–20%	38–44%	28–34%	33–37%	66–72%
Оптові продажі	7–13%	34–40%	20–26%	32–38%	N/A
Телекомунікації	8–14%	27–33%	14–20%	26–32%	47–53%
Квитки та розваги	10–16%	33–39%	14–20%	26–32%	61–67%
Послуги	8–14%	42–48%	14–20%	28–34%	41–47%
Медичне страхування	10–16%	24–30%	14–20%	26–32%	61–67%
Авіаквитки	3–9%	28–34%	4–10%	18–24%	36–42%
Туризм	3–9%	20–26%	6–12%	18–24%	34–40%
Регіональна торгівля	5–11%	29–35%	13–19%	22–28%	30–36%

Сплата податків та освіта	8–14%	18–24%	11–17%	25–31%	N/A
---------------------------	-------	--------	--------	--------	-----

Як свідчать тенденції останніх років, масштаби фінансового шахрайства продовжують зростати. За даними аналітичного звіту компанії NSN Consultants, у 2014 році сукупні втрати внаслідок шахрайських транзакцій досягли 21,84 більйона доларів США.

На рис. 1.2 наведено усереднені показники фінансових збитків, зафіксованих протягом десятирічного періоду. Водночас важливо відзначити, що за кожні 100 доларів, що проходять через платіжні системи, приблизно 6 доларів припадає на операції з ознаками шахрайства (див.рис. 1.3)[9] .

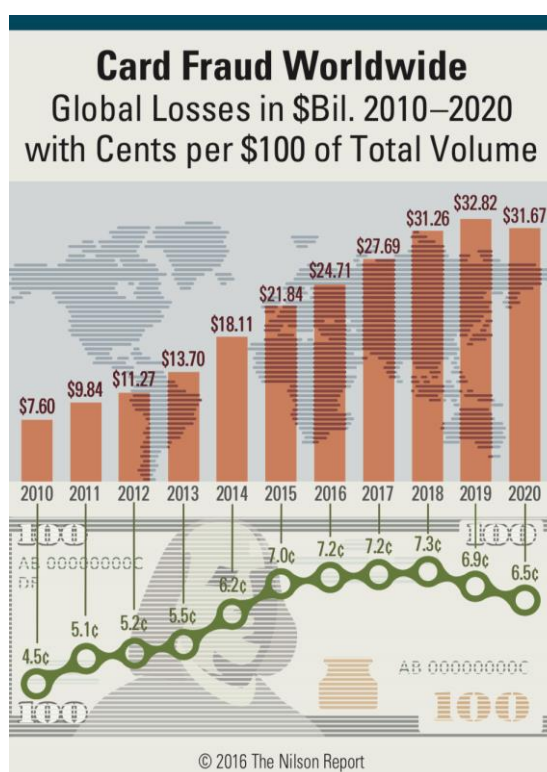


Рисунок 1.2 – Динаміка фінансових втрат, спричинених шахрайськими операціями



Рисунок 1.3 – Частка шахрайських втрат на кожні 100 доларів транзакцій

Основними джерелами шахрайських транзакцій вважаються такі категорії:

- Використання фальшивих платіжних карток;
- Операції типу CNP (card-not-present), коли транзакції здійснюються без фізичної присутності картки – наприклад, при оплаті через електронну пошту, телефон, соціальні мережі або сумнівні вебзастосунки;
- Мобільні або десктопні додатки-шахраї, які непомітно списують кошти з рахунку користувача;
- Використання викрадених або загублених карток;
- Так зване “дружнє шахрайство” (friendly fraud), що має місце тоді, коли клієнт ініціює повернення коштів за послугу або товар, яким фактично скористався [12].

Для оцінки потенційних загроз, пов'язаних із шахрайськими транзакціями, в [13] було проаналізовано вибірку з приблизно 230 000 операцій, здійснених за допомогою кредитних карток. Згідно з наведеними даними, 205 000 транзакцій було ідентифіковано як справжні, а близько 25 000 – як фродові, які були відхилені платіжною системою. Візуалізація розподілу цих даних подана на рис. 1.4



Рисунок 1.4 – Аналіз даних вибірки

Було встановлено, що найбільший обсяг підозрілих транзакцій фіксується у таких країнах, як Мексика, Перу, Малайзія, Франція, США та Канада. Відповідні результати представлені на рис. 1.5.

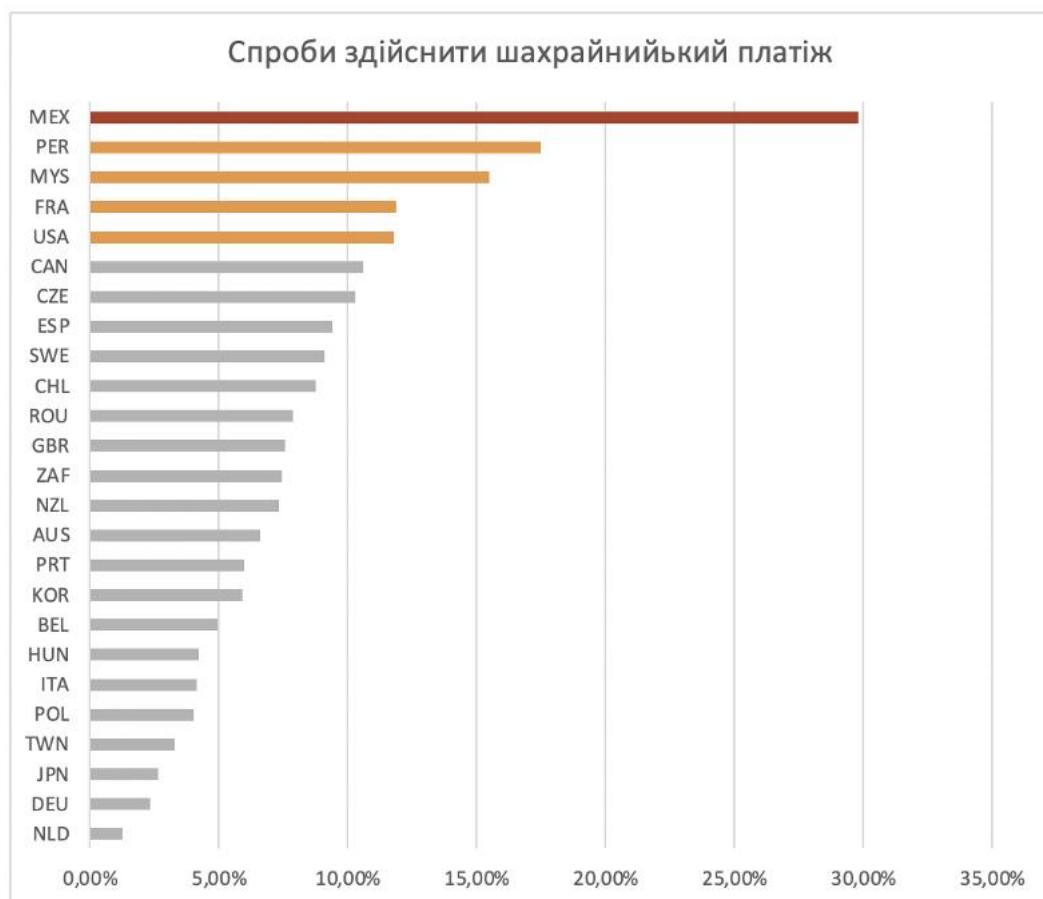


Рисунок 1.5 – Географічний розподіл спроб здійснення шахрайських транзакцій

Підвищений рівень шахрайських операцій у таких країнах, як Мексика, Перу та Малайзія, переважно пояснюється широким розповсюдженням випадків використання викрадених банківських карток. У той же час у Нідерландах, Німеччині, Японії та Тайвані частка фрод-транзакцій залишається незначною. Це пов'язано з тим, що в цих державах активно використовуються альтернативні платіжні системи – серед найпопулярніших: Alipay, WebMoney, WeChat, QIWI. Впровадження таких рішень суттєво знижує частоту CNP-операцій (тобто транзакцій без фізичної присутності картки), які є одним із головних векторів шахрайства.

У межах аналізу також було розглянуто основні причини, через які платіжна система блокує підозрілі транзакції. Їхній розподіл подано на рис. 1.6.

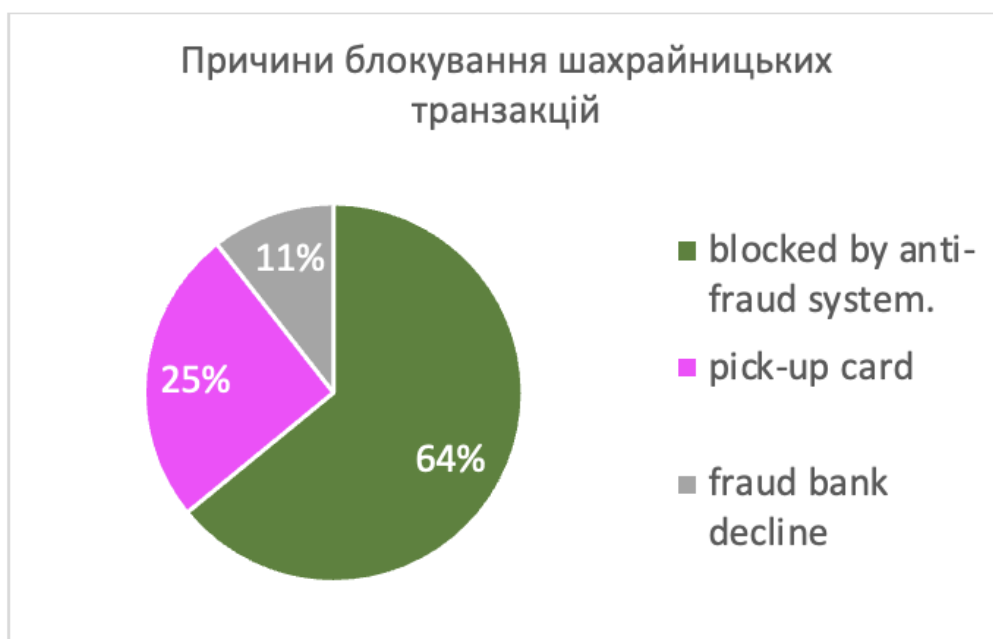


Рисунок 1.6 – Ключові фактори, що спричиняють блокування підозрілих транзакцій

Серед основних причин блокування транзакцій, зафіксованих у процесі дослідження, можна виділити кілька категорій:

- операції, заблоковані автоматизованою антифрод-системою платформи через підозрілу активність, наприклад, коли BIN-код картки внесено до чорного списку або користувача раніше вже було ідентифіковано як джерело високого ризику;
- транзакції, зупинені банківськими алгоритмами захисту – зазвичай це відбувається, коли операція відрізняється від звичного шаблону (наприклад, проводиться з незвичної для власника карти геолокації);
- платежі, що були ініційовані з викрадених платіжних карток і розпізнані як шахрайські.

Окремо було проаналізовано залежність між типом платіжної картки та частотою аномальних операцій. Як показано на рис. 1.7, найменша кількість фродових транзакцій припадає на Mastercard, тоді як найбільший рівень шахрайства зафіксовано для карток типу Discover.

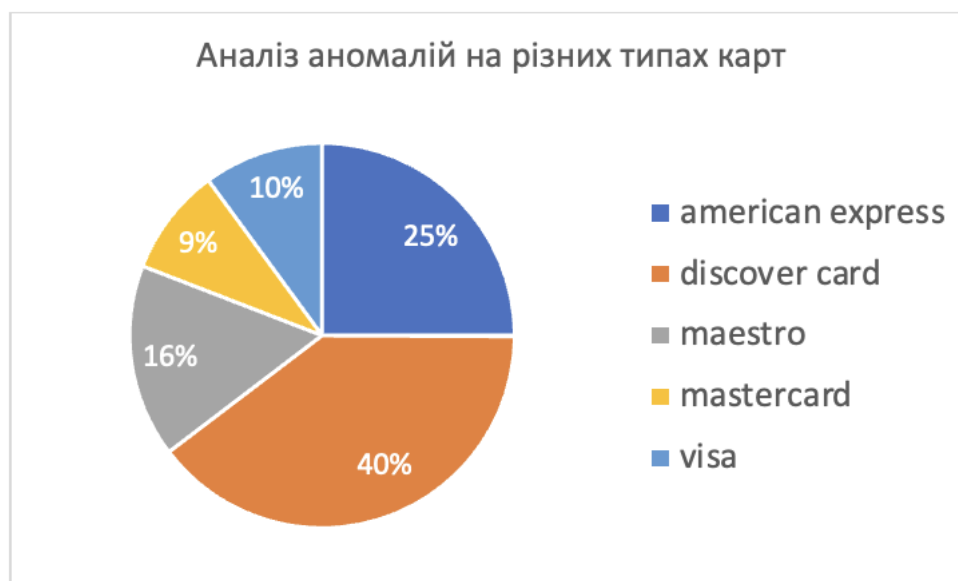


Рисунок 1.7 - Частка виявлених шахрайських транзакцій за типами платіжних карток

Як вже зазначалось раніше зазначалось, згідно з директиви про регулювання платежів, відповідальність за шахрайницькі платежі лягає на продавця (сервіс, додаток, веб-сайт, тощо), які надають можливість онлайн оплати.

Відповідно до норм, визначених у директиві щодо регулювання платіжних операцій, відповідальність за шахрайські транзакції в онлайн-середовищі переважно покладається на комерційні майданчики – це можуть бути сервіси, мобільні додатки чи веб-платформи, які забезпечують можливість безготівкових розрахунків.

Ті ситуації, коли оплата була здійснена через певний інтернет-ресурс, а запит на повернення коштів було подано безпосередньо через банк, позначаються терміном чарджбек (chargeback). У більшості випадків такі транзакції класифікуються як “дружнє шахрайство” (friendly fraud) – коли клієнт намагається повернути гроші, вже скориставшись послугою. Однією з найтипівіших причин цього явища є списання за підписки або освітні продукти, якими користувач більше не цікавиться [13]. Відповідну статистику наведено на рис. 1.8.

Слід додати, що Visa та MasterCard регламентують граничні показники chargeback-транзакцій: не більше 1% або 100 випадків від загального обсягу. У разі перевищення цих меж провайдер зобов'язаний сплатити штраф за кожну додаткову операцію, що підпадає під цю категорію: 50 доларів США у випадку з Visa; 25 доларів США для MasterCard [14].

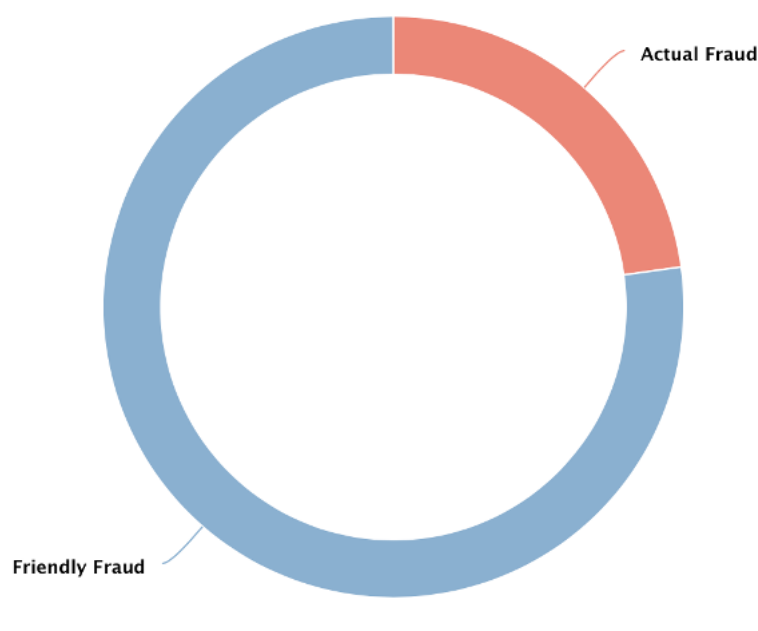


Рисунок 1.8 - Статистичний розподіл транзакцій типу chargeback за даними [14]

Розглянемо вхідний набір даних з точки зору кількості транзакцій, що були відхилені через підозру на шахрайство, а також визначимо частку операцій, що підпали під категорію chargeback.

Зокрема, для платіжних карток системи Visa зафіксовано, що 14% транзакцій мали ознаки фродової активності, а 2% були класифіковані як повернення коштів на вимогу клієнта (chargebacks). Деталізація цих показників наведена на рис. 1.9.

З огляду на те, що загальний обсяг операцій з картками Visa становив 47 534 транзакції, можна підрахувати, що приблизно 950 з них були повернуті клієнтам у межах процедури chargeback.

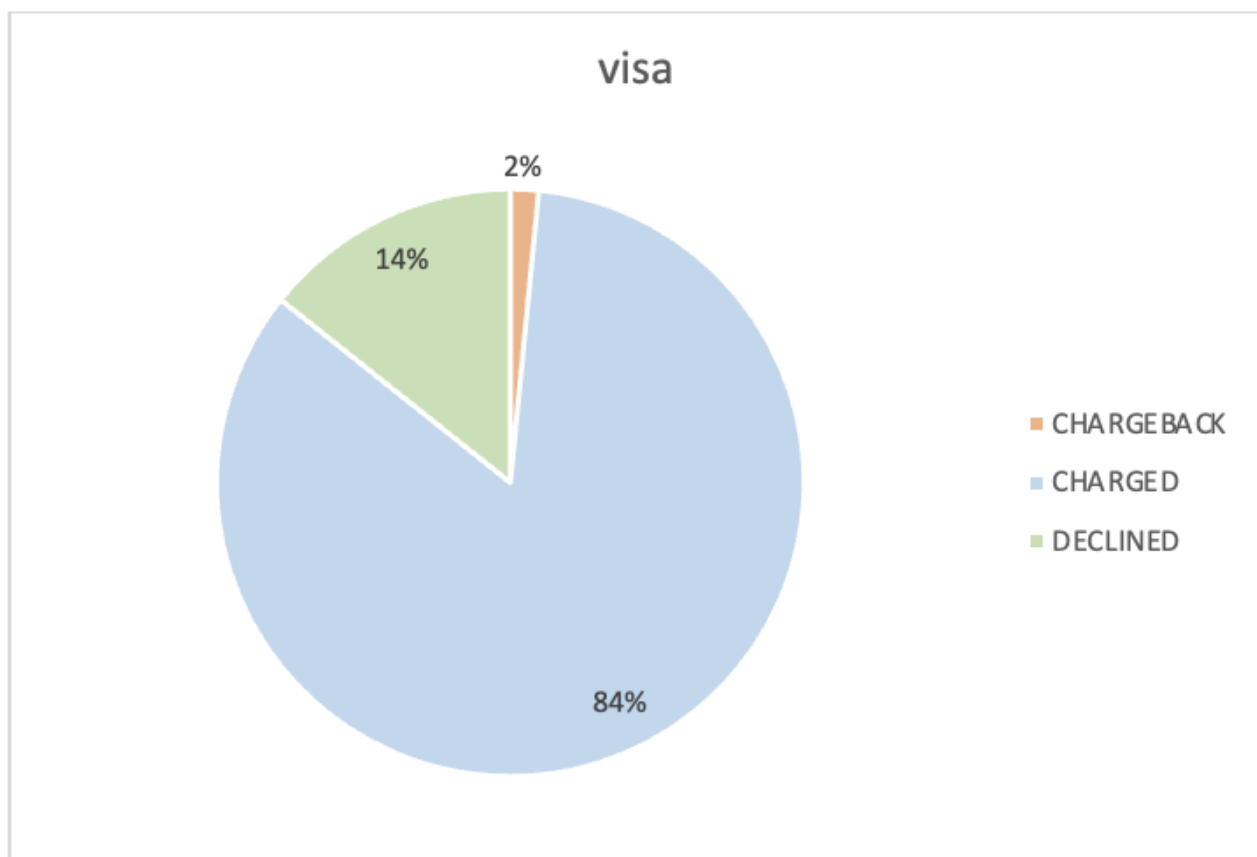


Рисунок 1.9 – Аналіз вибірки за показниками chargeback-операцій та виявлених фродових транзакцій

1.2 Аналіз вже існуючих програмних рішень та досліджень для створення систем штучного інтелекту (СШІ) в онлайн-фінансах

1.2.1 Огляд готових ІТ-рішень для виявлення транзакційних аномалій

Серед сучасних рішень у сфері виявлення фінансових шахрайств однією з найефективніших платформ вважається система ThreatMark. На відміну від класичних систем AFS (Anti-Fraud Systems), які зазвичай складаються з декількох окремих модулів – таких як контроль транзакцій, управління кейсами, виявлення мереж фроду тощо – ThreatMark орієнтується на швидкість реакції та адаптивність до нових типів загроз. Хоча традиційні рішення можуть забезпечувати більш гнучке налаштування та ширші функції для обміну даними, їх впровадження часто вимагає значних часових і технічних ресурсів.

Крім того, класичні антифрод-системи складніші в управлінні та потребують значного внутрішнього супроводу для підтримки та оптимізації. Важливо наголосити, що більшість таких рішень покладаються на сигнатурний підхід і аналіз лише транзакційної активності, що не дозволяє ефективно протидіяти сучасним загрозам, зокрема атакам нульового дня, захопленню сесій, соціальній інженерії чи злому через браузер користувача. Також такі системи практично не враховують поведінкову біометрію, що знижує їхню здатність точно ідентифікувати аномалії та призводить до великої кількості хибнопозитивних спрацьовувань.

Ще одним недоліком традиційних рішень є їх вразливість до обхідних дій з боку зловмисників. Наприклад: Фродери можуть поступово «навчити» систему, використовуючи один і той самий пристрій та виконуючи дії з низьким ризиком, аби сформувати «безпечний» профіль перед шахрайською транзакцією. Вони здатні використовувати пристрої самих жертв, застосовуючи шкідливе ПЗ для дистанційного доступу, що дозволяє імітувати справжню поведінку користувача.

Інший поширений метод – автоматизовані скрипти, які виконуються у сесіях жертв після входу, і непомітно ініціюють перекази коштів на заздалегідь визначені рахунки без явної компрометації облікових даних.

Система ThreatMark AFS була створена як відповідь на ці недоліки – вона здатна оперативно адаптуватися до нових типів загроз, демонструючи вищу гнучкість і швидкодію порівняно з традиційними підходами. Інтерфейс системи та її функціональні можливості зображено на рис. 1.10 [15].

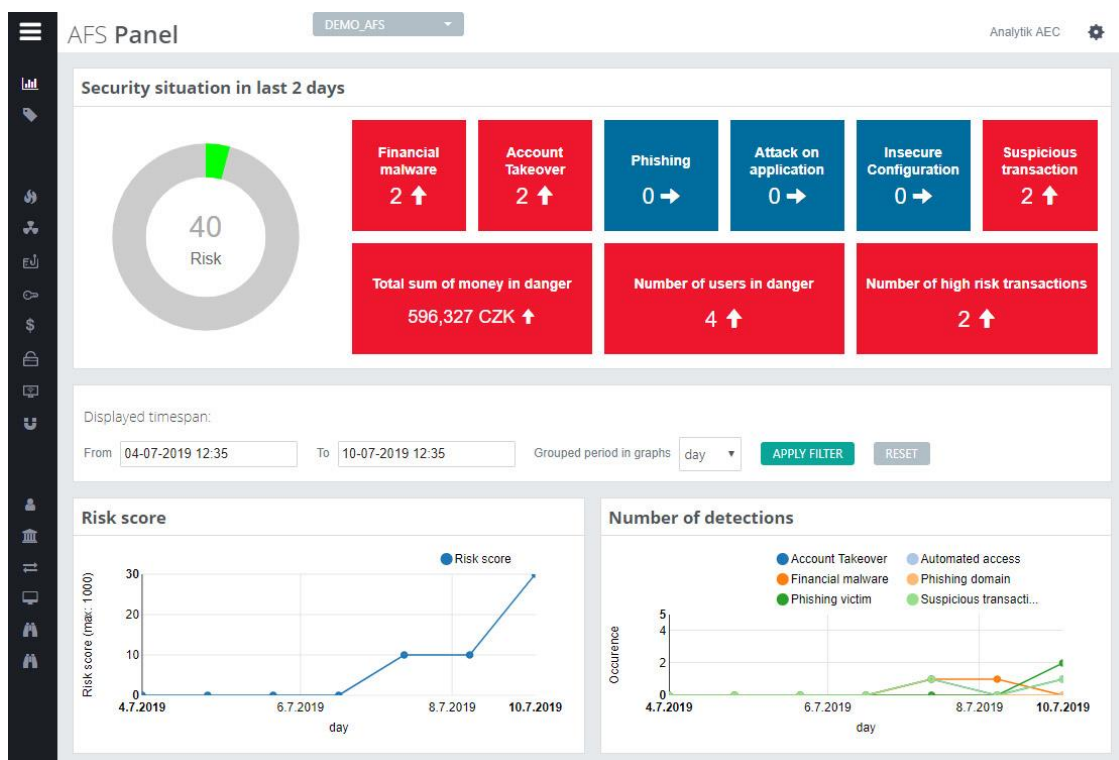


Рисунок 1.10 – Візуальне представлення інтерфейсу платформи виявлення шахрайства ThreatMark

Для всебічної оцінки системи ThreatMark розглянемо її основні сильні та слабкі сторони. До ключових переваг варто віднести наступне: Система AFS функціонує як сервіс, що базується на розгорнутому програмному стеку з використанням компонентів відкритого коду та специфічного середовища ОС Linux. Кожна версія платформи строго пов'язана з конкретними бібліотеками, конфігураціями та версіями ПЗ, що унеможливорює її інсталяцію в невідконтрольному середовищі. Це гарантує стабільність та керованість усіх інсталяцій. Використання так званої «чорної скриньки» дає змогу зберігати однакову конфігурацію системи на всіх клієнтських інсталяціях. Усі оновлення базуються на стабільному, відомому стані системи, що забезпечує оперативність і передбачуваність оновлень. Завдяки цьому значно зменшуються витрати на технічне обслуговування, а вивільнені ресурси можуть бути спрямовані на розробку нових функціональних можливостей.

Одним із ключових продуктів компанії ThreatMark є система Clair, зображена на рис. 1.11.

Clair – це SaaS-рішення, орієнтоване на виявлення шахрайських дій у цифрових кредитних додатках, що використовуються кінцевими споживачами. Платформа ґрунтується на технологіях поведінкової біометрії та детальному аналізі даних, які збираються під час користувацьких онлайн-сеансів. Завдяки цьому система дозволяє оперативно оцінювати ризики та ідентифікувати фрод-активність у режимі реального часу [17].

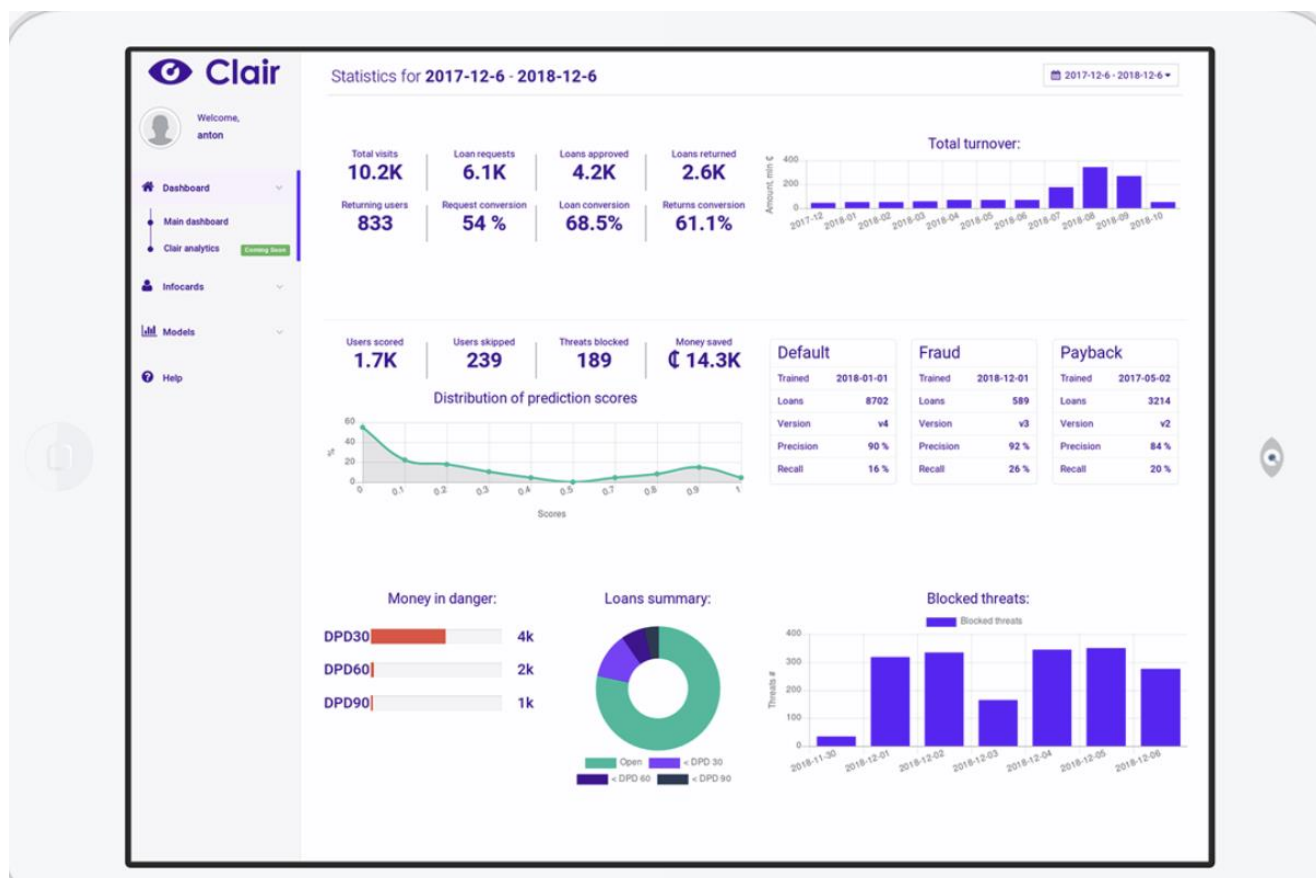


Рисунок 1.11 - Візуалізація інтерфейсу підсистеми Clair для виявлення шахрайства

З метою виявлення сильних і слабких сторін кожного з розглянутих рішень було проведено їх детальний порівняльний аналіз. Основні аспекти функціональності, технічних вимог, ефективності виявлення шахрайства та гнучкості налаштування систем зведено у формат узагальнюючої табл.1.2

Таблиця 1.2 – Порівняння існуючих програмних рішень

	Вартість використання	Сумісність та впровадження	Формат подання даних
ThreatMark	0,01 \$ за одну операцію; додатково передбачено регулярну плату та окрему оплату за інтеграцію	Інтеграція проходить без ускладнень, однак система підтримує лише обмежену кількість сценаріїв	Збирає широке коло користувацьких параметрів і демонструє їх у вигляді інтерактивних панелей
Clair	0,01 \$ за транзакцію + регулярні витрати на користування сервісом	Оптимізована під кредитні онлайн-сервіси, гнучкість застосування – частково обмежена	Відображає транзакційний аналіз за допомогою графічних панелей у режимі реального часу

На основі проаналізованих даних, що подані в таблиці, можна зробити висновок, що одним із ключових обмежень досліджених рішень є значні витрати, пов'язані з їх впровадженням та подальшим технічним супроводом.

1.2.2 Методи машинного навчання для ідентифікації ризиків онлайн-оплат

Одним із поширених підходів до виявлення фродової активності є аналіз аномалій через статистичне моделювання. Зокрема, ефективним інструментом

виступає використання Гауссівського розподілу, який дозволяє описати поведінку нормальних (нефродових) транзакцій.

Розподіл Гаусса застосовується для опису ймовірностей безперервної випадкової величини X , щільність розподілу якої визначається наступною формулою:

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

де:

μ — математичне сподівання,

σ — середнє квадратичне сподівання.

Ймовірність того, що випадкова величина X потрапить у заданий проміжок, обчислюється як площа під кривою щільності в межах цього інтервалу.

інтервалу (α, β) :

$$P(\alpha < x < \beta) = \Phi\left(\frac{\beta-\mu}{\sigma}\right) - \Phi\left(\frac{\alpha-\mu}{\sigma}\right)$$

де:

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_0^x e^{-\frac{x^2}{2}} dx \quad \text{— функція Лапласа}$$

Стандартний нормальний розподіл, що має форму симетричної дзвіноподібної кривої, характеризується середнім значенням $\mu = 0$ та стандартним відхиленням $\sigma = 1$

Варто підкреслити, що значення щільності ймовірності є максимальним поблизу середнього, після чого стрімко знижується зі зростанням віддаленості від центру розподілу.

Припустимо тепер, що маємо заданий набір спостережень $\{x^{(1)}, x^{(2)}, \dots, x^{(m)}\}$, Наближену форму Гауссівського розподілу можна визначити, застосувавши такі оцінки параметрів, що дозволяють описати поведінку даних на основі їх емпіричних характеристик:

$$\mu = \frac{1}{m} \sum_{i=1}^m x^{(i)}$$

$$\sigma^2 = \frac{1}{m} \sum_{i=1}^m (x^{(i)} - \mu)^2$$

Оцінювання параметрів здійснюється методом максимальної правдоподібності. У цьому контексті відстань між конкретним елементом даних і обчисленим середнім значенням використовується як індикатор його "аномальності". Для виявлення відхилень установлюється певний пороговий рівень, перевищення якого свідчить про аномалію. Слід зауважити, що різні підходи в межах цього класу можуть застосовувати відмінні способи визначення як самої відстані, так і граничного значення [19].

Введемо правило, згідно з яким можна буде класифікувати спостереження у вибірці як нормальні або аномальні (див.рис. 1.12):

$f(x_{tst}) < \varepsilon$ – умова за якої транзакція аномальна

$f(x_{tst}) \geq \varepsilon$ – умова за якої транзакція є нормальною

де:

ε – це деяке достатньо мале значення.

$f(x_{tst})$ – ймовірність x_{tst} в гауссовому розподілі

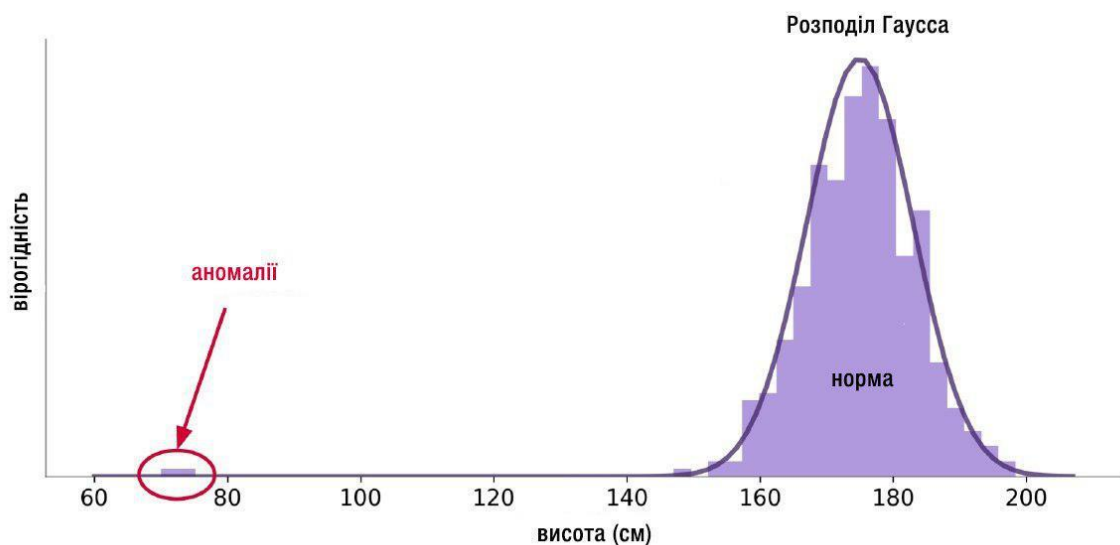


Рисунок 1.12 – Виявлення відхилення з використанням розподілу Гаусса

Під аномальною транзакцією розуміється така операція, яка має надзвичайно низьке значення ймовірності згідно з обраною моделлю розподілу. Спираючись на описаний вище підхід, можна сформулювати загальну послідовність дій для виявлення аномалій:

- Спочатку передається вхідний масив даних, що включає як звичайні, так і підозрілі транзакції.
- Далі цей масив розбивається на підгрупи, кожна з яких характеризується двома ознаками. Наприклад: час і сума операції; час та геолокація користувача; або час і тип пристрою, з якого була ініційована транзакція.
- Для кожного піднабору обчислюються ймовірнісні характеристики.
- Отримані результати візуалізуються – на основі графіків стає можливим визначення транзакцій, що значно відхиляються від типових, тобто вважаються аномальними.

Ще одним підходом до виявлення аномалій є статистичні методи, відомі також як моделі, що базуються на ймовірнісних припущеннях. Вони ґрунтуються на ідеї, що "нормальні" дані підкоряються певній стохастичній (випадковій) моделі. Основна концепція полягає в побудові генеративної моделі, яка добре узгоджується з типовими спостереженнями у вибірці. Усі об'єкти, які мають дуже низьке значення ймовірності за цією моделлю, розглядаються як потенційні аномалії або викиди. Одним із ключових методів цієї категорії є оцінювання параметрів за принципом максимальної правдоподібності [20].

Нехай ζ - дискретна випадкова величина, що залежна від параметру θ . Нехай вона приймає значення з вибірки $\{x_1 x_2 \dots x_l\}$, із ймовірностями $\{p_1(\theta) p_2(\theta) \dots p_k(\theta)\}$ Задаємо таку вибірку значень випадкової величини ζ : $x_1 x_2 \dots x_n$.

Функцією правдоподібності дискретної випадкової величини ζ називають функцію:

$$L(x_1, x_2, \dots x_n, \theta) = p_1^{m_1}(\theta) \cdot p_2^{m_2}(\theta) \cdot \dots \cdot p_l^{m_l}(\theta),$$

де:

$$m_k - \text{число членів вибірки, котре співпадає з } x_k, k = \overline{1, l}, \sum_{k=1}^l m_k = n$$

У ролі оцінки невідомого параметра $\widehat{\theta}_n$ приймається таке його значення, при якому функція правдоподібності досягає свого максимуму. Отриману величину, що максимізує функцію, позначають як $\widehat{\theta}_n$ і трактують як оцінку максимальної правдоподібності.

$$\begin{aligned} \frac{dL}{d\theta} &= 0, \\ \frac{d \ln L}{d\theta} &= 0 \end{aligned}$$

— логарифмічне рівняння правдоподібності.[21]

Головне обмеження параметричних моделей полягає в тому, що в реальних умовах форма розподілу даних часто залишається невідомою або складною для точного визначення.

Шахрайські дії, як правило, потребують оперативного реагування, тому в таких задачах віддається перевага моделям, які забезпечують швидке навчання та високу швидкість прогнозування. Одним із таких методів є логістична регресія, яка, згідно з [19], продемонструвала високу ефективність у виявленні окремих типів фродово. Логістична регресія є окремим випадком багатofакторного регресійного аналізу, основною метою якого є вивчення взаємозв'язку між кількома незалежними змінними та однією залежною. Цей метод широко застосовується для вирішення задач класифікації.

Бінарна логістична регресія використовується тоді, коли цільова змінна може набувати лише двох можливих значень (наприклад, «фрод» або «не фрод»). Іншими словами, логістична модель дозволяє оцінити ймовірність настання певної події для конкретного об'єкта спостереження.

Математичний вигляд регресійної моделі можна подати у формі наступного рівняння:ї активності.

$$y = F(x_1, x_2, \dots x_n)$$

У моделі множинної лінійної регресії передбачається, що цільова змінна має лінійний зв'язок із незалежними змінними, і цей зв'язок можна описати за допомогою наступного математичного виразу:

$$y = a_0 + \sum_{i=1}^n a_i x_i,$$

де:

$a_0 \dots a_i \dots a_n$ – коефіцієнти моделі

x_i – вхідні фактори моделі

Варто зауважити, що одним із обмежень цього підходу є його неспроможність відображати поступовість змін, оскільки модель працює з бінарною залежною змінною, яка може набувати лише двох значень – 0 або 1. Для подолання цієї проблеми застосовується логіт-перетворення, що дозволяє інтерпретувати результат як ймовірність:

$$P = \frac{1}{1 + e^{-y}},$$

де:

P – ймовірність того, що станеться подія, котра нас цікавить

y – стандартне рівняння регресії

У результаті застосування логіт-функції вихідні значення трансформуються у ймовірності, що належать інтервалу від 0 до 1 (див.рис. 1.13).

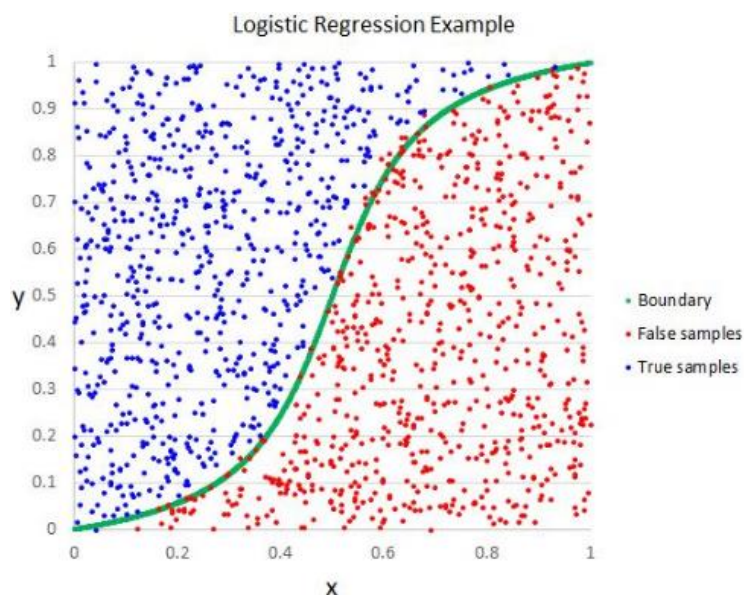


Рисунок 1.13 – Приклад класифікації за допомогою логістичної регресії

Більшість переваг і недоліків, притаманних лінійній регресії, певною мірою характерні й для логістичної моделі. Зокрема, серед її обмежень можна виділити складність тлумачення отриманих результатів – коефіцієнти не мають прямої адитивної інтерпретації, оскільки впливають на модель мультиплікативно через логіт-функцію.

Ще одним потенційним ускладненням є ситуація так званого повного розділення класів. Якщо в наборі даних присутня ознака, яка абсолютно точно розділяє об'єкти на два класи, логістична регресія не зможе побудувати адекватну модель. Це пояснюється тим, що відповідна вага прагнути до нескінченності, оскільки оптимальне значення параметра в таких умовах математично не існує. Водночас, якщо дані й так розділяються простим правилом – застосування машинного навчання просто не потрібне. Вирішенням проблеми повного поділу може бути використання регуляризації (штрафів на ваги) або залучення апріорних припущень щодо розподілу параметрів.

Серед переваг логістичної регресії варто відзначити не лише її здатність класифікувати об'єкти, але й можливість генерувати ймовірнісні оцінки належності до класів. Це є суттєвим плюсом порівняно з моделями, які надають лише жорстке рішення без оцінки впевненості. Наприклад, розуміння того, що

ймовірність належності об'єкта до певної категорії становить 99%, значно корисніше, ніж просто знання факту класифікації [2].

Крім того, логістичну регресію можна адаптувати до багатокласових задач. Така розширена версія відома як мультиноміальна регресія [22].

Дерева рішень – це моделі, які аналізують окремі характеристики транзакцій (наприклад, суму або геолокацію), щоб побудувати ієрархічну структуру рішень. Такий підхід дозволяє ефективно виявляти шаблони, притаманні шахрайській поведінці. Наприклад, операція, здійснена з нетипової країни та на велику суму, може бути автоматично віднесена до підозрілих.

Для математичного опису процесу поділу даних у дереві рішень вводиться поняття ентропії. Припустимо, що маємо множину A , яка містить n елементів, з яких m володіють певною характеристикою S . Тоді ступінь невизначеності (ентропію) цієї множини відносно ознаки S можна розрахувати за наступною формулою:

$$H(A, S) = -\frac{m}{n} \log_2 \frac{m}{n} - \frac{n-m}{n} \log_2 \frac{n-m}{n}$$

Як можна помітити, значення ентропії залежить від того, наскільки рівномірно елементи множини розподілені між можливими класами. Якщо співвідношення між класами зростає від 0 до 0,5, ентропія також збільшується; після цього значення вона починає спадати симетрично.

У випадку, коли характеристика

S не є бінарною й може набувати L різних значень, кожне з яких зустрічається у m_i випадках, формула для обчислення ентропії узагальнюється наступним чином:

Щоб знайти цю оцінку, необхідно проаналізувати поведінку функції правдоподібності, застосовуючи до неї таку формулу:

$$H(A, S) = -\sum_{i=1}^L \frac{m_i}{n} \log \frac{m_i}{n}$$

Ще одним важливим показником, що використовується для вибору найкращого атрибута в побудові дерева рішень, є інформаційний приріст –

теоретико-інформаційний критерій, який визначає доцільність розбиття даних за певною ознакою.

Припустимо, маємо множину об'єктів A , де деяка їх частина володіє властивістю S . Для класифікації цієї властивості використовується атрибут Q , що може набувати q різних значень. У такому випадку інформаційний приріст ($gain$) обчислюється за наступною формулою:

$$Gain(A, Q) = H(A, S) - \sum_{i=1}^q \frac{|A_i|}{A} \cdot H(A_i, S)$$

де A_i — це множина елементів A , на яких атрибут Q приймає значення i .

На кожній ітерації алгоритм надає перевагу тому атрибуту, який забезпечує максимальний приріст інформації порівняно з іншими варіантами.

Ще одним не менш значущим показником, який використовується при побудові дерев рішень, є індекс Джині. Цей критерій базується на принципі оцінки "чистоти" розподілу за певною ознакою. Для вибірки A і властивості S , що має s різних значень, індекс Джині розраховується за наступною формулою:

$$Gini(A, S) = 1 - \sum_{i=1}^s \frac{|A_i|}{A}$$

Відповідно, для набору тестів A і атрибуту Q , що має q значень і цільової властивості S , що має s значень, індекс вираховується наступним чином:

$$Gini(A, Q, S) = Gini(A, S) - \sum_{i=1}^q \frac{|A_i|}{A} \cdot Gini(A_i, S)$$

Індекс Джині частково нейтралізує тенденцію інформаційного приросту до вибору ознак з великою кількістю можливих розгалужень (див. рис. 1.14)..

Водночас обидва критерії зазвичай демонструють схожу поведінку – розбіжності у виборі оптимального атрибута спостерігаються менш ніж у ~2% випадків [25].

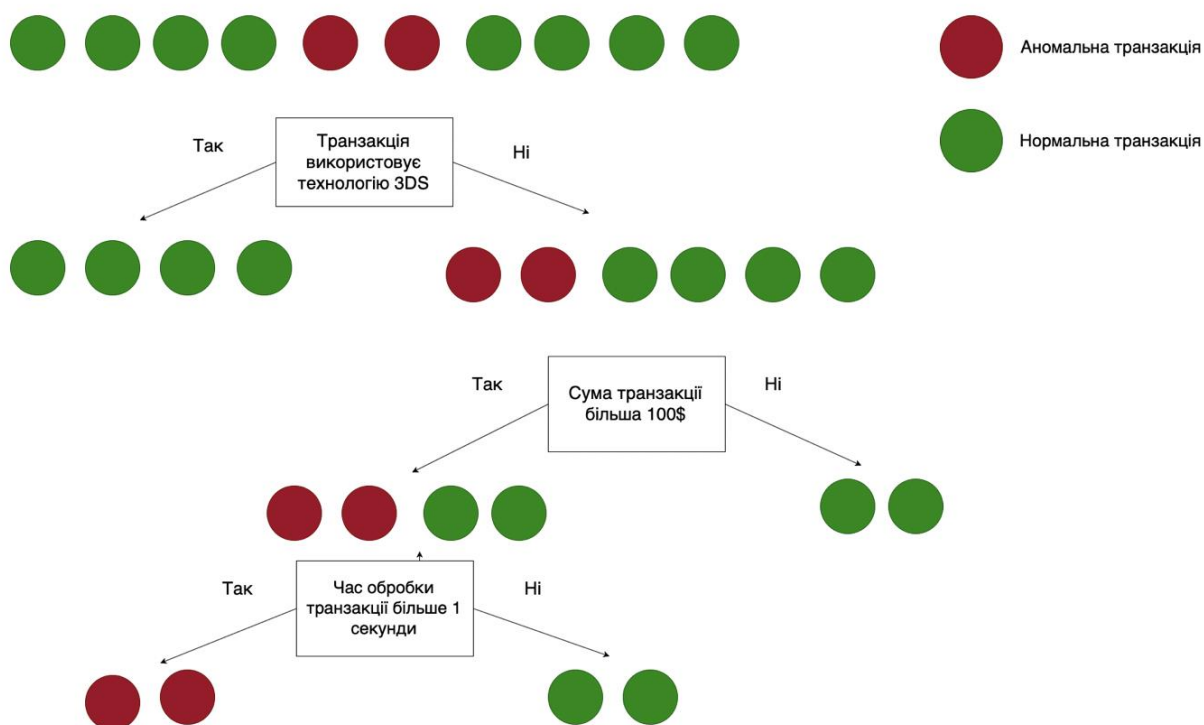


Рисунок 1.14 – Приклад використання дерева рішень для ідентифікації підозрілої транзакції

- На основі опрацьованих даних було сформовано такий підхід до побудови моделі:
- На початковому етапі подається вхідний набір, що містить як типові, так і фродові транзакції.
- Дані поділяються на дві частини: тренувальну множину для побудови моделі та тестову для перевірки її якості.
- Визначаються релевантні ознаки (атрибути), які можуть слугувати індикаторами шахрайства – наприклад, час проведення операції, геолокація, сума, тип пристрою.

- Задаються правила для зупинки росту дерева або обрізання гілок – зокрема, мінімальна кількість об'єктів у вузлі або допустимий рівень похибки.

Дерева рішень добре підходять як базові моделі для методів ансамблювання, зокрема беггінгу, оскільки вони мають високу гнучкість і здатні досягати майже нульової похибки на навчальній вибірці.

Для зменшення взаємної корельованості між окремими деревами та запобігання перенавчанню ефективно застосовується метод випадкових підпросторів. Його суть полягає в тому, що кожна модель навчається на випадково вибраній підмножині вхідних ознак, що підвищує різноманітність ансамблю (див. рис. 1.15).

Побудова ансамблю моделей із використанням цього підходу здійснюється за такою послідовністю:

- Припустимо, що маємо - N , а кількість ознак – D
- Оберемо L - число моделей для ансамблю
- Кожній моделі l обираємо dl ($dl < D$) як число ознак для l .
- Кожній моделі l створюємо навчальну вибірку, обравши dl ознак з D та навчаємо модель.
- Для застосування ансамблевої моделі до нового прикладу необхідно агрегувати результати, отримані від кожного з окремих класифікаторів

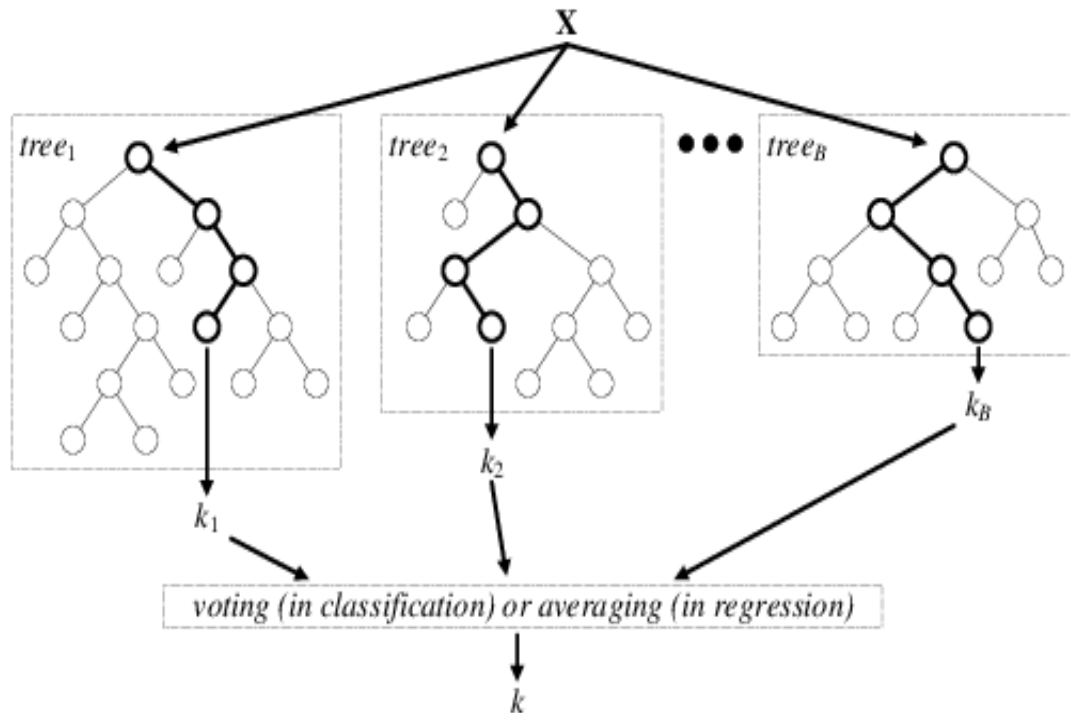


Рисунок 1.15 – Демонстрація функціонування алгоритму Random Forest на прикладі

Для формування випадкового лісу, який включає N окремих дерев рішень, застосовується наступна послідовність:

Для кожного $n = 1, \dots, N$:

1. Створюється навчальна підвибірка X_n за допомогою бутстрапа
2. На основі вибірки X_n будується дерев b_n
3. На кожному кроці будівництва дерева серед випадково відібраної підмножини ознак обирається та, що дає найкраще розділення відповідно до обраного критерію (наприклад, Gini або information gain), після чого здійснюється поділ вузла.
4. Процес повторюється доти, доки:
 - або кількість об'єктів у вузлі не стане меншою або рівною заданому порогу n_{min} ,
 - або не буде досягнута максимально дозволена глибина дерева.

У результаті побудови ансамблю формуємо узагальнену модель-класифікатор такого вигляду:

$$a(x) = \frac{1}{N} \sum_{i=1}^N b_i(x)$$

Варто зазначити, що в задачах класифікації зазвичай встановлюється $m = \sqrt{n}$, де n – кількість ознак, які враховуються при кожному поділі. Побудова дерева триває доти, поки в кожному листі не залишиться лише один елемент [24, 25].

Ще одним популярним підходом до розв'язання задач класифікації є метод k найближчих сусідів (K-Nearest Neighbors, KNN). Припустимо, що маємо певну кількість об'єктів, кожен з яких вже належить до одного з відомих класів. Завдання полягає в тому, щоб розробити правило, яке дозволяє віднести новий об'єкт до відповідної категорії.

Суть методу полягає в наступному: новий елемент відноситься до того класу, представників якого найбільше серед його k найближчих "сусідів" – тобто об'єктів, подібних до нього за ключовими характеристиками. (рис. 1.16)

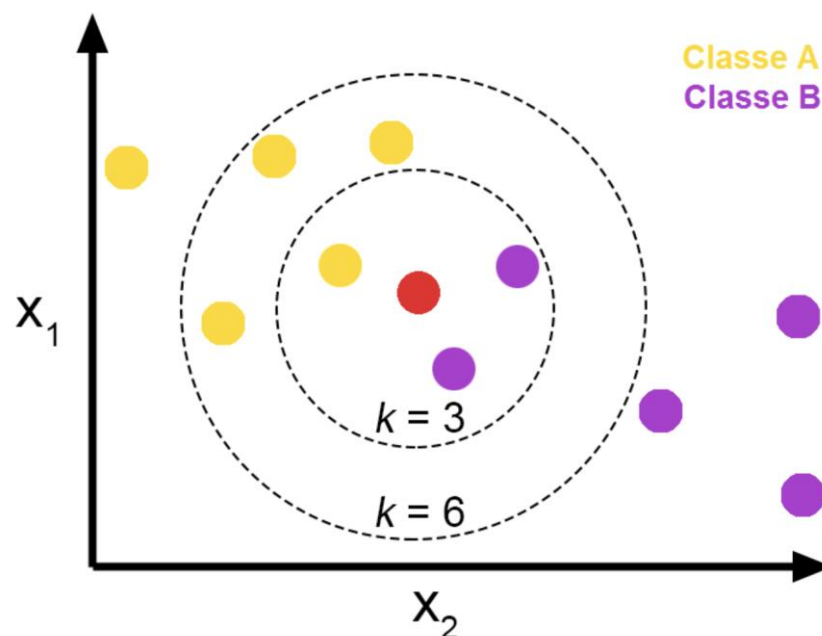


Рисунок 1.16– Приклад K-Nearest Neighbors

Відстань між об'єктами може визначатися, зокрема, за допомогою евклідової метрики, яка є одним із найпоширеніших способів вимірювання подібності:

$$d(p, q) = d(q, p) = \sqrt{(q_1 - p_1)^2 + (q_2 - p_2)^2 + \dots + (q_n - p_n)^2} = \sqrt{\sum_{i=1}^n (q_i - p_i)^2}$$

Переваги методу:

- Відсутність припущень про розподіл даних – алгоритм ефективний навіть у випадках, коли залежності між змінними є складними або нелінійними.
- Простота реалізації та інтерпретації – логіка методу інтуїтивно зрозуміла, що робить його зручним для пояснення результатів.
- Загалом хороша точність – KNN здатен забезпечувати прийнятний рівень правильності класифікації, хоча й може поступатися складнішим алгоритмам.
- Гнучкість у застосуванні – метод може бути використаний як у задачах класифікації, так і регресійного прогнозування [26].

Обмеження методу:

- Обчислювальна складність – на відміну від багатьох інших моделей, KNN потребує збереження всіх навчальних прикладів, що уповільнює роботу при великому обсязі даних.
- Високе навантаження на пам'ять – оскільки зберігаються всі (або майже всі) об'єкти навчальної множини.
- Повільне прогнозування – оскільки під час передбачення виконується пошук серед усіх навчальних прикладів.
- Вразливість до нерелевантних ознак і масштабів – алгоритм чутливо реагує на шум та непропорційні дані, що може знижувати його ефективність.

Наyavi та Ravi в дослідженні [29] провели порівняльний аналіз різноманітних алгоритмів машинного навчання – зокрема, методу опорних векторів (SVM) і штучних нейронних мереж (ANN) – у контексті виявлення шахрайських операцій із кредитними картками. Це дослідження стало фундаментом для побудови систем фрод-детекшену на основі ML-підходів, продемонструвавши ефективність різних моделей у розпізнаванні складних шаблонів поведінки.

Результати роботи свідчать про здатність сучасних алгоритмів перевершувати традиційні системи, що базуються на жорстко заданих правилах. Попри це, автори також звертають увагу на певні обмеження, пов'язані з високою обчислювальною вартістю та труднощами в інтерпретації рішень моделей

У дослідженні [30] представлено інноваційний підхід, що базується на використанні ансамблю моделей глибинного навчання. Зокрема, авторами було розроблено архітектуру D3EF, яка поєднує кілька нейронних мереж для підвищення точності розпізнавання фродових транзакцій.

Дослідження демонструє високий потенціал глибинного навчання в ідентифікації складних закономірностей у даних, що дозволяє досягти більш точного виявлення шахрайських дій. Разом з тим, автори звертають увагу на значні обчислювальні ресурси, які потребує такий підхід, а також на зростаючу складність інтерпретації результатів подібних моделей.

1.3 Постановка проблеми та формування задач

Зі зростанням популярності веб-пошти значно збільшилася й кількість інших типів онлайн транзакцій. Нині вже нікого не дивує, що люди здійснюють банківські операції, оплачують рахунки та роблять покупки через інтернет. У більшості таких випадків користувач має обліковий запис у відповідній установі. Також існують ситуації, коли особа має віртуальний онлайн-акаунт – наприклад, як учасник різних клубів за інтересами, які мають власні веб-сайти та форуми. Доступ до таких акаунтів зазвичай здійснюється через веб-браузери[7].

Більшість опитаних – близько 65% – повідомили, що користувачі здійснюють транзакції з різноманітних типів пристроїв. Водночас тільки трохи більше половини (53%) використовують двоетапну перевірку особистості для захисту цих операцій. Половина компаній запровадили системи моніторингу шахрайства в режимі реального часу, хоча це вважається найефективнішим інструментом боротьби з кіберзагрозами.

Цікаво, що значна частка респондентів (48%) обмежилася лише зниженням рівня ризику замість повного запобігання інцидентам. До того ж 29% представників визнали, що економічно вигідніше реагувати на шахрайські випадки постфактум, аніж інвестувати в системи запобігання.

Протиправна діяльність становить серйозну загрозу для різних секторів економіки, підриваючи фінансову стійкість, шкодячи репутації компаній і створюючи ризики для інформаційної безпеки. Традиційні методи виявлення шахрайства часто виявляються малоефективними перед обличчям постійно змінюваних тактик зловмисників. У відповідь на це спостерігається стрімке зростання інтересу до використання методів машинного навчання (ML), які дають змогу ефективно виявляти й запобігати шахрайським операціям у режимі реального часу.

Виявлення аномалій фактично виступає інструментом виявлення шахрайських дій, оскільки підозрілі транзакції, як правило, відхиляються від загальноприйнятих шаблонів поведінки. Алгоритми такого типу ідентифікують нестандартні або неочікувані дії в системі, що найчастіше вказують саме на фродову активність [24]

Алгоритми машинного навчання здатні обробляти великі обсяги транзакційних даних, виявляючи приховані закономірності, аномальні відхилення та нетипову поведінку, які можуть залишитися непоміченими при традиційному аналізі. Зокрема, вони дозволяють виявити незвичні шаблони витрат, розбіжності в геолокації транзакцій, а також підозрілі мережеві зв'язки, що можуть свідчити про шахрайську активність.

Загальна структура побудови системи виявлення шахрайства включає такі етапи:

1. Збір та підготовка даних: Необхідно зібрати первинні транзакційні дані, що містять інформацію про суми, час проведення операцій, географічне розташування та профілі користувачів. Далі виконується очищення даних, усунення пропусків та аномалій, стандартизація форматів – задля забезпечення коректного функціонування алгоритмів.
2. Формування ознак (feature engineering): На основі наявних даних потрібно сформувати інформативні ознаки. Наприклад, обчислення середніх сум транзакцій, виявлення різких змін у поведінці користувача, аналіз географічної стабільності або часових інтервалів між операціями. Такі ознаки дозволяють алгоритмам точніше ідентифікувати потенційно шахрайські дії.
3. Вибір і навчання моделей: Серед наявних методів машинного навчання (наприклад, дерева рішень, випадкові ліси, метод опорних векторів, класифікатори на основі k-ближчих сусідів тощо) необхідно обрати ті, що найкраще відповідають природі даних та меті виявлення шахрайства. Навчання моделей відбувається на заздалегідь розміченому наборі даних.
4. Оцінка якості моделей та їх оптимізація: Моделі слід оцінити за допомогою метрик якості – таких як точність (accuracy), повнота (recall), точність позитивних передбачень (precision), F1-міра тощо. За результатами оцінки може бути проведене налаштування гіперпараметрів або обрання іншого алгоритму.
5. Впровадження моделі та моніторинг: Після досягнення прийнятного рівня якості модель інтегрується у виробниче середовище для аналізу нових транзакцій у режимі реального часу. Важливо забезпечити постійний моніторинг її ефективності та своєчасне оновлення у разі зміни поведінкових патернів шахрайства.

На основі описаних етапів формуються задачі, які необхідно реалізувати в рамках роботи:

- Збір та попередня обробка вхідних даних для подальшого аналізу

- Побудова навчальної та тестової вибірок для моделювання
- Навчання моделі машинного навчання та оцінка її якості за допомогою метрик точності, повноти та F1-міри
- Збереження навченої моделі у форматі, придатному для інтеграції у прикладні рішення
- Розробка програмного модуля для автоматичного прогнозування fraud rate на основі навченої моделі
- Проведення завершального тестування з метою перевірки коректності роботи алгоритму в реальних умовах

Кожна задача відповідає окремому етапу побудови системи виявлення шахрайства та забезпечує поступовий перехід від збору сирих даних до розгортання готової моделі у реальному середовищі. Такий підхід дозволяє структурувати процес дослідження, виділити ключові технічні компоненти та забезпечити цілісність розробки системи виявлення аномалій на основі методів машинного навчання.

1.4 Обґрунтування вибору підходів

Спираючись на результати опрацювання літературних джерел, було сформовано порівняльну характеристику основних алгоритмів, що застосовуються для виявлення шахрайства в цифрових фінансових системах. Для кожного з них розглянуто середній рівень точності, продемонстрований у відповідних дослідженнях. Зведена табл. 1.3 з порівнянням методів подана нижче .

Таблиця 1.3 – Порівняльний аналіз методів

Метод	Стійкість до аномалій	Робота з обмеженими даними	Підтримка масштабування	Багатокласова класифікація	Орієнтовна точність
Імовірнісний підхід (на основі нормального розподілу)	Так	Так	Ні	Ні	Середня ($\approx 82\text{--}91\%$)
Логістична модель	Ні	Ні	Так	Так	Висока ($\approx 87\text{--}92\%$)
Метод k-близьких прикладів (KNN)	Так	Ні	Ні	Так	Висока ($\approx 84\text{--}94\%$)
Алгоритм дерева прийняття рішень	Так	Ні	Так	Так	Середня ($\approx 81\text{--}89\%$)
Випадковий ліс (Random Forest)	Так	Ні	Так	Так	Висока ($\approx 87\text{--}96\%$)

На основі порівняльної характеристики розглянутих методів машинного навчання, найбільш придатними для задачі виявлення аномалій у фінансових транзакціях є метод k-близьких прикладів (KNN) та алгоритм випадкового лісу (Random Forest).

Обидва методи демонструють високу точність класифікації (в межах 84–96%) та підтримують багатокласову класифікацію, що є критично важливим у

контексті різноманітних типів шахрайської поведінки. Random Forest, крім того, добре масштабується на великі обсяги даних, тоді як KNN виявляє високу стійкість до аномалій.

Висновки до розділу 1

У першому розділі було здійснено ґрунтовний огляд предметної області, пов'язаної з ризиками в онлайн-платежах, а також досліджено сучасні технології для їх виявлення. Було виявлено, що попри впровадження низки нормативних ініціатив (таких як PCI DSS, PSD2, VAMP) та активну автоматизацію фінансових сервісів, рівень шахрайства в електронних транзакціях залишається високим. Причиною цього є не лише зростання обсягу цифрових платежів, але й постійна еволюція тактик зловмисників, що вимагає більш динамічних і гнучких підходів до захисту. Розглянуті програмні рішення, зокрема ThreatMark і Clair, демонструють прогрес у виявленні аномалій, але супроводжуються істотними витратами на впровадження та технічну підтримку.

Окрему увагу було приділено аналізу алгоритмів машинного навчання, серед яких логістична регресія, дерева рішень, Random Forest і метод k-ближніх сусідів показали найбільшу ефективність у виявленні шахрайства. Для реалізації поставленої задачі було обрано алгоритми KNN та Random Forest як найбільш придатні з огляду на точність і практичну ефективність. Таким чином, закладено теоретичну основу для подальшого розроблення власного підходу до виявлення фродових транзакцій.

Методи машинного навчання знаходять широке застосування в різноманітних галузях наукових досліджень, особливо з огляду на активне впровадження цифрових платіжних систем і мобільних фінансових сервісів. Однією з поширених проблем, з якою стикаються науковці під час роботи з такими даними, є дисбаланс класів – ситуація, коли кількість шахрайських транзакцій у

наборі даних суттєво менша, ніж легітимних. Класичні статистичні моделі, як правило, не дають бажаних результатів у подібних умовах, що зумовлює необхідність застосування більш ефективних алгоритмів із галузі сучасного машинного навчання.

РОЗДІЛ 2. ХАРАКТЕРИСТИКА ТА ПОСТАНОВКА ЗАДАЧІ ПОБУДОВИ МОДЕЛІ

2.1 Характеристика об'єкта дослідження

Об'єктом дослідження виступають методи машинного навчання для ідентифікації ризиків онлайн-оплат, зокрема шахрайства. Серед основних напрямів використання машинного навчання у виявленні шахрайства можна виділити такі:

Виявлення аномалій (Anomaly Detection): Алгоритми навчаються на історичних транзакційних даних і визначають нормальні шаблони поведінки. Відхилення від цих шаблонів інтерпретуються як потенційно шахрайські дії. Це дозволяє автоматично ідентифікувати підозрілу активність без необхідності задавати фіксовані правила.

Оцінка ризику (Risk Scoring): Побудовані моделі можуть присвоювати транзакціям або користувачам оцінки ризику на основі різноманітних факторів: сума транзакції, геолокація, частота, історична поведінка тощо. Це дозволяє пріоритезувати перевірки й ефективно використовувати ресурси служби безпеки.

Аналіз мережевих зв'язків (Network Analysis): Шахраї часто діють організовано, утворюючи складні взаємозв'язані структури. Методи графового аналізу дають змогу виявляти такі мережі шляхом дослідження взаємозв'язків між користувачами, акаунтами чи пристроями та ідентифікації нетипових кластерів.

Обробка текстових даних (Text Analysis): Алгоритми можуть аналізувати неструктуровані текстові джерела (електронні листи, відгуки користувачів, повідомлення в соціальних мережах) з метою виявлення ключових слів або шаблонів, які можуть свідчити про шахрайство.

Перевірка особистості (Identity Verification): Методи машинного навчання застосовуються для аналізу й автоматичної верифікації персональних даних –

наприклад, зображень документів чи обличчя користувача – з метою запобігання крадіжці особистих даних.

Адаптивне навчання (Adaptive Learning): Однією з ключових переваг машинного навчання є здатність моделей адаптуватися до змін. У міру того, як шахраї змінюють свої тактики, моделі можна перенавчати на нових даних, що дозволяє зберігати високу актуальність і точність виявлення

У даній роботі проблему ідентифікації ризиків онлайн-оплат визначаємо як прогнозування Fraud Rate (показник фроду) наступним чином.

Нехай набір векторів $\langle u_i, x_i, y_i \rangle, i = 1, 2, \dots, N$, де u_i і x_i відображає користувачів та транзакцію, відповідно. Якщо для u_i транзакція виявляється фродом x_i , то $y_i = 1$, інакше $y_i = 0$. Прогнозування Fraud Rate полягає в тому, щоб передбачити, чи для користувач u_j банк ідентифікує транзакцію як fraud x_j , тобто $p = f(u_j, x_j)$, де p називається Fraud Rate .

Математично формуємо функцію $p = f(u, x)$ для отримання Fraud Rate шляхом мінімізації функції втрат перехресної ентропії, яка надається таким чином:

$$L = -\frac{1}{N} \sum_{i=1}^N [y_i \times \log p_i + (1 - y_i)(1 - \log p_i)],$$

де $y_i = 0$ (або 1) - цільова мітка, $p_i \in [0; 1]$ – прогнозований Fraud Rate, N – розмір вибірки

2.2 Структура і характеристика СШІ та їх компонентів

Рис. 2.1 ілюструє загальну архітектуру системи, яка включає модуль первинної обробки даних, модуль розподілу даних на тренувальний і тестовий вибірки, а також модуль реалізації алгоритмів виявлення аномальних транзакцій.

На початковому етапі обробки даних передбачено виконання таких процедур, як перевірка вибірки на баланс між класами, виявлення та усунення дублікатів, аналіз і обробка пропущених значень, а також масштабування (нормалізація) числових ознак.

Після завершення цього етапу підготовлені дані поділяються на тренувальну та тестову вибірки для подальшого моделювання.

Основна обчислювальна частина системи реалізує застосування моделей машинного навчання до очищених і структурованих даних. У межах даного дослідження використовуються такі алгоритми, як Random Forest, метод k-ближчих сусідів (KNN) та комбінована модель (Voting Classifier), що поєднує Random Forest і Decision Tree.

Результати класифікації та показники ефективності моделей виводяться у вигляді візуалізацій на інтерактивному дашборді для подальшого аналізу (див. рис. 2.1).

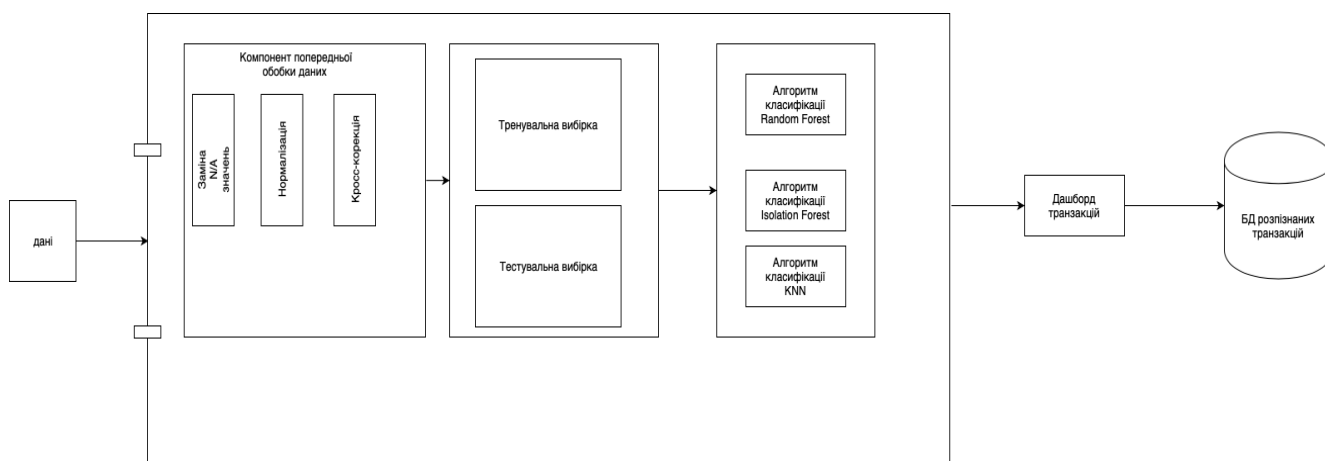


Рисунок 2.1 – Структура і характеристика СІІІ та їх компонентів

У подальших підрозділах буде детально розглянуто кожен компонент

2.1.1 Алгоритми попередньої обробки даних

Перш ніж розпочати аналіз вибірки, слід переконатися у її збалансованості та провести базову підготовку даних.

У зв'язку з тим, що початкові дані мали дисбаланс класів, а вихідні ознаки були замінені на закодовані змінні, виникла необхідність виконати нормалізацію та

обрати релевантні характеристики для подальшого опрацювання алгоритмами. З цією метою було застосовано такі методи:

Нормалізація даних

Для нормалізації буде використано метод головних компонент (Principal Component Analysis), який дає змогу зменшити розмірність вибірки без істотної втрати інформаційної цінності.

Основна ідея PCA полягає у заміні початкової k -вимірної випадкової величини на m -вимірну (де $m < k$) з мінімальним зниженням рівня інформативності. Під втратою інформації розуміється зменшення здатності лінійних комбінацій відтворювати або наближати початкові змінні.

Один із підходів передбачає побудову найточнішого передбачення вихідної величини на основі m лінійних функцій. Найкращим варіантом таких функцій буде обрано перші m головних компонент, оскільки саме вони найефективніше зберігають структуру даних.

Надамо означення терміну “головна компонента”. Припустімо, що задано k ознак: $X_1, \dots, X_k$. Першою головною компонентою буде названо Y_1 – лінійну комбінацію цих ознак, яка максимально зберігає відстані між точками у новому просторі ознак.

$$Y_1 = a_{11}X_1 + \dots + a_{k1}X_k$$

де коефіцієнти $a_{11} \dots a_{k1}$, обирає, щоб дисперсія $D(Y_1) = \lambda_1$ була максимальною

Це узгоджується з тим, що за першою головною компонентою індивіди повинні виявлятися з максимально можливою відмінністю. Друга головна компонента також є лінійною комбінацією початкових ознак:

$$Y_2 = a_{12}X_1 + \dots + a_{k2}X_k$$

Коефіцієнти $a_{11} \dots a_{k1}$, буде обрано так, щоб забезпечити некорельованість між Y_1 та Y_2 , а також максимально можливу дисперсію $D(Y_2) = \lambda_2$ серед усіх можливих лінійних комбінацій, що не мають кореляції з Y_1 . Це означає, що

компонента Y_2 повинна містити найбільший обсяг нової інформації, не пов'язаної з попередньою компонентою.

У подальшому інші головні компоненти формуються за аналогічною логікою. Загальна формула має вигляд [23]:

$$Y_j = \sum_{i=1}^k a_{ij} X_i, \quad j = 1 \dots k$$

Алгоритм дії методу головних компонент представлено на рис. 2.2:

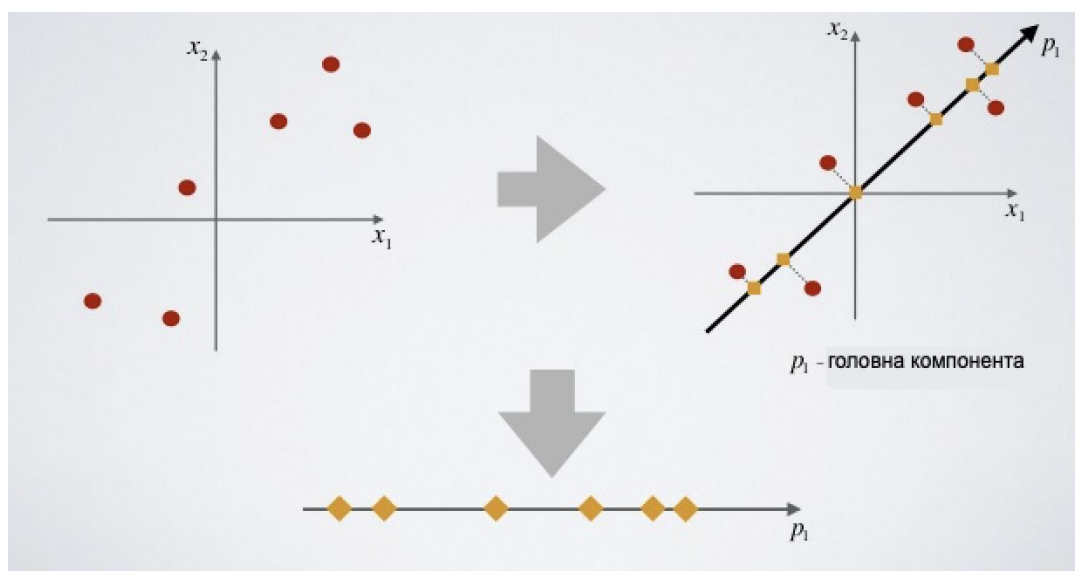


Рисунок 2.2 – Метод головних компонент

Кореляція Пірсона

Коефіцієнти кореляції за Пірсоном дають змогу оцінити наявність лінійного зв'язку між двома змінними. Побудова відповідної кореляційної матриці дозволяє виявити, наскільки сильно пов'язані між собою окремі характеристики у вибірці (див. рис. 2.3).

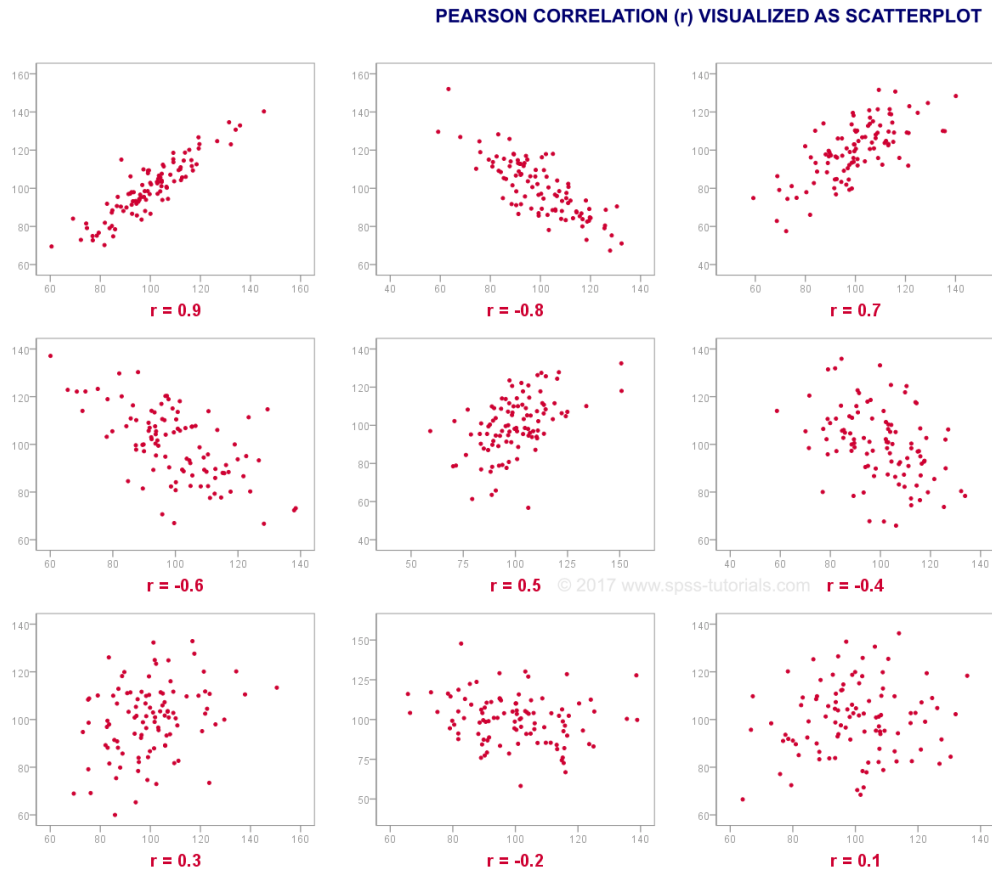


Рисунок 2.3 – Кореляція за Пірсоном на прикладі

Припустимо, що маємо дві вибірки: вибірки $x^m = (x_1, \dots, x_m)$ та $y^m = (y_1, \dots, y_m)$,

Коефіцієнт кореляції за Пірсоном між цими наборами значень буде обчислено за такою формулою:

$$r_{xy} = \frac{\sum_{i=1}^m (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^m (x_i - \bar{x})^2 \sum_{i=1}^m (y_i - \bar{y})^2}} = \frac{cov(x, y)}{\sqrt{s_x^2 s_y^2}},$$

Де:

$\bar{x}, \bar{y}$ – вибіркове середнє x^m та y^m ,

$s_x^2 s_y^2$ – вибіркова дисперсії

$$r_{xy} \in [-1,1]$$

Також коефіцієнт кореляції Пірсона можуть назвати щільність лінійного зв'язку:

$$|r_{xy}| = 1 \Rightarrow x, y \text{ лінійно залежні,}$$

$$r_{xy} = 0 \Rightarrow x, y \text{ лінійно незалежні [32]}$$

2.1.2 Алгоритм KNN

Алгоритм KNN належить до методів розв'язання задач класифікації. Припустімо, що маємо m спостережень, кожне з яких асоційоване з певним класом. Завдання полягає у визначенні класової приналежності нового спостереження на основі вже наявних даних.

Перед тим як перейти до класифікації, зобразимо наявні дані у візуальній формі (див. рис. 2.4).

0. відображення даних

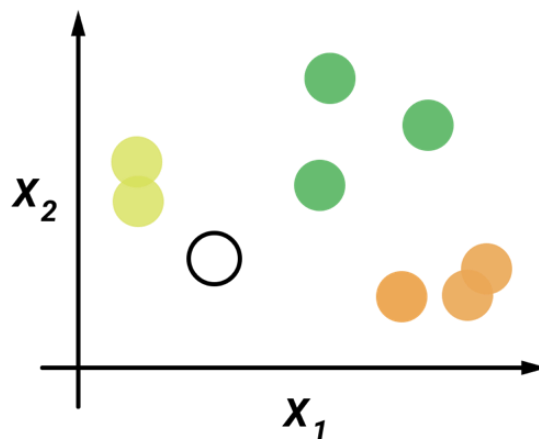


Рисунок 2.4 – Візуалізація даних

Початковим етапом роботи алгоритму є вибір значення k – кількості найближчих сусідів, які враховуватимуться при класифікації. Варто зазначити, що має бути дотримано умову: $k > 1$. Далі виконується пошук тих k спостережень, які

знаходяться на найменшій відстані від вектора ознак нового об'єкта (тобто найближчих сусідів).

Функція, яка використовується для обчислення цієї відстані, повинна відповідати таким критеріям:

$$d(x, y) \geq 0, d(x, y) = 0 \text{ тоді і тільки тоді, коли } x = y$$

$$d(x, y) = d(y, x)$$

$$d(x, z) \leq d(x, y) = d(y, z), \text{ за умови що точки } x, y, z \text{ лежать на одній прямій.}$$

Для порівняння використовується вектор x, y, z ознак кожного об'єкта. У випадку, коли значення ознак є впорядкованими, для оцінки відстані між об'єктами буде використано евклідову метрику:

$$D_E = \sqrt{\sum_i^N (x_i - y_i)^2}$$

де n – кількість атрибутів (див.рис. 2.5 та 2.6).

1. обрахунок відстаней

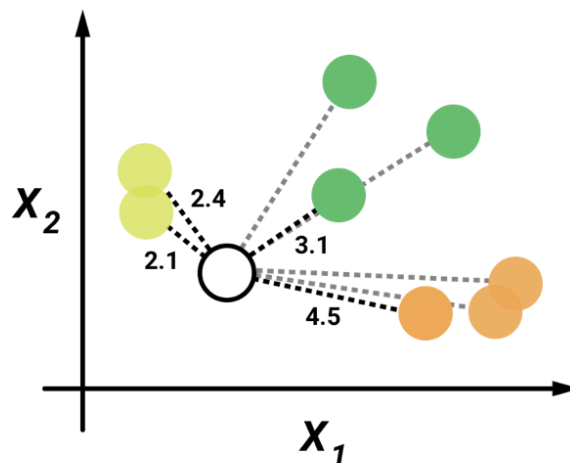


Рисунок 2.5 – Обрахунок відстаней

2. пошук сусідів

Точка		Відстань	
○	●	2.1	→ 1 сусід
○	●	2.4	→ 2 сусід
○	●	3.1	→ 3 сусід
○	●	4.5	→ 4 сусід

Рисунок 2.6 – Пошук сусідів

На третьому етапі алгоритму здійснюється процедура голосування серед k найближчих сусідів для визначення класу нового об'єкта (див. рис. 2.7).

3. голосування

Клас	# голосів		
●	2	→	Клас ● виграє голосування
●	1		Точку ○ можна віднести до класу ●
●	1		

Рисунок 2.7 - Голосування серед k найближчих сусідів

Голосування за клас проводиться за наступною формулою

$$votes(class) = \sum_{i=1}^n \frac{1}{d^2(X, Y)}$$

де $d^2(X, Y)$ Тут під відстанню мається на увазі квадрат евклідової відстані між відомим спостереженням Y_i та новим об'єктом X .

Позначення n відповідає кількості відомих спостережень, що належать до класу, для якого виконується підрахунок голосів. Параметр `class` вказує на назву відповідного класу [34].

2.1.3 Random Forest

Розглянемо підхід випадкових лісів як один із методів виявлення аномалій. Перш ніж перейти до самого алгоритму, слід пояснити поняття “бегінг” (bagging).

Нехай маємо деякий алгоритм навчання $\mu(X)$. Побудуємо на його основі модифікований варіант $\tilde{\mu}(X)$, який працює на випадковій підвибірці $\bar{X}$, сформованій за допомогою бутстрапінгу. У такому випадку: $\mu: \tilde{\mu}(X) = \mu(X)$ У контексті нашого дослідження бутстрапінг передбачає випадкове вибирання 1 об'єктів з початкової вибірки з поверненням, що означає: деякі елементи можуть потрапити у вибірку кілька разів, тоді як інші – жодного разу.

Якщо один і той самий об'єкт включено до бутстрапінгової вибірки кілька разів, то відповідна вага цього об'єкта у функціоналі зростає – таким чином, помилки на ньому впливатимуть сильніше.

У межах бегінгу необхідно навчити певну кількість базових моделей $b_n(x)$ за допомогою алгоритму $\tilde{\mu}(X)$, після чого підсумковий результат буде побудовано як середнє значення виходів усіх базових моделей:

$$a_N(x) = \frac{1}{N} \sum_{n=1}^N b_n(x) = \frac{1}{N} \sum_{n=1}^N \tilde{\mu}(X)(x)$$

Метод випадкових лісів ґрунтується на застосуванні бегінгу до дерев рішень.

Суттєвою перевагою цього методу є зниження кореляції між окремими моделями шляхом випадковості, яку вводять на двох рівнях: у виборі об'єктів та у виборі ознак. Зокрема, кожне дерево навчається на бутстрапінговій підвибірці, а під час розбиття у кожній вершині використовується випадкова підмножина ознак.

У випадкових лісах ознаку для розбиття на кожному вузлі буде обрано з випадкової підмножини розміру m .

Для задач класифікації рекомендовано брати $m = \lfloor \sqrt{d} \rfloor$, а для задач регресії – $m = \lfloor \frac{d}{3} \rfloor$, де d – загальна кількість ознак.

Оскільки виявлення аномалій відноситься до задач класифікації, доцільно формувати дерево до такого моменту, поки в кожному листі не залишиться лише один об'єкт.

Кожне дерево в складі випадкового лісу навчається на власній бутстрапінговій підвибірці. Ті об'єкти, які не були включені до підмножини X_n , слугують для цього дерева тестовими (out-of-bag).

Це дозволяє для кожного об'єкта x_i знайти ті дерева, які не використовували його під час навчання, і на основі їхніх прогнозів обчислити out-of-bag-помилку за наступною формулою:

$$OOB = \sum_{i=1}^l L \left(y_i, \frac{1}{\sum_{n=1}^N [x_i \notin X_n]} \sum_{n=1}^N [x_i \notin X_n] b_n(x_i) \right)$$

де $L(y,z)$ – функція втрат.

Із ростом кількості дерев N ця оцінка наближається до leave-one-out-перевірки, але водночас значно легша у реалізації та обчисленні [35].

2.1.6 Метрики оцінки точності

У проаналізованій літературі модель CatBoost, попри її високий потенціал, майже не згадується як інструмент для виявлення шахрайства. Це можна пояснити її відносною новизною – бібліотека була представлена публічно лише у 2017 році. Проте саме ця модель є однією з найперспективніших для вирішення подібних задач, оскільки:

- поєднує високу точність та стабільність на малих і середніх вибірках;
- підтримує роботу з необробленими категоріальними ознаками без втрати інформації;
- застосовує механізм "ordered boosting", який мінімізує переобучення;
- має ефективну реалізацію з точки зору обчислювальної складності.

У цьому дослідженні було вирішено протестувати CatBoost як основну модель побудови системи ідентифікації шахрайських транзакцій. Це дозволило оцінити її ефективність у порівнянні з класичними підходами та розширити спектр інструментів, які потенційно можуть застосовуватись у реальному комерційному середовищі.

2.1.5 Метрики оцінки точності

Робоча характеристика приймача (ROC-крива) є поширеним інструментом для візуалізації результатів у задачах бінарної класифікації в машинному навчанні. Водночас, при роботі з вибірками, де класи представлені нерівномірно, криві Precision-Recall (PR) надають точніше уявлення про ефективність моделі.

Дослідження показують, що між просторами ROC та PR існує глибока відповідність: крива буде домінувати у ROC-просторі тоді й лише тоді, коли вона домінує у PR-просторі [36].

Оскільки ассигасу (точність класифікації) є неінформативною при суттєвому дисбалансі класів, варто зосередити увагу на інших метриках, які дають більш об'єктивну оцінку якості моделі:

Матриця помилок (confusion matrix) – таблиця, що узагальнює кількість правильних передбачень та типи допущених помилок.

Precision (точність) – відношення кількості істинно позитивних передбачень до загальної кількості позитивних прогнозів. Цей показник також відомий як позитивна прогностична значущість. Низький рівень precision свідчить про велику кількість хибнопозитивних результатів.

Recall (повнота) – частка істинно позитивних об'єктів, які були правильно ідентифіковані. Інші назви цієї метрики – чутливість або істинна позитивна частота. Якщо recall низький – це означає, що багато позитивних випадків модель пропускає.

F1-міра – гармонійне середнє між precision та recall, яке забезпечує збалансовану оцінку у випадках, коли важливі обидва аспекти.

Припустімо, що задано вибірку, яка містить об'єкти двох класів, і є алгоритм, який призначає кожному з них класову належність.

У такому випадку матрицю помилок можна подати у вигляді, наведеному на рис. 2.8.

	$y = 1$	$y = 0$
$\hat{y} = 1$	True Positive (TP)	False Positive (FP)
$\hat{y} = 0$	False Negative (FN)	True Negative (TN)

Рисунок 2.8– Confusion matrix

На рис. 2.8, $\hat{y}$, відображає результат роботи алгоритму на вибірці а y – вже наявну інформацію щодо того, до якого класу належить кожен об'єкт. Таким чином, можна виокремити основні типи помилок, які виникають під час класифікації:

False Negative – об’єкт позитивного класу помилково віднесено до негативного

False Positive – об’єкт негативного класу помилково класифіковано як позитивний

Ще однією ключовою метрикою, що використовується для оцінювання якості класифікації, є асигасу – частка коректно класифікованих об’єктів. Її можна обчислити за наступною формулою:

$$accuracy = \frac{1}{l} \sum_{i=1}^l [a(x_i) = y_i]$$

$$accuracy = \frac{TP + TN}{TP + FN + FP + TN}$$

Зазначена метрика вважається одним із найелементарніших підходів до оцінювання ефективності класифікаційного алгоритму [37].

Для обчислення метрик точності та повноти використовуємо наступні формули:

$$precision = \frac{TP}{TP + FP}$$

Точність відображає, який відсоток об’єктів, віднесених класифікатором до позитивного класу, насправді є такими.

$$recall = \frac{TP}{TP + FN}$$

Повнота, своєю чергою, показує, яка частка усіх дійсно позитивних об’єктів була правильно ідентифікована як позитивна.

Варто мати на увазі, що у випадку, якщо $a(x) = [p(x) > t]$, то зі зростанням порогу t (де t – це обраний поріг класифікації) спостерігається підвищення точності, водночас повнота буде знижуватись.

Слід підкреслити, що ні точність, ні повнота не залежать від співвідношення кількості об'єктів у кожному з класів. Навіть якщо позитивний клас представлений значно меншою кількістю прикладів порівняно з негативним, ці метрики залишаються коректними індикаторами якості класифікації.

Для узагальнення оцінки на основі обох показників існує кілька підходів. Одним із найбільш поширених є F-міра, яка розраховується як гармонійне середнє між точністю та повнотою. Її формула має вигляд

$$F = \frac{2 \cdot precision \cdot recall}{precision + recall}$$

Однією з характерних властивостей гармонійного середнього є те, що за умови, коли хоча б один із параметрів прямує до нуля, усе значення також наближається до нуля. Завдяки цьому F-міра вважається більш надійною метрикою порівняно з арифметичним середнім, особливо у випадках нерівномірного балансу між точністю та повнотою.

Ще одним важливим показником для оцінки ефективності класифікатора є площа під ROC-кривою (AUC-ROC, Area Under ROC Curve).

Розглянемо двовимірний простір, де одна координата відповідає частці хибнопозитивних передбачень (False Positive Rate, FPR), а інша – частці істинно позитивних передбачень (True Positive Rate, TPR):

$$FPR = \frac{FP}{FP + TN}$$

$$TPR = \frac{TP}{TP + FN}$$

Кожен вибір порогу t відповідає точці в даному просторі. Існує $l+1$ таких порогів. Максимальний поріг $t_{max} = \max_i b(x_i)$ дає класифікатор з $TPR = 0$, $FPR = 0$. Мінімальний поріг $t_{min} = \min_i b(x_i) - \varepsilon$ дасть $TPR = 1$, $FPR = 1$.

ROC-крива – це крива з кінцями в точках $(0,0)$ и $(1, 1)$, яка послідовно з'єднує точки, що відповідають порогам $b(x_{(1)}) - \varepsilon, b(x_{(1)}), b(x_{(2)}), \dots, b(x_{(l)})$.

Площа під даною кривою називається AUC-ROC, і приймає значення від 0 до 1. Якщо поріг t може бути підібраний так, що алгоритм $a(x)$ не допускати помилок, то AUC-ROC буде дорівнює одиниці; якщо ж $b(x)$ ранжирує об'єкти випадковим чином, то AUC-ROC буде близький до 0.5. [37]

Площа, обмежена ROC-кривою, називається AUC-ROC і може набувати значень у діапазоні від 0 до 1. У випадку, коли існує такий поріг t , за якого алгоритм $a(x)$ класифікує об'єкти без жодної помилки, значення AUC-ROC дорівнює 1. Натомість, якщо функція $b(x)$ визначає ранжування об'єктів у довільному порядку (без врахування реальної належності до класів), тоді AUC-ROC наближатиметься до 0.5 [38].

2.3 Методи, моделі і моделювання систем виявлення ризиків онлайн-оплат

2.3.1 Методи побудови та синтезу компонент систем виявлення шахрайства

Як основний метод дослідження застосовано технології машинного навчання, що дозволяють виявляти приховані структури в даних про транзакції. Запропонований підхід охоплює два ключові напрями: глибоку аналітику даних та формування обчислювального ядра, здатного до виявлення нетипових шаблонів поведінки.

Структура дослідження: багаторівнева методологія Запропонована дослідницька модель базується на поетапному підході, в межах якого кожен рівень аналізу послідовно вдосконалює механізми виявлення шахрайських транзакцій.

1. Формування вибірки та її попередня обробка. Перший крок полягає у збиранні базових вхідних даних, що містять інформацію про фінансові операції – такі як суми переказів, часові мітки, геолокація транзакцій та профілі користувачів.

Цей етап передбачає детальне очищення, заповнення пропусків і приведення інформації до єдиного формату. Можна уявити це як ретельну підготовку необробленої сировини перед подальшою аналітикою – процес, від якого залежить якість усієї системи.

2. Побудова характеристик (інженерія ознак). Сирі дані не мають практичної цінності без глибшого перетворення. На цьому етапі застосовується доменна експертиза для створення нових ознак – аналітично значущих змінних, отриманих із наявних даних. Наприклад, обчислюються середні витрати користувача, виявляються різкі коливання у поведінці або географічні аномалії. Ці характеристики стають основою для виявлення потенційно шахрайських транзакцій.

3. Вибір моделей і процес навчання. Наступним кроком є визначення найпридатніших алгоритмів машинного навчання. Розглядаються різні варіанти, кожен з яких має певні переваги й обмеження. Після вибору здійснюється навчання моделей на розмічених підмножинах даних, де приклади шахрайства та звичайної поведінки дозволяють алгоритму сформулювати правила виявлення підозрілих операцій. Цей етап можна умовно порівняти з підготовкою аналітика, який вивчає характерні ознаки злочину.

4. Оцінка якості та вдосконалення моделей. Жодна модель не є ідеальною з першого разу. Після навчання системи тестуються на окремих даних, не залучених під час тренування. Аналізуються ключові метрики – точність, повнота, рівень хибнопозитивних спрацювань. Моделі налаштовуються, гіперпараметри коригуються, помилки аналізуються – з метою досягнення максимальної ефективності в реальних умовах.

Таким чином, система підтримує високий рівень чутливості до нетипової активності навіть у динамічному середовищі.

2.3.2 Моделі та методи оптимізації систем ідентифікації шахрайських транзакцій

Оптимізація процесу виявлення шахрайства реалізується шляхом налаштування гіперпараметрів моделей (кількість дерев у Random Forest, значення k у KNN, розмірність ознакового простору). Застосовуються методи бутстрапінгу, крос-валідації, grid search та random search для підбору оптимальних параметрів.

Технічне вдосконалення системи можливо завдяки впровадженню хмарних рішень, зокрема інфраструктури на базі Amazon Web Services (AWS) (див. рис. 2.9). Архітектура такої системи передбачає кілька взаємопов'язаних етапів:

- Сховище даних DynamoDB виявляє оновлення та спрямовує їх у відповідний стрім для подальшої обробки.
- Ключовий компонент – AWS Glue – періодично отримує дані з вказаної таблиці у DynamoDB. Ці дані використовуються для запуску процедури навчання моделі на платформі Amazon SageMaker, а отримані результати зберігаються в Amazon S3 у вигляді модельних артефактів.
- Інша задача AWS Glue полягає в автоматичному розгортанні оновленої моделі на передбаченій кінцевій точці SageMaker, де вона застосовується для детекції аномальних патернів у режимі online, наприклад, із використанням алгоритму Random Forest.
- Механізм AWS Lambda взаємодіє з потоком подій із DynamoDB і ініціює звернення до моделі, отримуючи висновки у вигляді класифікаційних результатів.

- У разі виявлення підозрілих транзакцій, Lambda автоматично надсилає відповідні сигнали у клієнтські застосунки або інші частини системи для негайного реагування [40].

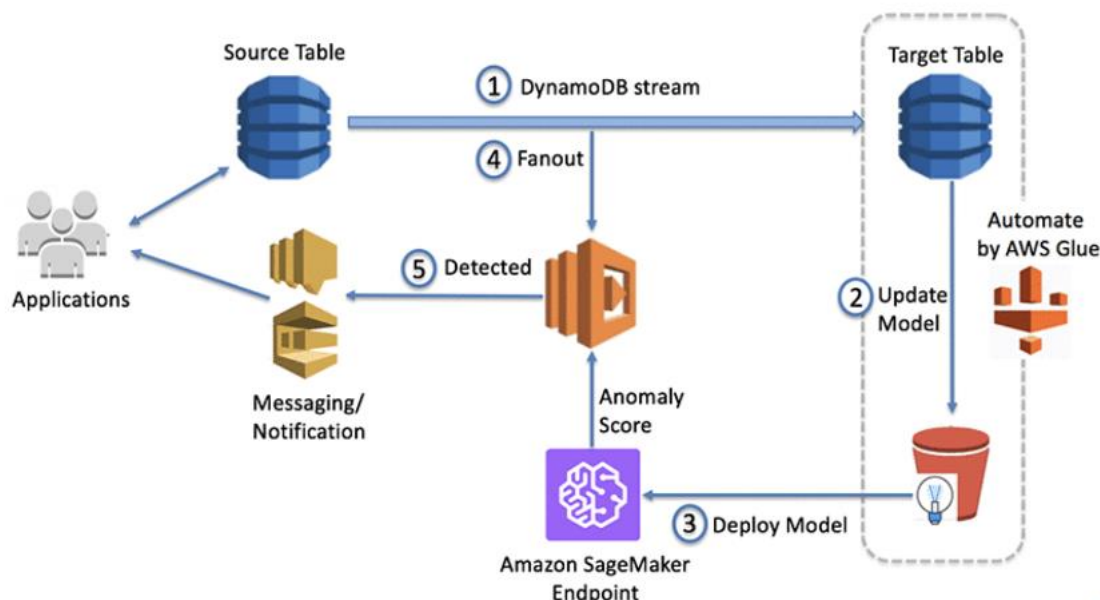


Рисунок 2.9 – Архітектурна схема хмарного рішення для виявлення нетипової активності

Здатність системи до масштабування забезпечує оперативніше виявлення підозрілих фінансових операцій, що, своєю чергою, дозволяє мінімізувати фінансові ризики для комерційних структур.

2.3.3 Методи та моделі управління поведінкою систем виявлення онлайн-шахрайства

У цьому контексті під управлінням мається на увазі здатність системи адаптивно реагувати на нові типи транзакцій та швидко перебудовувати внутрішні правила аналізу в умовах змінного середовища. У рамках проєкту реалізовано підхід до безперервного донавчання моделей на основі актуальних потоків даних (online learning), з подальшою інтеграцією в реальне середовище.

Для забезпечення автоматизації процесів було впроваджено практику MLOps (Machine Learning Operations) – щоденне оновлення прогнозних моделей здійснюється за допомогою планувальника наприклад Prefect

Після розгортання моделі проводиться А/В тестування для оцінки ефективності практичного використання прогнозу. В рамках експерименту контрольна група обробляється без використання Fraud rate, тоді як у тестовій групі модель активно застосовується для виявлення підозрілих транзакцій. При ідентифікації високого ризику у тестовій групі ініціюється автоматичне повернення коштів (refund). Після завершення експерименту порівнюється рівень шахрайських операцій між групами. Це дозволяє оцінити не лише точність передбачення, але й фактичну результативність впровадження прогнозної моделі у бізнес-процеси.

Висновки до розділу 2

У другому розділі було детально охарактеризовано об'єкт дослідження – систему штучного інтелекту для виявлення ризиків в онлайн-оплатах – та описано архітектуру її побудови. Особливу увагу приділено підходам до попередньої обробки даних, включаючи методи нормалізації, вибір релевантних ознак і балансування вибірки. Розглянуто ключові алгоритми класифікації, зокрема Random Forest , CatBoost та KNN, а також метрики оцінки їх ефективності (Precision, Recall, F1, AUC), що дозволяють адекватно вимірювати якість в умовах дисбалансованих класів.

Окрему увагу приділено методам моделювання систем виявлення шахрайства, побудові ознак, синтезу моделей і підходам до оптимізації (включаючи крос-валідацію та Grid Search). Такий комплексний підхід дозволяє сформувати гнучку систему з високою здатністю до виявлення шахрайських операцій у режимі, близькому до реального часу.

РОЗДІЛ 3. РОЗРОБЛЕННЯ ПРОЕКТНИХ РІШЕНЬ

3.1 Опис бази для системи оцінки ризику транзакцій в онлайн-платежах

У рамках цього дослідження джерелом інформації слугували дані про транзакційну активність з вебплатформи Dating-Lift. Підключення до відповідного сховища даних здійснювалося через аналітичну систему Vertica, доступ до якої було отримано в межах проходження виробничої практики (див. рис. 3.1)..

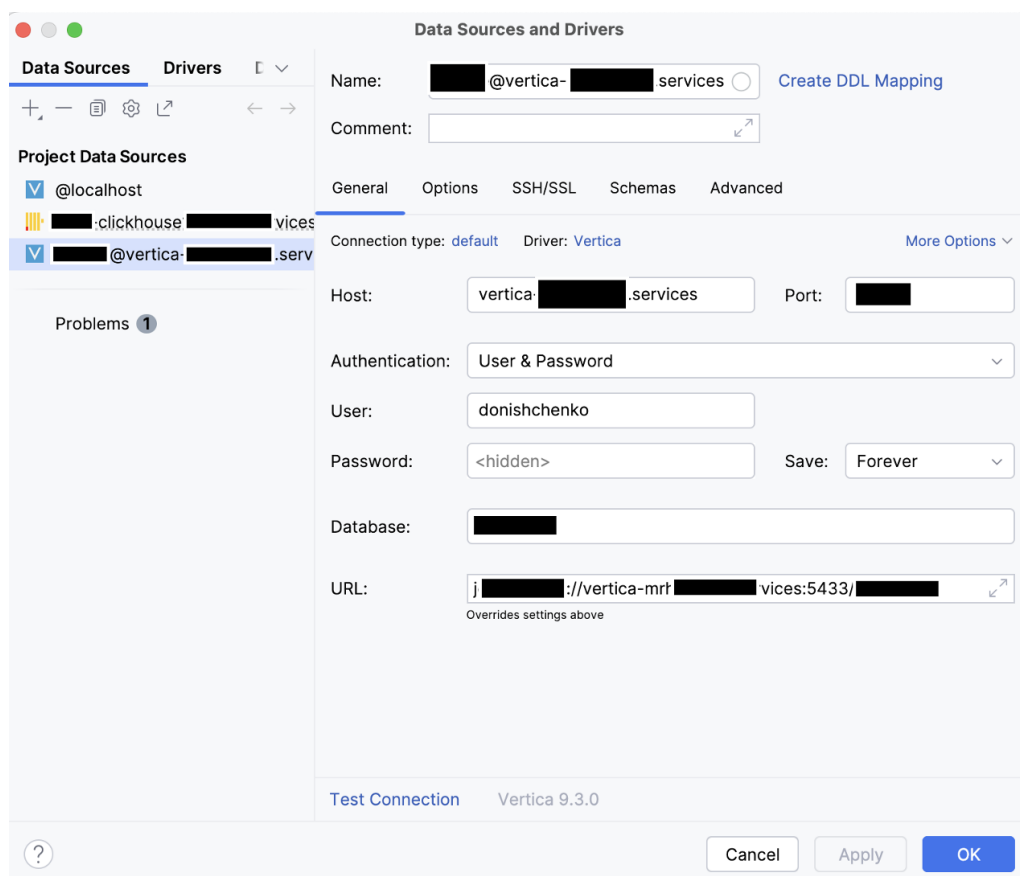


Рисунок 3.1 – Підключення до бази даних Vertica (конфіденційні дані були скриті).

Важливо зазначити, що база даних уже містила попередньо налаштований механізм виявлення підозрілих транзакцій, сформований на основі сигналів від

платіжного провайдера Solidgate. Саме цей постачальник фінансових сервісів забезпечує інструменти для передачі випадків шахрайства (див. рис. 3.2).

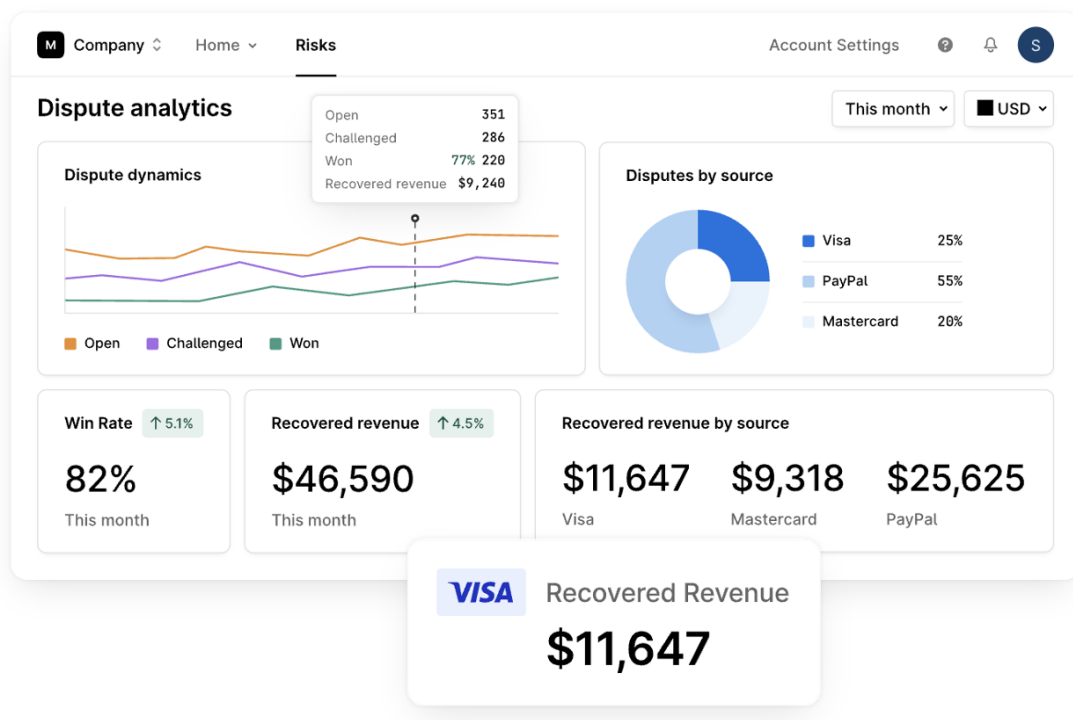


Рисунок 3.2 – Приклад адмін-панелі клієнта Solidgate

Для побудови моделей інтелектуального аналізу було використано історичну сукупність даних, яка охоплює останні 12 місяців активності вебресурсу. Загальний обсяг вибірки становить 267 300 транзакцій, серед яких 523 відмічені як нетипові або шахрайські (див. рис. 3.1).

Первинна структура даних включає винятково числові параметри, що були сформовані в результаті застосування методу зниження розмірності – методу головних компонент (РСА). Через обмеження, пов'язані з конфіденційністю, вихідні характеристики було замінено на узагальнені маркери типу F1, F2, ..., F30, які є ортогональними латентними ознаками. Крім того, в датасеті збережено дві незмінні змінні: "Timestamp" – час у секундах відносно першої транзакції в наборі, та "TransactionValue" – сума відповідної операції.

Класова належність транзакції закодована у полі "Label": значення 1 означає, що операцію було ідентифіковано як шахрайську, а 0 – як нормальну.

Для об'єктивної оцінки продуктивності алгоритмів машинного навчання, всю сукупність було розділено на тренувальну та валідаційну частини в співвідношенні 70% до 30%. Такий підхід дозволяє запобігти перенавчанню моделей і забезпечує адекватну перевірку їх здатності до узагальнення на нових даних.

3.2 Реалізація програмного компоненту

З метою реалізації СШІ ідентифікації ризиків онлайн-оплат за допомогою алгоритмів машинного навчання було обрано мову програмування Python, яка на сьогоднішній день посідає провідні позиції у сфері аналізу даних, машинного навчання та штучного інтелекту. Її універсальність, активна спільнота користувачів та велика кількість спеціалізованих бібліотек роблять Python оптимальним вибором для розв'язання задач прикладної аналітики.

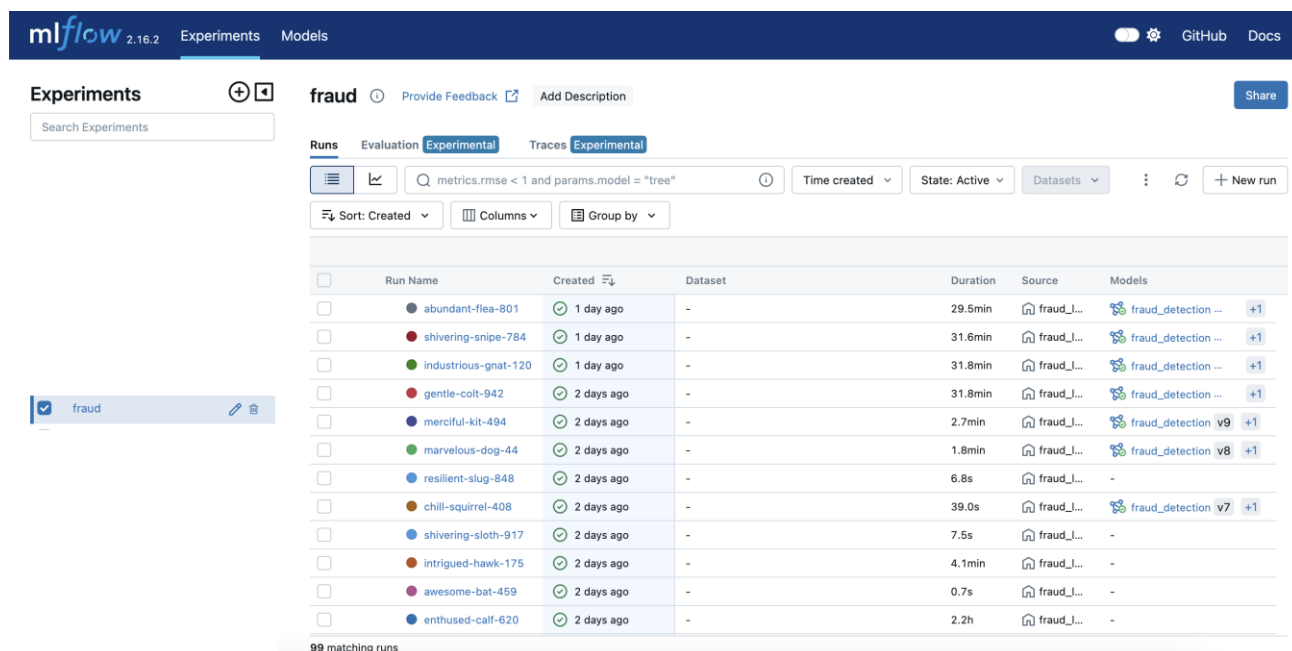
У межах реалізації прототипу системи для виявлення аномальних транзакцій було використано два взаємодоповнювальні інструменти: JupyterLab – як інтерактивне середовище розробки, та MLflow – як платформа для моніторингу, керування та документування експериментів у сфері машинного навчання.

JupyterLab забезпечив зручний інтерфейс для проведення аналітичної роботи, що охоплювала попередню обробку даних, побудову візуалізацій, розробку моделей та оцінювання їхньої якості. Серед основних переваг цього середовища варто виокремити:

- підтримку графічного представлення результатів з використанням популярних бібліотек (Matplotlib, Seaborn, Plotly);
- зручну взаємодію з кодом завдяки cell-орієнтованій структурі;
- можливість документування процесу аналізу за допомогою Markdown;
- інтеграцію з базами даних, зокрема з Vertica, яка використовувалася у межах даного дослідження.

MLflow, у свою чергу, було застосовано для організації повного циклу управління машинним навчанням. Платформа дозволила фіксувати параметри експериментів, зберігати артефакти, реєструвати версії моделей та контролювати

їх еволюцію. На рис. 3.3 показано приклад збереження тренуваних моделей у межах цієї роботи.



The screenshot shows the MLflow Experiments interface for an experiment named 'fraud'. The interface includes a search bar, filters, and a table of runs. The table has columns for Run Name, Created, Dataset, Duration, Source, and Models. The runs are listed in descending order of creation time.

Run Name	Created	Dataset	Duration	Source	Models
abundant-flea-801	1 day ago	-	29.5min	fraud_1...	fraud_detection ... +1
shivering-snipe-784	1 day ago	-	31.6min	fraud_1...	fraud_detection ... +1
industrious-gnat-120	1 day ago	-	31.8min	fraud_1...	fraud_detection ... +1
gentle-colt-942	2 days ago	-	31.8min	fraud_1...	fraud_detection ... +1
merciful-kit-494	2 days ago	-	2.7min	fraud_1...	fraud_detection v9 +1
marvelous-dog-44	2 days ago	-	1.8min	fraud_1...	fraud_detection v8 +1
resilient-slug-848	2 days ago	-	6.8s	fraud_1...	-
chill-squirrel-408	2 days ago	-	39.0s	fraud_1...	fraud_detection v7 +1
shivering-sloth-917	2 days ago	-	7.5s	fraud_1...	-
intrigued-hawk-175	2 days ago	-	4.1min	fraud_1...	-
awesome-bat-459	2 days ago	-	0.7s	fraud_1...	-
enthused-calf-620	2 days ago	-	2.2h	fraud_1...	-

99 matching runs

Рисунок 3.3 – Інтерфейс MLflow із прикладом збереження результатів тренування моделей

До основних переваг MLflow належать:

- автоматичне відстеження запущених експериментів із збереженням усіх відповідних метрик;
- централізований реєстр моделей, що спрощує їх версіонування та розгортання;
- гнучкість у збереженні результатів (ваги, графіки, журнали роботи тощо);
- підтримка широкого спектра фреймворків, серед яких scikit-learn, TensorFlow тощо.

Таким чином, JupyterLab виступав як зручний інструмент для реалізації обчислювальної логіки та візуального аналізу, тоді як MLflow забезпечував структуроване збереження результатів, контроль версій і повторюваність експериментів. Спільне використання цих двох середовищ дозволило сформувати повноцінний і прозорий процес побудови системи виявлення аномалій.

Для реалізації процесу моніторингу транзакцій у режимі, наближеному до реального часу, у рамках даного дослідження було використано інструмент Prefect. Ця платформа призначена для створення, планування та керування дата-пайплайнами з високим ступенем надійності та гнучкою логікою виконання.

Prefect є сучасною оркестраційною системою, яка дозволяє автоматизувати та масштабувати ETL-процеси, а також керувати залежностями між задачами. На відміну від традиційних засобів, таких як cron або Airflow, Prefect пропонує декларативний підхід до опису робочих потоків, дозволяє легко обробляти помилки, а також має інтуїтивно зрозумілий інтерфейс для моніторингу статусу виконання.

У контексті даного проєкту Prefect використовується для організації автоматичного виконання пайплайну з виявлення потенційно шахрайських транзакцій. Цей процес передбачає щоденне оновлення моделі, яка отримує на вхід нові дані з бази Vertica, проводить попередню обробку, застосовує попередньо натреновану модель, після чого фіксує результати та надсилає сповіщення про ризикові випадки.

Запуск цього пайплайну налаштовано з періодичністю раз на 24 години, що дозволяє ефективно реагувати на нові аномальні активності з мінімальною затримкою, зберігаючи при цьому стабільне навантаження на систему. Важливо відзначити, що Prefect забезпечує гнучкий механізм повторного запуску в разі помилки, а також веде логування всіх виконаних задач.

На рис. 3.4 зображено приклад реалізації автоматизованого робочого процесу (flow) у середовищі Prefect, який відповідає за щоденне виконання моделі прогнозування ймовірності шахрайства. Видно, що запуск заплановано у визначений час, а всі етапи завдання успішно завершено. Інтерфейс також демонструє кількість виконаних підзадач, статуси запусків, а також інформацію про черги та пул ресурсів, за допомогою яких було реалізовано виконання.Птимізацію.

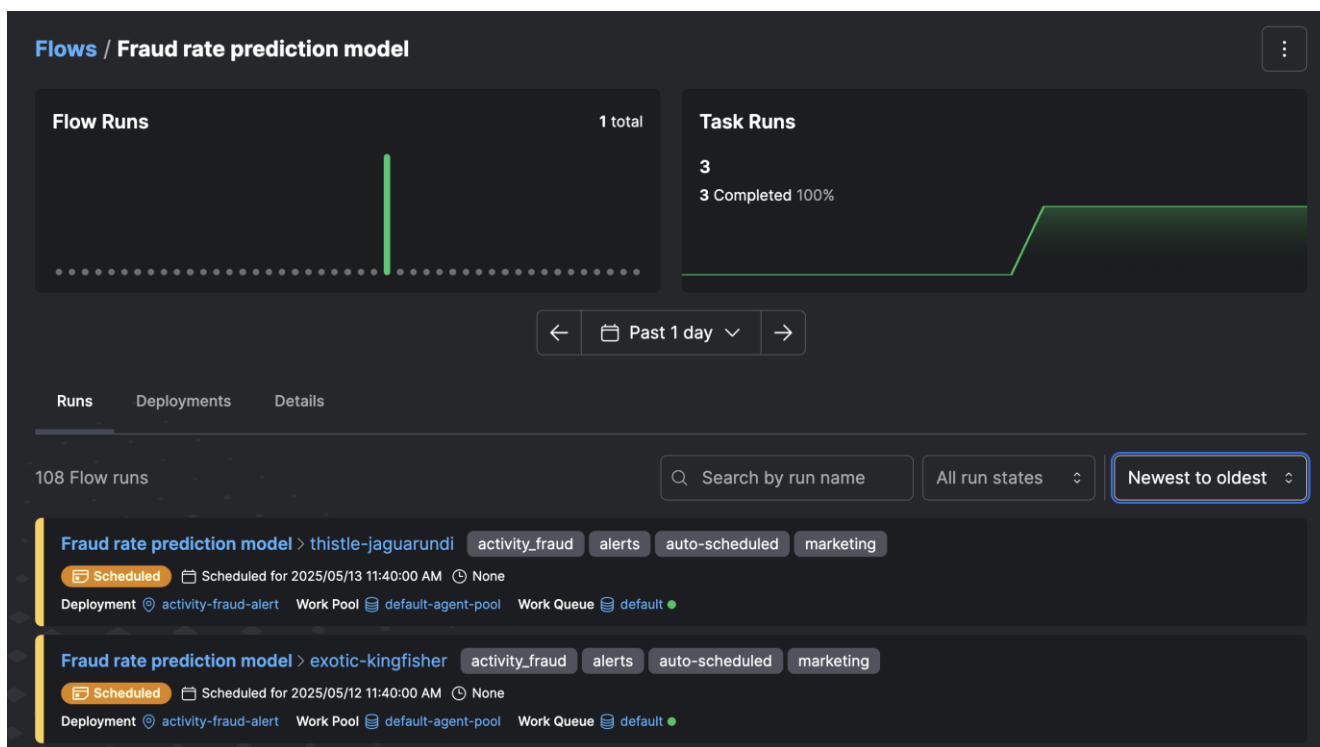


Рисунок 3.4 – Інтерфейс платформи Prefect із прикладом налаштованого пайплайну для прогнозування ризикових транзакцій

Результати роботи моделі прогнозування зберігаються у базі даних Vertica, яка виступає основним аналітичним сховищем у межах даного дослідження. Щоденні оновлення прогнозів передаються до цієї системи для централізованого зберігання та подальшого використання в аналітичних процесах.

Після інтеграції моделі було проведено А/В тестування. У межах експерименту контрольна група працювала без урахування прогнозного ризику, тоді як у тестовій групі модель активно застосовувалась для виявлення підозрілих транзакцій. Для візуалізації результатів А/В тестування було використано Tableau Online – це хмарна аналітична платформа, яка забезпечує доступ до дашбордів без встановлення програмного забезпечення. Серед основних переваг: автоматичне оновлення даних, зручна система керування доступами, можливість інтерактивного аналізу та спільної роботи, а також повна сумісність з різними джерелами даних, зокрема Vertica.

Рис.3.5 демонструє приклад дашборду в Tableau Online, на якому відображено порівняння результатів між контрольним та тестовим сегментами за підсумками A/B тесту.

card_brand		control	test
Grand Total	% Fraud rate \$	5.4%	2.8%
	% Diff Fraud rate \$		-47.14%
	VAMP	1.7%	1.4%
	% Diff VAMP		-15.64%
	\$ fraud transactions	\$677	\$389
	\$ all success transactions	\$12,629	\$13,730
VISA	% Fraud rate \$	6.0%	6.5%
	% Diff Fraud rate \$		8.03%
	VAMP	1.7%	1.4%
	% Diff VAMP		-15.64%
	\$ fraud transactions	\$421	\$386
	\$ all success transactions	\$6,973	\$5,925
MC	% Fraud rate \$	4.5%	0.0%
	% Diff Fraud rate \$		-99.32%
	VAMP		
	% Diff VAMP		
	\$ fraud transactions	\$256	\$2
	\$ all success transactions	\$5,655	\$7,805

Рисунок 3.5 – Приклад дашборду в Tableau Online

У межах дослідження було реалізовано повний цикл побудови та впровадження системи виявлення аномальних транзакцій, який охоплює всі ключові етапи – від збирання даних до візуалізації результатів.

Дані надходять до сховища Vertica, звідки автоматично обробляються за допомогою Prefect. Побудова та тестування моделі здійснюється в JupyterLab, а всі експерименти фіксуються через MLflow, який також забезпечує версіонування моделей. Після розгортання прогнозовані значення знову зберігаються у Vertica.

Для оцінки ефективності проводиться A/B тестування, результати якого візуалізуються в Tableau Online, що дозволяє оперативно порівнювати показники

між тестовою та контрольної групами. Узагальнену архітектуру системи представлено на рис. 3.6.

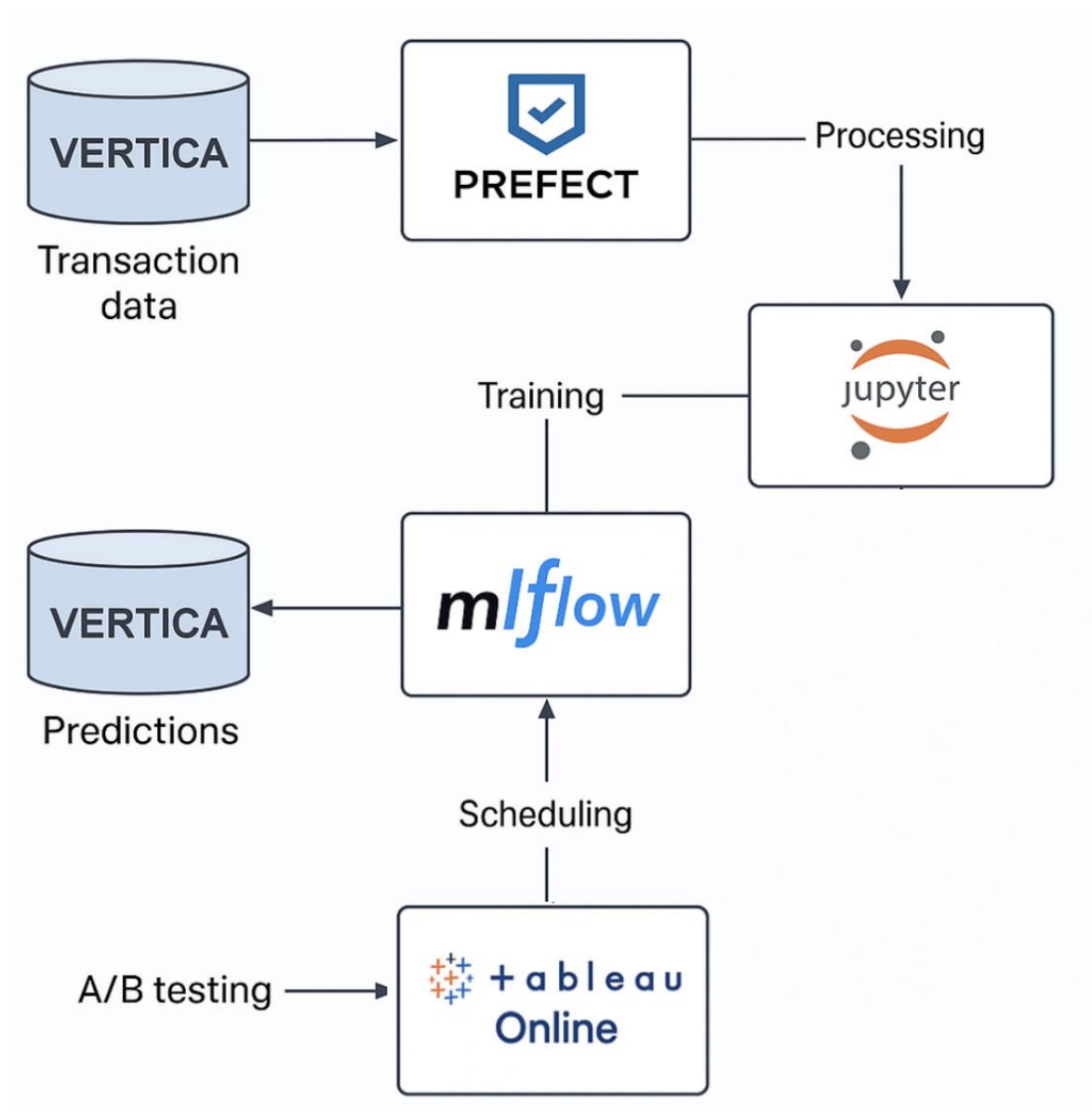


Рисунок 3.6 – Узагальнена схема взаємодії компонентів системи виявлення аномальних транзакцій

3.1 Проектування забезпечувальних підсистем СШ. Реалізація системи

3.2.1 Формування вибірки та її попередня обробка

Розглянемо окремо вплив базових параметрів, таких як час виконання операції та її тип (рис. 3.7), а також взаємозв'язок між сумою транзакції й кількістю операцій (рис. 3.8 та рис. 3.9). Аналіз демонструє наявність специфічних часових інтервалів, у межах яких спостерігається суттєве зростання частки аномальних транзакцій.

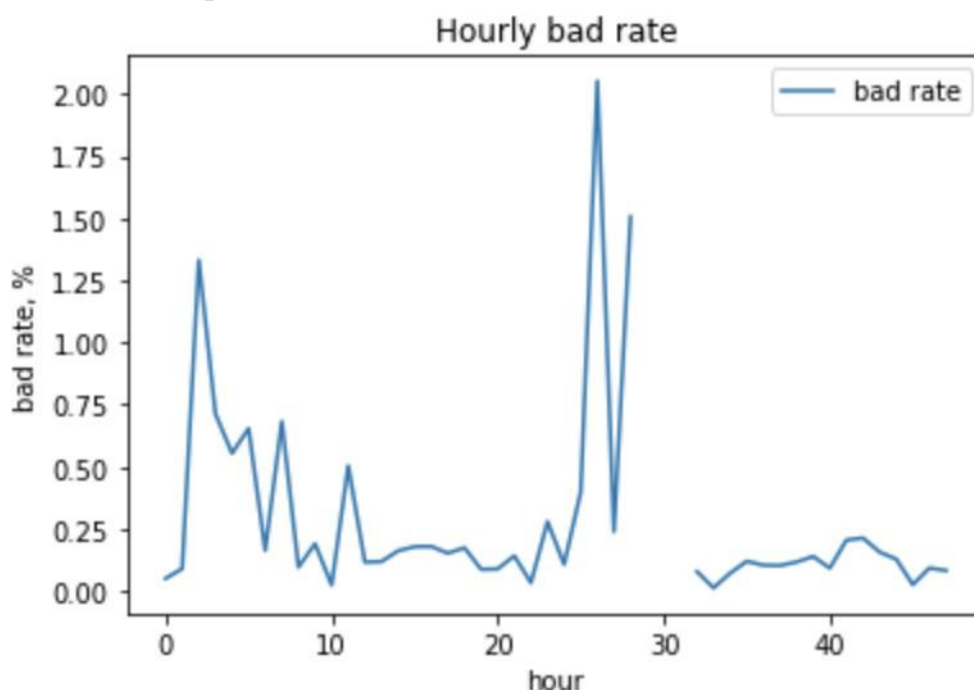


Рисунок 3.7 – Погодинний розподіл.

Як видно з рис. 3.8 та рис. 3.9 зображено характер розподілу сум транзакцій. Незважаючи на те, що шахрайські операції можуть відбуватись на різні суми, переважна їх частина здійснюється на ті ж значення, що характерні й для звичайних (нормальних) транзакцій.

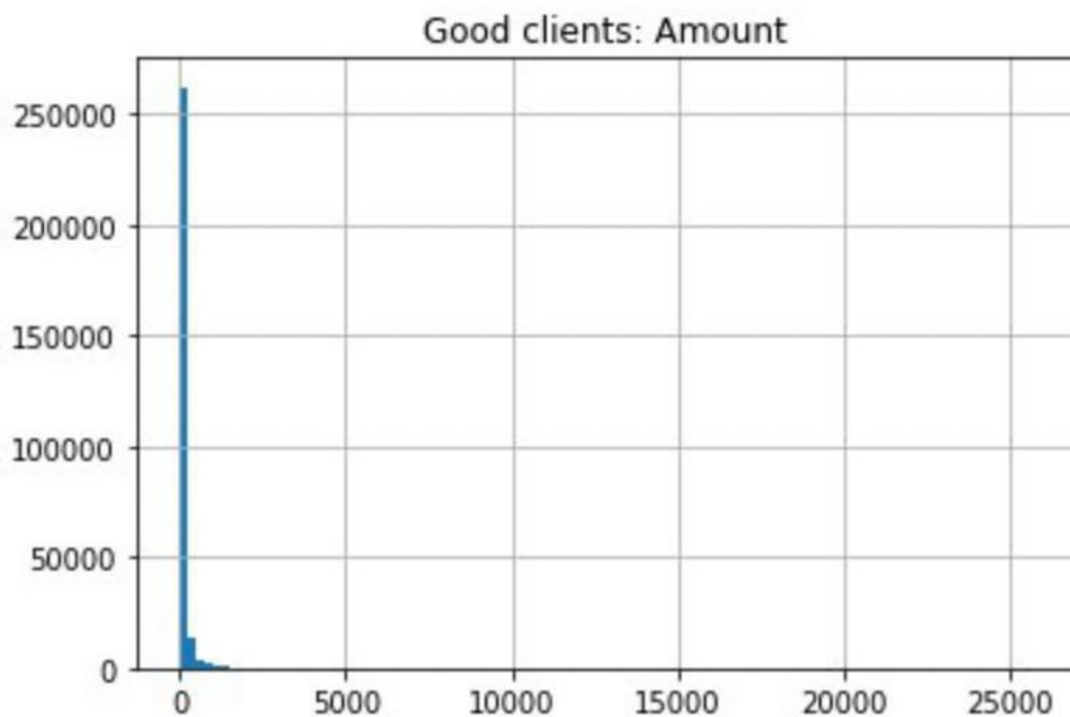


Рисунок 3.8 – Розподіл кількості транзакцій, віднесених до категорії аномальних, залежно від суми операції.

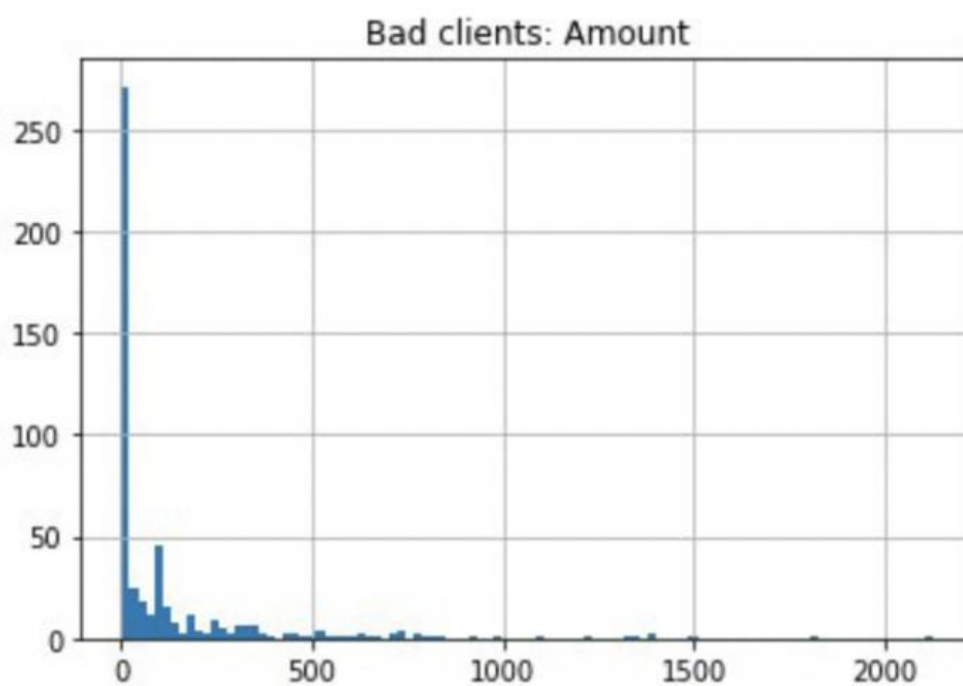


Рисунок 3.9 – Розподіл кількості транзакцій, віднесених до категорії аномальних, залежно від суми операції для нормальних транзакцій.

На початковому етапі дослідження здійснюється попередній аналіз вибірки, що дозволяє сформулювати уявлення про структуру, характеристики та загальні властивості наявних даних (див.рис. 3.10).

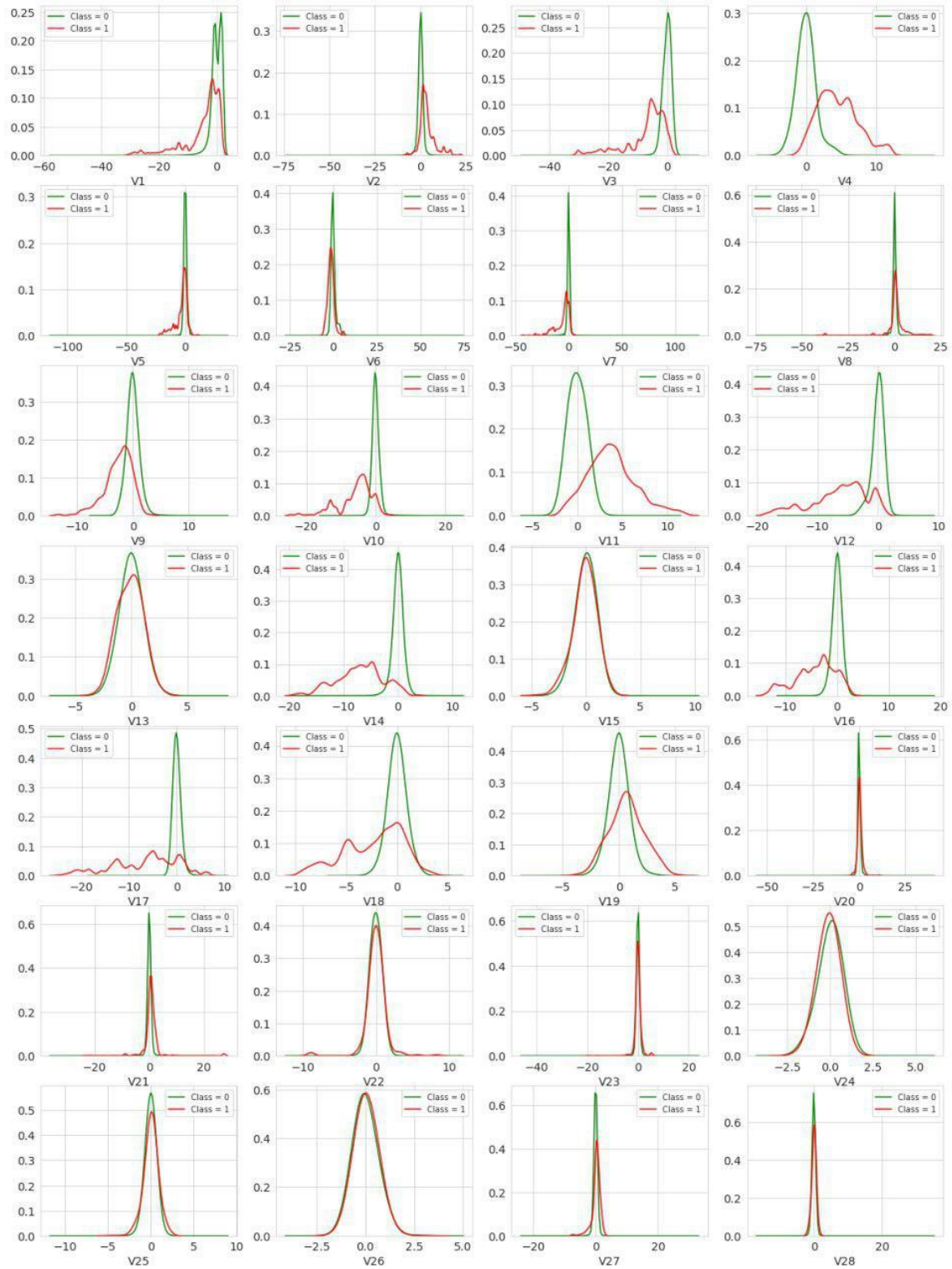


Рисунок 3.10 - Розподіл транзакцій у вибірці

На наступному етапі опрацювання даних здійснюється перевірка наявності дублікатів у вибірці. Ідентифіковані повторювані записи, що належать до категорії звичайних (неаномальних) транзакцій, підлягають видаленню. Загальна кількість таких транзакцій становить 1054 (див. рис. 3.11). Водночас дублікати, які відповідають класу шахрайських операцій, зберігаються у вибірці без змін. Це обумовлено суттєвим дисбалансом класів у початковому наборі даних, а також обмеженою кількістю прикладів аномальної поведінки.

```
In [4]: display(
        'Duplicated rows, Class values frequency:',
        transactions_df.loc[
            transactions_df.duplicated(),
            'Class'
        ].value_counts()
    )

transactions_df = transactions_df.drop_duplicates()

'Duplicated rows, Class values frequency:'

0      1062
1        19
Name: Class, dtype: int64
```

Рисунок 3.11 – Наявності дублікатів у вибірці

На подальшому етапі здійснюється нормалізація числових характеристик. Оскільки всі змінні, за винятком показника вартості операції, вже були трансформовані за допомогою методу головних компонент (РСА), постає необхідність у приведенні й цього параметра до аналогічного масштабу. З цією метою до поля "TransactionAmount" було застосовано алгоритм головних компонент, що дозволяє зменшити вплив масштабної відмінності між ознаками на подальше моделювання (див. рис. 3.12).

```
In [5]: std_scaler = StandardScaler()
normed_amount = std_scaler.fit_transform(
    transactions_df['Amount'].values.reshape(-1, 1)
)

transactions_df['Amount'] = normed_amount

In [6]: display(
    'Normalized "Amount" feature stats:',
    transactions_df['Amount'].describe()
)

'Normalized "Amount" feature stats:'

count      2.837260e+05
mean        5.504111e-15
std         1.000002e+00
min         -3.533268e-01
25%         -3.309625e-01
50%         -2.654671e-01
75%         -4.378088e-02
max         1.022476e+02
Name: Amount, dtype: float64
```

Рисунок 3.12 – Нормалізація "TransactionAmount"

Наступним кроком є перевірка взаємозв'язку між ознаками. Для цього будується матриця кореляції за коефіцієнтами Пірсона, що дозволяє виявити надмірно скорельовані змінні

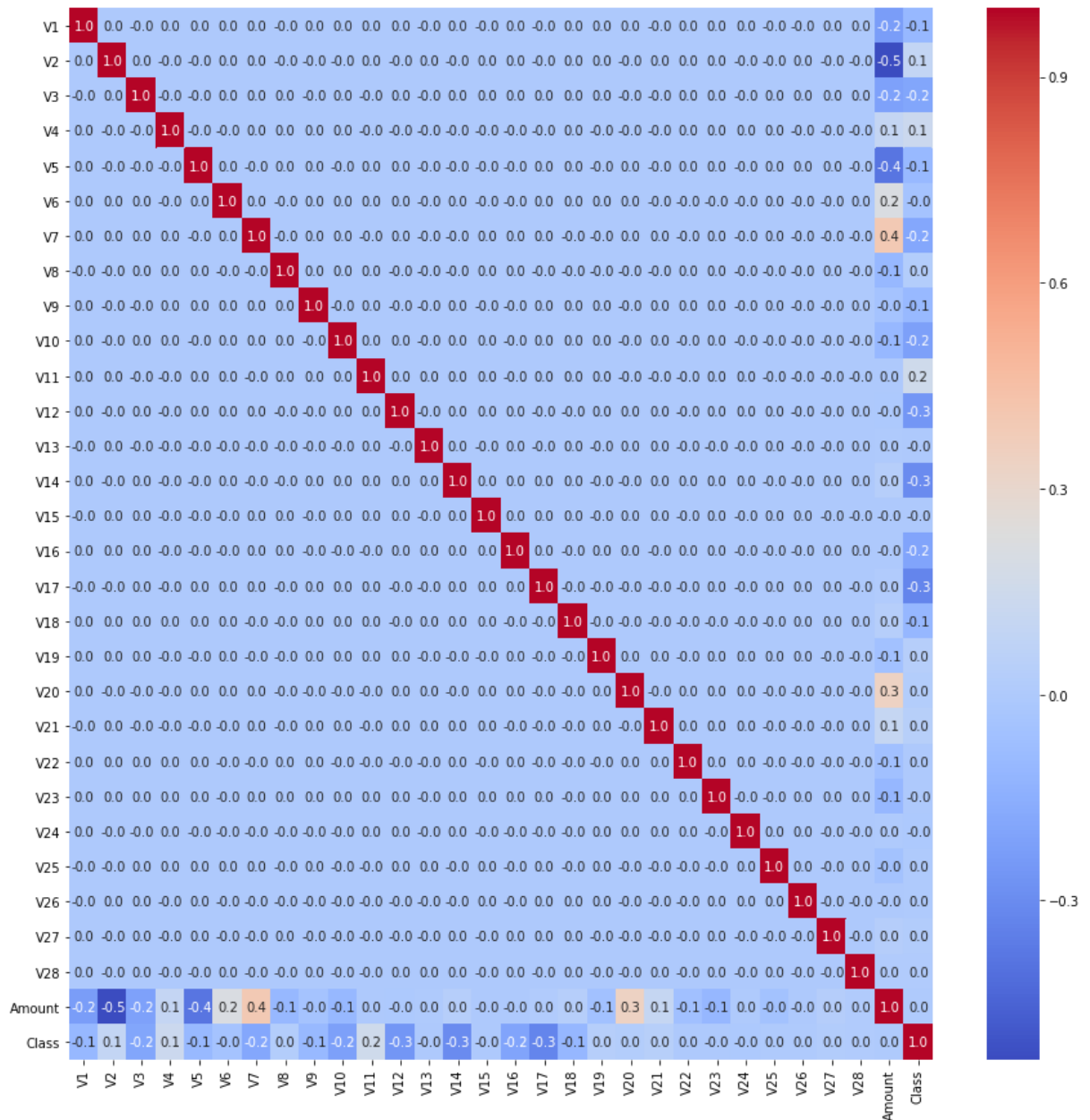


Рисунок 3.13 – Матриця кореляції за коефіцієнтами Пірсона

Як показано на рис. 3.13 спостерігається помірна кореляція окремих ознак із полями "Timestamp" та "TransactionAmount". Водночас між самими ознаками високих кореляцій не виявлено.

Далі виконується аналіз залежності кожної змінної від цільового показника (див.рис. 3.14).

```

'Correlations with target feature:'
V22      0.000805
V23      0.002685
V25      0.003308
V15      0.004223
V26      0.004455
V13      0.004570
Amount   0.005632
V24      0.007221
V28      0.009536
V27      0.017580
V8        0.019875
V20      0.020090
V19      0.034783
V21      0.040413
V6        0.043643
V2        0.091289
V5        0.094974
V9        0.097733
V1        0.101347
V18      0.111485
V4        0.133447
V11      0.154876
V7        0.187257
V3        0.192961
V16      0.196539
V10      0.216883
V12      0.260593
V14      0.302544
V17      0.326481
Class     1.000000
Name: Class, dtype: float64

```

Рисунок 3.14 – Кореляція з таргетом

Аналіз кореляції між ознаками та цільовим значенням показав, що найбільш інформативними є змінні F17, F14, F12, F10, F16, F3, F7 та F4. Решта параметрів виявили слабкий зв'язок із таргетом, що свідчить про їхню обмежену прогностичну цінність. У цьому контексті доцільним є виключення малозначущих ознак з моделі, що дозволяє зменшити розмірність простору та пришвидшити обчислення. Такий підхід особливо ефективний при застосуванні алгоритмів із високою чутливістю до кількості вхідних змінних, зокрема методу К найближчих сусідів (KNN). Для досягнення балансу між класами у вибірці застосовуються методи попередньої обробки, такі як SMOTE або undersampling. З огляду на значну нерівномірність розподілу між класами у нашому наборі даних, обґрунтованим є використання техніки SMOTE (Synthetic Minority Over-sampling Technique). Її суть полягає у

створенні нових синтетичних прикладів, які структурно подібні до вже наявних елементів класу меншості, проте не є їх прямими копіями. Для цього обчислюється різниця між ознаками наявного об'єкта та його найближчого сусіда, після чого згенерований запис розташовується на векторі між ними. Метод `undersampling` полягає у навмисному зменшенні кількості прикладів класу більшості шляхом видалення частини його спостережень. Проте, незважаючи на простоту реалізації, такий підхід має суттєвий недолік: існує ризик втрати важливої інформації, яка може бути критичною для побудови якісної моделі. Видалення значущих зразків здатне спричинити формування недостатньо репрезентативного набору даних, що негативно вплине на точність прогнозування, особливо під час тестування моделі. На рис. 3.15 та рис. 3.16 продемонстровано приклад результату виконання програмного коду, що реалізує балансування вибірки за допомогою методів SMOTE та `undersampling` відповідно

До балансування:

```
0    133800
1     2400
dtype: int64
```

Після SMOTE:

```
0    133800
1    133800
dtype: int64
```

Рисунок 3.15– Результат до та після застосування SMOTE.

```

До балансування:
0      133800
1       2400
dtype: int64

Після Undersampling:
0      2400
1      2400
dtype: int64

```

Рисунок 3.16 – Результат до та після застосування Undersampling.

3.2.2 Використання методу випадкового лісу

Для виявлення нетипових транзакцій у межах дослідження було застосовано алгоритм Random Forest, який належить до класу ансамблевих методів машинного навчання. Його ефективність у задачах класифікації обумовлена здатністю зменшувати переобучення та підвищувати стійкість до шумових даних.

Далі наведено узагальнену послідовність кроків, що реалізуються в межах роботи цього методу:

1. Для $n = 1 \dots N$ згенеруємо $\tilde{X}_n$ використовуючи бутстрапінг
2. Будуємо дерево рішення $b_n(x)$ за вибіркою $\tilde{X}_n$
 - а. Дерево будуємо поки на кожному листку не буде не більш ніж n_{min} об'єктів
 - б. При кожному розбитті обираємо m випадкових ознак з p , і оптимальне розбиття шукаємо для них
3. Повертаємо композицію $a_N(x) = \frac{1}{N} \sum_{n=1}^N b_n(x)$

У реалізації методу Random Forest було використано бібліотеку scikit-learn мови програмування Python, зокрема клас RandomForestClassifier, який забезпечує

зручний інтерфейс для тренування моделі, налаштування гіперпараметрів та оцінки якості класифікації.

В результаті роботи програми з попередньо обробленими даними, було розпізнано 93% аномальних транзакцій.

Були отримані наступні результати:

$$\text{confusion matrix} = \begin{pmatrix} 9401 & 20 \\ 27 & 131324 \end{pmatrix}$$

$$\text{Precision} = 0.83$$

$$\text{Recall} = 0.86$$

$$\text{F1 Score} = 0.839$$

$$\text{AUC} = 0.931$$

$$\text{Gini} = 0.922$$

А також побудована відповідна ROC AUC крива на рис. 3.17

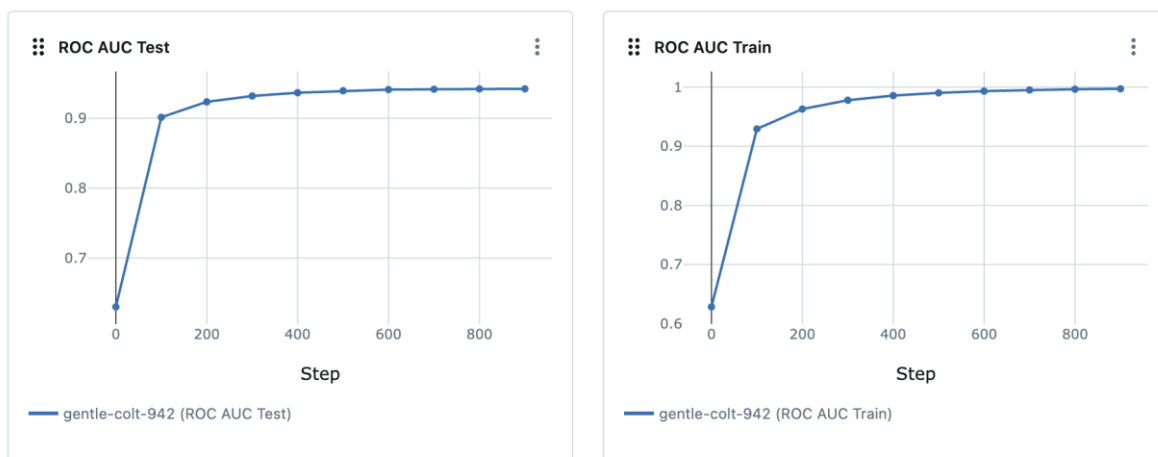


Рисунок 3.17 – ROC AUC крива для Random Forest

3.2.3 Використання методу KNN

Ще одним підходом, застосованим у межах виявлення аномальних транзакцій, є метод К найближчих сусідів (KNN), який належить до класу алгоритмів на основі вимірювання відстаней між об'єктами

Для реалізації цього підходу було використано бібліотеку scikit-learn мови Python, зокрема клас KNeighborsClassifier, який забезпечує зручний механізм побудови моделі, налаштування параметра k та оцінки її якості.

У результаті застосування методу до попередньо обробленої вибірки вдалося досягти рівня виявлення аномальних транзакцій на рівні 90%. Отримані результати підтверджують доцільність використання цього алгоритму у задачах детекції транзакційних відхилень.

$$\text{confusion matrix} = \begin{pmatrix} 93469 & 1154 \\ 38 & 99 \end{pmatrix}$$

$$\text{Precision} = 0.731$$

$$\text{Recall} = 0.883$$

$$\text{F1 Score} = 0.800$$

$$\text{AUC} = 0.9$$

А також побудована відповідна ROC AUC крива на рис. 3.18



Рисунок 3.18 – ROC AUC крива для алгоритму KNN

Слід враховувати, що алгоритм важко масштабується і обрахунки виконуються досить повільно, тобто при збільшенні кількості даних – алгоритм не буде достатньо ефективним.

3.2.4 Використання методу Voting model

Для підвищення якості класифікації було проведено експериментальне дослідження з комбінуванням двох алгоритмів – логістичної регресії та методу випадкових лісів. Такий підхід базується на гіпотезі, що об'єднання моделей з різною природою прийняття рішень дозволить збалансувати переваги кожної з них і покращити загальну ефективність виявлення аномальних транзакцій. Для реалізації цього експерименту було використано мову програмування Python, зокрема бібліотеку scikit-learn, яка надає зручні інструменти для побудови як логістичної регресії (LogisticRegression), так і випадкових лісів (RandomForestClassifier). Комбінування моделей здійснювалося з використанням модулів VotingClassifier та Pipeline, що дозволило інтегрувати обидва підходи в єдину прогнозну систему.

$$\text{confusion matrix} = \begin{pmatrix} 93470 & 15 \\ 48 & 97 \end{pmatrix}$$

$$\text{Precision} = 0.67$$

$$\text{Recall} = 0.87$$

$$\text{F1 Score} = 0.76$$

$$\text{AUC} = 0.96$$

А також побудована відповідна ROC AUC крива на рис. 3.19

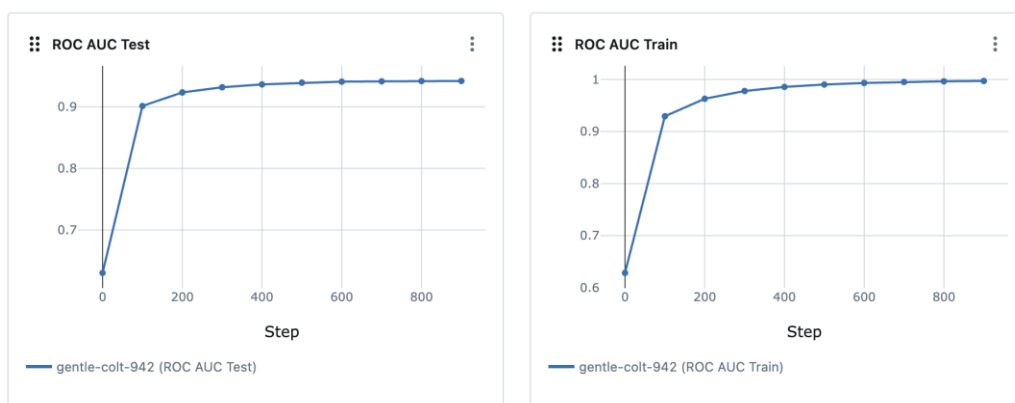


Рисунок 3.19 – ROC AUC крива для алгоритму Voting model

3.2.5 Використання методу CatBoost

Ще одним методом, залученим у межах побудови системи виявлення аномальних транзакцій, є градієнтний бустинг на основі дерев рішень, реалізований за допомогою бібліотеки CatBoost. Даний алгоритм є оптимізованим рішенням від компанії Yandex і демонструє високу ефективність при роботі з табличними даними, особливо за наявності категоріальних ознак або слабо виражених нелінійних залежностей. Для реалізації цього підходу було використано офіційну бібліотеку catboost для мови Python, зокрема клас CatBoostClassifier, який дозволяє виконувати навчання моделей із використанням GPU або CPU, забезпечує автоматичну обробку категоріальних змінних, контроль переобучення та вбудовану оцінку якості моделі. Застосування CatBoost до очищеної вибірки дало змогу досягти високих результатів у задачі класифікації аномальних транзакцій. Ключові метрики якості моделі наведено нижче:

$$\text{confusion matrix} = \begin{pmatrix} 93472 & 1180 \\ 36 & 103 \end{pmatrix}$$

$$\text{Precision} = 0.91$$

$$\text{Recall} = 0.89$$

$$\text{F1 Score} = 0.9$$

$$\text{AUC} = 0.97$$

А також побудована відповідна ROC AUC крива на рис. 3.20

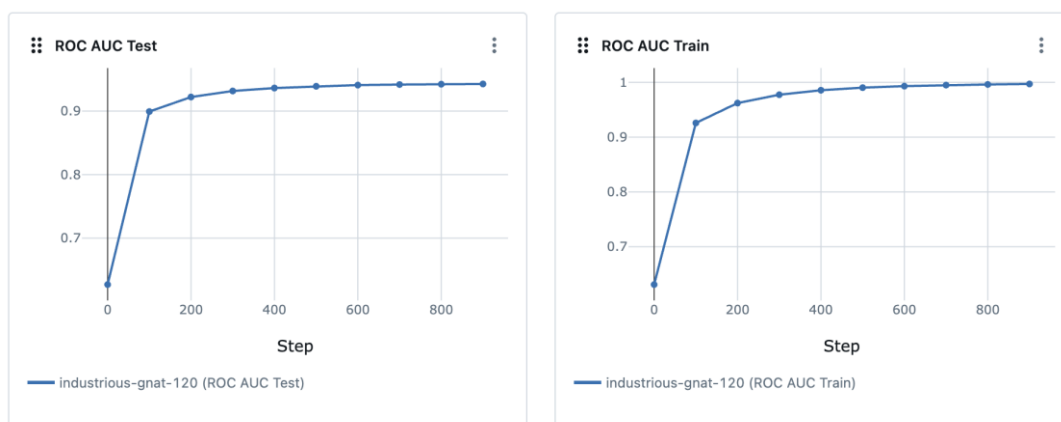


Рисунок 3.20 - ROC- крива для алгоритму CatBoost

3.3 Організаційно-економічне забезпечення А/В тестування для перевірки ефективності системи

Перед запуском експерименту було проведено порівняльний аналіз декількох алгоритмів машинного навчання за ключовими метриками якості класифікації (Precision, Recall, F1-міра, AUC). Найвищу стабільність і точність продемонстрував CatBoost, який і був обраний як основна модель для інтеграції в систему виявлення аномальних транзакцій.

- Після впровадження моделі в продакшн-середовище було організовано А/В тестування – експериментальний підхід, що дозволяє порівняти дві групи користувачів: контрольну (А), яка працює без змін, та тестову (В), де застосовується нове рішення. У нашому випадку це дозволяє об'єктивно оцінити вплив прогнозної моделі на бізнес-метрики, зокрема Fraud rate та Vamp rate.

У контрольній групі транзакції оброблялись за стандартною процедурою. У тестовій групі модель CatBoost здійснювала оцінку ризику кожної транзакції в режимі реального часу, після чого для високоризикових операцій автоматично застосовувалась механіка рефанда – повернення коштів без залучення підтримки. Такий підхід дозволив знизити Fraud rate без шкоди для загального доходу (Gross Revenue), зберігаючи при цьому користувацький досвід.

Ключові метрики аналізуються в розрізі карткових брендів (Visa, Mastercard тощо), що дозволяє враховувати специфіку платіжних систем. Для моніторингу результатів використовується Tableau Online, де створено інтерактивні дашборди, які відображають динаміку Fraud rate, Vamp rate, частку рефандів і поведінкові зміни у групах.

На рис. 3.21 представлено дашборд, що використовується для візуалізації прогресу А/В тесту.

Fraud rate prediction Test

card_brand		control	test
Grand Total	% Fraud rate \$	5.4%	2.8%
	% Diff Fraud rate \$		-47.14%
	VAMP	1.7%	1.4%
	% Diff VAMP		-15.64%
	\$ fraud transactions	\$677	\$389
	\$ all success transactions	\$12,629	\$13,730
VISA	% Fraud rate \$	6.0%	6.5%
	% Diff Fraud rate \$		8.03%
	VAMP	1.7%	1.4%
	% Diff VAMP		-15.64%
	\$ fraud transactions	\$421	\$386
	\$ all success transactions	\$6,973	\$5,925
MC	% Fraud rate \$	4.5%	0.0%
	% Diff Fraud rate \$		-99.32%
	VAMP		
	% Diff VAMP		
	\$ fraud transactions	\$256	\$2
	\$ all success transactions	\$5,655	\$7,805

Рисунок 3.21 – Візуалізації прогресу А/В тесту.

Станом на момент підготовки цієї роботи тест ще триває, оскільки наявний обсяг даних є недостатнім для отримання статистично значущих результатів. Згідно з розрахунком необхідного розміру вибірки методом статистичної потужності ($\alpha = 0.05$, power = 0.8, очікуваний uplift – 20%), досягнення цільового обсягу очікується в липні 2025 року.

Варто підкреслити, що незавершеність А/В тестування на момент написання цієї роботи не свідчить про неповноту дослідження. Адже відповідно до поставленої мети – розробити точну модель для ідентифікації ризикових транзакцій – основні технічні й аналітичні завдання були виконані. А/В тестування виступає наступним кроком комерційної валідації моделі вже у виробничому середовищі.

Факт запуску тесту та використання моделі для обробки реальних транзакцій на веб-платформі Dating-Lift свідчить про практичну цінність створеного рішення та його інтеграцію в реальні бізнес-процеси. Таким чином, результати дослідження не лише залишаються актуальними в науковому сенсі, а й демонструють приклад застосування аналітичних методів машинного навчання у прикладному комерційному контексті. Це тестування виконує роль фінального етапу перевірки системи в реальних умовах, забезпечуючи як технічну, так і економічну валідацію впровадженого рішення.

Висновки до розділу 3

У третьому розділі описано реалізацію прототипу системи виявлення аномальних транзакцій на прикладі вебплатформи Dating-Lift. Використано дані з аналітичної бази Vertica та алгоритми машинного навчання, зокрема Random Forest, KNN, Voting Classifier і CatBoost. Найвищу ефективність показав CatBoost, що й було обрано як базову модель для інтеграції в A/B тест.

Було реалізовано повний технологічний стек – від обробки даних до візуалізації результатів у Tableau Online. Інструменти JupyterLab, MLflow і Prefect забезпечили контрольоване середовище для розробки, моніторингу та розгортання моделі. A/B тестування, незважаючи на незавершеність, вже продемонструвало потенціал моделі до зниження Fraud rate. Важливо, що ця частина дослідження підтвердила не лише технічну доцільність розробки, але й її практичну реалізованість у комерційному середовищі.

ВИСНОВКИ

У межах даної кваліфікаційної роботи було спроектовано та протестовано систему для виявлення ризикованих транзакцій в онлайн-оплатах із використанням сучасних алгоритмів машинного навчання. Враховуючи складність виявлення аномалій у великих обсягах фінансових даних, запропонований підхід дозволяє з високою точністю ідентифікувати потенційно шахрайські операції, зберігаючи при цьому здатність адаптації до змін у поведінці користувачів і прозорість моделі – ключові аспекти для впровадження в платіжну інфраструктуру.

Актуальність теми зумовлена стрімким зростанням обсягів онлайн-платежів у глобальному цифровому середовищі, що супроводжується не менш динамічним розвитком схем шахрайства. Забезпечення безпеки транзакцій стає критично важливим завданням для фінансових установ, платіжних платформ та електронної комерції, що потребує впровадження інноваційних технологічних рішень.

Під час виконання дослідження було проведено ґрунтовний аналіз екосистеми онлайн-платежів та типових загроз. Розглянуто особливості різних методів оплати, зокрема банківські картки, альтернативні фінансові інструменти, криптовалютні платформи та ваучерні системи. Також здійснено огляд країн з підвищеним рівнем транзакційного ризику та класифіковано основні фактори, що сприяють виникненню шахрайських схем.

На основі теоретичного аналізу було сформовано вимоги до моделі та обрано найбільш придатні алгоритми: Random Forest, CatBoost і KNN. Їх порівняння за метриками якості показало доцільність використання ансамблевих методів, зокрема CatBoost, який продемонстрував найкращі результати. Модель CatBoost досягла точності (Precision) 92%, повноти (Recall) 87% та AUC-ROC на рівні 0.976, що свідчить про її високу ефективність в умовах суттєвого дисбалансу класів.

Було створено інфраструктуру для моніторингу та автоматичного оновлення моделі з використанням таких інструментів, як Prefect, MLflow та Tableau. A/B тестування дало змогу перевірити ефективність моделі в умовах живої взаємодії з

користувачами. Попри те, що тест триває, перші результати свідчать про зниження рівня шахрайства без шкоди для бізнес-показників.

Практичне значення роботи підтверджується впровадженням моделі в рамках реального вебсервісу, що дозволяє розглядати створене рішення як готове до масштабування. Модель може бути інтегрована в інші сервіси з подібною архітектурою даних, забезпечуючи адаптивний захист від нових типів шахрайства.

Таким чином, поставлену мету роботи – розробити ефективну, інтерпретовану та впроваджену систему ідентифікації ризикованих транзакцій – було досягнуто повністю. Робота має як теоретичну, так і практичну цінність, демонструючи можливість синергії наукових підходів і бізнес-рішень у сфері безпеки онлайн-платежів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Оніщенко Д. С. Виявлення ризиків шахрайства в онлайн-оплатах за допомогою алгоритмів машинного навчання // VI Міжнародна науково-практична конференція молодих вчених, аспірантів і студентів «Сучасні інформаційні технології та системи в управлінні». 11 квітня 2025 р.
2. Оніщенко Д. С., Донєв Д. Р. Аспекти кібербезпеки соціально-економічних систем в умовах інформаційної війни // Матеріали V Міжнародної науково-практичної конференції молодих вчених, аспірантів і студентів «Сучасні інформаційні технології та системи в управлінні». – Київ: КНЕУ, 18–19 квітня 2024 р.
3. Оніщенко Д. С., Донєв Д. Р. Economic Cybernetics – Theory, Practice and Development Directions // Матеріали 5-ї Міжнародної науково-практичної конференції «Economic Cybernetics – Theory, Practice and Development Directions». – Одеса: Національний політехнічний університет, 29–30 листопада 2023 р.
4. Explainable machine learning for fraud detection / Psychoula I., Kertyzopoulos K., Sotiriadis S., Psannis E. // Computer. 2021. Vol. 54, no. 10. P. 49–59. <https://doi.org/10.1109/mc.2021.3081249> (дата звернення: 08.04.2025).
5. Finding fraud. Secrets of machine learning. 2024. P. 115–119. https://doi.org/10.1142/9781800614895_0017 (дата звернення: 08.04.2025).
6. Fraud detection using machine learning and deep learning // International Research Journal of Modernization in Engineering Technology and Science. 2023. <https://doi.org/10.56726/irjmets39476> (дата звернення: 08.04.2025).
7. Manish Korde. Fraud Detection in Financial Systems Using Machine Learning Techniques. Journal of Information Systems Engineering and Management. 2025. Vol. 10, no. 33s. P. 921–932. URL: <https://doi.org/10.52783/jisem.v10i33s.5737> (date of access: 21.05.2025).
8. Suriya S., Madhumitha N. H. Heart Failure Prediction using Gaussian Naïve Bayes Algorithm. June 2023. 2023. Vol. 5, no. 2. P. 125–143. URL: <https://doi.org/10.36548/jitdw.2023.2.004> (date of access: 21.05.2025).

- 9 Data mining for credit card fraud: A comparative study / S. Bhattacharyya et al. Decision Support Systems. 2011. Vol. 50, no. 3. P. 602–613. URL: <https://doi.org/10.1016/j.dss.2010.08.008> (date of access: 21.05.2025).
- 10 Hanbali N., El-Yahyaoui A. Advanced machine learning and deep learning approaches for fraud detection in mobile money transactions. Innovations in Systems and Software Engineering. 2025. URL: <https://doi.org/10.1007/s11334-025-00605-5> (date of access: 21.05.2025).
- 11 Domingues R. Machine learning for unsupervised fraud detection: thesis. 2015. URL: <http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-181027> (дата звернення: 08.04.2025).
- 12 Jabardi M. Support Vector Machines: Theory, Algorithms, and Applications. Infocommunications journal. 2023. Vol. 17, no. 1. P. 66–75. URL: <https://doi.org/10.36244/icj.2025.1.8> (date of access: 21.05.2025).
- 13 How much is a chargeback fee? // Verifi. URL: <https://www.verifi.com/in-the-news/much-chargeback-fee/> (дата звернення: 08.04.2025).
- 14 Credit Card Fraud Detection: A Novel Approach Using Aggregation Strategy and Feedback Mechanism / C. Jiang et al. IEEE Internet of Things Journal. 2018. Vol. 5, no. 5. P. 3637–3647. URL: <https://doi.org/10.1109/jiot.2018.2816007> (date of access: 21.05.2025).
- 15 Kaspersky Lab. Global IT Security Risks Survey. 2015. URL: <https://media.kaspersky.com/pdf/global-it-security-risks-survey-2015.pdf> (дата звернення: 08.04.2025).
- 16 Kumar G., Kumar S., Prakash A. A. Credit card fraud detection using machine learning // International Journal of Engineering and Advanced Technology. 2021. Vol. 10, no. 4. P. 124–126. <https://doi.org/10.35940/ijeat.d2344.0410421> (дата звернення: 08.04.2025).
- 17 Lalitha Sree Thatavarthi N. Leveraging machine learning for payment fraud detection // International Journal of Science and Research (IJSR). 2020. Vol. 9, no. 1. P. 1939–1941. <https://doi.org/10.21275/sr24615131232> (дата звернення: 08.04.2025).

18 Xu-Ying Liu, Jianxin Wu, Zhi-Hua Zhou. Exploratory Undersampling for Class-Imbalance Learning. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics). 2009. Vol. 39, no. 2. P. 539–550. URL: <https://doi.org/10.1109/tsmcb.2008.2007853> (date of access: 21.05.2025).

19 ÇAĞLAYAN M., BAHTİYAR Ş. Money Laundering Detection with Node2Vec. GAZI UNIVERSITY JOURNAL OF SCIENCE. 2021. URL: <https://doi.org/10.35378/gujs.854725> (date of access: 21.05.2025).

20 Mobile money fraud detection using data analysis and visualization techniques / R. Al-Sayyed et al. Multimedia Tools and Applications. 2023. URL: <https://doi.org/10.1007/s11042-023-16068-4> (date of access: 21.05.2025)

21 Lvyas T. Machine Learning Neural Network Handwriting Recognition. SSRN Electronic Journal. 2022. URL: <https://doi.org/10.2139/ssrn.4047164> (date of access: 21.05.2025)

22 Midigator. The year in chargebacks: an annual report. 2019. URL: <https://midigator.com/the-year-in-chargebacks-report-2019/> (дата звернення: 08.04.2025).

23 Moth D. Alternative payments used in 11% of online purchases in the UK. 2012. URL: <https://econsultancy.com/alternative-payments-used-in-11-of-online-purchases-in-the-uk/> (дата звернення: 08.04.2025).

24 Ngai E. W., Hu Y., Wong Y. H., Chen Y., Sun X. The application of data mining techniques in financial fraud detection: a classification framework and academic review // Decision Support Systems. 2011. Vol. 50, no. 3. P. 559–569.

25 Nilson Report. 2016. URL: https://nilsonreport.com/upload/content_promo/The_Nilson_Report_10-17-2016.pdf (дата звернення: 08.04.2025).

26 PCI DSS. Quick Reference Guide. 2019. URL: <https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf> (дата звернення: 08.04.2025).

27 Rokach L., Maimon O. Decision Trees // Data Mining and Knowledge Discovery Handbook. 2005. P. 165–192. https://doi.org/10.1007/0-387-25465-X_9.

28 Roy A., Sunitha C., Saha S. LSTM-based deep learning model for detecting financial fraud // International Journal of Engineering Research & Technology (IJERT). 2020. Vol. 9, no. 9. P. 45–49.

29 Sekar M. Fraud and anomaly detection // Machine Learning for Auditors. Berkeley, CA: Apress, 2022. P. 193–202. https://doi.org/10.1007/978-1-4842-8051-5_21 (дата звернення: 08.04.2025).

30 ShiftProcessing. Credit card fraud statistics. URL: <https://shiftprocessing.com/credit-card-fraud-statistics/> (дата звернення: 08.04.2025).

31 Stripe. How machine learning works for payment fraud detection and prevention // Stripe Blog. URL: <https://stripe.com/resources/more/how-machine-learning-works-for-payment-fraud-detection-and-prevention> (дата звернення: 08.04.2025).

32 The Payment Services Directive: what it means for consumers. URL: https://web.archive.org/web/20130530163006/http://ec.europa.eu/internal_market/payments/docs/framework/psd_consumers/psd_en.pdf (дата звернення: 08.04.2025).

33 Visa Acquirer Monitoring Program (VAMP) in 2025: Merchant Edition // Solidgate. URL: <https://solidgate.com/blog/new-visa-acquirer-monitoring-program-vamp/> (дата звернення: 08.04.2025).

34 Xuan S., Liu G., Li Z., Zheng L., Wang S., Jiang C. Random Forest for credit card fraud detection // Proceedings of the 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC). IEEE, 2018. P. 1–6.

35 Collaris D., Vink L.M., van Wijk J.J. Instance-level explanations for fraud detection: a case study // arXiv preprint arXiv:1806.07129. 2018.

36 Goodall J.R., Ragan E.D., Steed C.A., Reed J.W., Richardson G.D., Huffer K.M., Bridges R.A., Laska J.A. Situ: identifying and explaining suspicious behavior in networks // IEEE Transactions on Visualization and Computer Graphics. 2018. Vol. 25, no. 1. P. 204–214.

37 Liu N., Shin D., Hu X. Contextual outlier interpretation // arXiv preprint arXiv:1711.10589. 2017.

- 38 Lundberg S.M., Lee S.I. A unified approach to interpreting model predictions // Advances in Neural Information Processing Systems. 2017. P. 4765–4774.
- 39 Nguyen Q.P., Lim K.W., Divakaran D.M., Low K.H., Chan M.C. Gee: a gradient-based explainable variational autoencoder for network anomaly detection // Proceedings of the 2019 IEEE Conference on Communications and Network Security (CNS). IEEE, 2019. P. 91–99.
- 40 Ribeiro M.T., Singh S., Guestrin C. “Why should I trust you?” explaining the predictions of any classifier // Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. 2016. P. 1135–1144.
- 41 Saia R., Carta S., et al. A frequency-domain-based pattern mining for credit card fraud detection // Proceedings of the IoTBDS Conference. 2017. P. 386–391.
- 42 Takeishi N. Shapley values of reconstruction errors of PCA for explaining anomaly detection // Proceedings of the 2019 International Conference on Data Mining Workshops (ICDMW). IEEE, 2019. P. 793–798.
- 43 Thennakoon A., Bhagyan C., Premadasa S., Mihiranga S., Kuruwitaarachchi N. Real-time credit card fraud detection using machine learning // Proceedings of the 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence). IEEE, 2019. P. 488–493.
- 44 Varmedja D., Karanovic M., Sladojevic S., Arsenovic M., Anderla A. Credit card fraud detection – machine learning methods // Proceedings of the 2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH). IEEE, 2019. P. 1–5.
- 45 Vu A.V., Hughes J., Pete I., Collier B., Chua Y.T., Shumailov I., Hutchings A. Turning up the dial: the evolution of a cybercrime market through set-up, stable, and COVID-19 eras // Proceedings of the ACM Internet Measurement Conference (IMC). 2020.

ДОДАТКИ

Додаток А Тези

Оніщенко Д. С., магістрант,
здобувачка 6 курсу гр. ІІІІ-601
спеціальності «8i09»
Київський національний економічний
університет імені Вадима Гетьмана
diana29.oni2@gmail.com

VISA ACQUIRER MONITORING PROGRAM ЯК ДРАЙВЕР ВПРОВАДЖЕННЯ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ ДЛЯ ВИЯВЛЕННЯ ШАХРАЙСТВА В ОНЛАЙН-ПЛАТЕЖАХ

У 2022 році глобальні втрати від шахрайства в онлайн-платежах сягнули \$41 мільярда, а до кінця 2023-го ця цифра, зросла до \$48 мільярдів. Через такі масштабні ризики протидія платіжному шахрайству стала одним із пріоритетів для бізнесу. Visa та її клієнти мають спільне завдання - захистити від шахрайства всіх учасників платіжного процесу.

Тож, починаючи з 1 квітня 2025 року, Visa запускає вдосконалену програму VAMP (Visa Acquirer Monitoring Program). З цим оновленням VAMP запроваджує метрику ризику та її порогові значення, які будуть впроваджуватися в два етапи. Ці зміни вимагатимуть від онлайн-продавців більш зваженого підходу до управління ризиками, щоб залишатися в межах порогових значень. Починаючи з квітня 2025 року, онлайн-бізнеси, які перевищують 1,5% коефіцієнт VAMP, потраплятимуть під негайний моніторинг зі штрафними санкціями в розмірі \$10 за кожен диспут. У 2026 році цей поріг ще більше знизиться – до 0,9%, що посилить тиск на компанії щодо впровадження ефективних інструментів боротьби з ризиками. VAMP сприяє підвищенню рівня безпеки в середовищі, в якому вони працюють.

Саме в цьому контексті програма Visa Acquirer Monitoring Program (VAMP) виступає як потужний стимул до впровадження алгоритмів машинного навчання для виявлення шахрайства в онлайн-платежах. Компанії, які обробляють платежі клієнтів, можуть ефективно використовувати системи на базі машинного навчання для виявлення та запобігання шахрайству в різних платіжних сценаріях.

Мобільні платежі. Цифровий "відбиток пристрою": алгоритми створюють унікальний профіль пристрою на основі таких параметрів, як модель смартфона, операційна система та IP-адреса. Це дозволяє виявити підозрілі дії, включаючи спроби захоплення акаунтів або використання одного пристрою для кількох профілів. Біометричні поведінкові характеристики: машинне навчання аналізує динаміку взаємодії користувача з пристроєм – швидкість введення тексту, жести, шаблони використання додатків – для верифікації особи та фіксації потенційних загроз.

Електронна комерція. Запобігання захопленню акаунтів: ML-моделі відстежують активність користувача при вході: кількість невдалих спроб авторизації, нові пристрої або IP-адреси. Виявлення аномалій дозволяє оперативно реагувати на спроби несанкціонованого доступу. Виявлення так званого «дружнього» шахрайства: у таких випадках покупці заперечують участь у транзакціях або стверджують, що товар не було доставлено. Алгоритми аналізують історію покупок, повернень і спірних операцій для ідентифікації шаблонів подібної поведінки.

Далі розглянемо сучасні алгоритми виявлення шахрайства на основі машинного навчання,

які впроваджуються компаніями з великим обсягом онлайн-платежів.

Gradient Boosting Machines (GBM) – це потужний підхід ансамблевого навчання, що базується на об'єднанні декількох слабких моделей (як правило, дерев рішень) у єдину, високоточну предиктивну систему. Головною перевагою цього методу є послідовне зменшення помилок за рахунок ітеративного навчання. Ця властивість робить GBM надзвичайно придатним для аналізу складних та неоднорідних даних, зокрема – у сфері виявлення фінансових махінацій.

Один із практичних прикладів успішного застосування GBM – досвід компанії **Capital One**, одного з провідних фінансових холдингів у США. Вони інтегрували алгоритми градієнтного бустингу у свою систему контролю транзакцій, що дало змогу значно покращити здатність виявляти шахрайські дії та своєчасно на них реагувати. Цей приклад підтверджує ефективність GBM як інструмента боротьби з шахрайством і може слугувати орієнтиром для інших компаній, які прагнуть зміцнити власні системи безпеки.

У контексті боротьби з фінансовими махінаціями нейронні мережі, особливо глибокі нейронні структури (deep learning), виявляють себе як надзвичайно перспективні. Вони здатні самостійно розпізнавати приховані закономірності в об'ємних наборах даних, що часто недоступні для традиційних моделей. Далі розглянемо приклади. Аналіз транзакцій у часі: Рекурентні нейронні мережі (RNN) допомагають відстежити послідовність операцій, виявляючи підозрілі шаблони поведінки. Обробка візуальної інформації: Конволюційні мережі (CNN) аналізують зображення – наприклад, скани чеків або документів – для виявлення підробок. Комбіновані підходи: Поєднання нейронних мереж з іншими алгоритмами (як-от градієнтний бустинг) дозволяє підвищити точність розпізнавання шахрайства.

XGBoost (Extreme Gradient Boosting) – ще один потужний інструмент у світі машинного навчання, який демонструє вражаючу ефективність у виявленні шахрайства. Цей алгоритм відрізняється високою точністю, гнучкістю та здатністю ефективно працювати з великими обсягами складних даних.

Одне з досліджень запропонувало використання XGBoost для боротьби з шахрайством у сфері мобільних платежів. Поєднуючи XGBoost із методами виявлення аномалій без учителя, дослідники досягли високих результатів при аналізі понад 6 мільйонів мобільних транзакцій. В іншому прикладі модель XGBoost була застосована до даних по кредитних картках: там для виділення шахрайських операцій використовували підхід на основі сумарної відстані між точками даних. Ще один цікавий випадок – дослідження з використанням даних Державної енергетичної корпорації Китаю (SGCC), де XGBoost поєднували з генетичними алгоритмами. Така інтеграція виявилася перспективною і відкрила нові напрями для подальших досліджень у сфері розпізнавання шахрайських дій.

Автоенкодера – це алгоритми стиснення даних, які автоматично навчаються з прикладів. Вони складаються з двох частин: енкодера, що перетворює вхідні дані на зменшену форму, та декодера, який намагається відновити ці дані. У процесі відновлення мережа вчиться знаходити ключові ознаки та виявляти відхилення, що робить автоенкодери ефективним інструментом виявлення аномалій. У сфері боротьби з шахрайством автоенкодери застосовуються для виявлення незвичних транзакцій. Наприклад, у кредитно-фінансовій сфері вони аналізують типові шаблони платежів і сигналізують про відхилення, які можуть свідчити про шахрайство.

Інтеграція ML-рішень у процеси захисту від шахрайства дозволяє компаніям зменшити фінансові ризики, підвищити довіру клієнтів та створити більш надійну екосистему обробки платежів.

Висновок: Програма Visa Acquirer Monitoring Program виступає важливим драйвером впровадження алгоритмів машинного навчання у сфері виявлення онлайн-шахрайства. Інтеграція ML-рішень у платіжну інфраструктуру дає змогу компаніям значно знизити фінансові ризики, покращити рівень клієнтської довіри та зміцнити безпеку екосистеми електронних платежів. Автоматизовані системи виявлення аномалій на основі машинного навчання не лише забезпечують оперативне реагування на загрози, а й підвищують загальну ефективність боротьби з шахрайством у цифровому середовищі.

Додаток Б

Тези

Онiщенко Д. С., магістрант,
студентка 5 курсу гр. ІІІІ-501
спеціальності «8i09»
Київський національний економічний
університет імені Вадима Гетьмана
diana29.oni2@gmail.com

Донєв Д. Р., магістрант,
студент 5 курсу гр. ІІІІ-501
спеціальності «8i09»
Київський національний економічний
університет імені Вадима Гетьмана
djdondan@gmail.com

ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ДАНИХ В РЕКЛАМІ

Проблематика: У сучасному цифровому середовищі онлайн-реклама є неодмінною складовою ефективної маркетингової стратегії для бізнесу будь-якого масштабу. У той час як рекламодавці інвестують значні кошти в цифрову рекламу, важливо мати інструменти, що допомагають передбачити ймовірність успіху рекламної кампанії. Конкуренція між рекламодавцями є вкрай жорсткою. Кожна компанія намагається залучити увагу інтернет-користувачів і перетворити цю увагу на кліки, продажі та конверсії.

Вступ: Бізнес інвестує мільйони в рекламу. Провідним сегментом рекламної індустрії сьогодні є реклама в Інтернеті. Онлайн-ігри, мобільні додатки, соціальні мережі, платформи електронної комерції, пошукові портали, онлайн-відео, банери та інші цифрові медіа - це лише кілька прикладів багатьох цифрових медіа, які використовуються в онлайн-рекламі для охоплення потенційних клієнтів. Інтелектуальний аналіз даних докорінно змінив підхід бізнесу до маркетингу, надаючи розуміння поведінки клієнтів, визначаючи нові можливості та удосконалюючи маркетингові стратегії. Основними компонентами інтелектуального аналізу даних, які підтримують інтернет-маркетинг, є збір, об'єднання, аналіз і відповідне відображення даних бізнес-аналітики. Після інтелектуального аналізу даних та аналітики бізнес-аналітика допомагає визначити реальну модель поведінки споживачів. Таким чином, акцент на персоналізації та кастомізації контенту в багатьох цифрових каналах є одним із головних наслідків впливу Big Data, в будь-якій формі, на цифровий маркетинг.

Теза 1: Перш за все, важливо розуміти поведінку споживачів, уподобань і моделей купівлі за допомогою аналізу даних, що дозволяє компаніям адаптувати маркетингові кампанії, розробляти нові продукти, оптимізувати стратегії продажів і підвищити рівень задоволеності клієнтів. Серед ключових підходів, які розглядаються в процесі інтелектуального аналізу даних є: ідентифікація проблеми, підготовка даних, розробка моделі, використання моделі та моніторинг моделі. Використовують низку методів для класифікації та регресійних моделей, включаючи дерева рішень, штучні нейронні мережі, еволюційні алгоритми та правила асоціацій. Для того, щоб

знайти приховані закономірності та ідеї з різних джерел даних, таких як документи, веб-матеріали та мультимедійні файли, досліджуються складні підходи до інтелектуального аналізу даних, такі як аналіз тексту, веб-аналіз та мультимедійний аналіз.

Крім того, розглядаються такі тактики CRM (customer relationship management), як готовність покупця, вигоди, поведінка, привід, психографія життя, демографія, життєвий цикл, географія, лояльність, продукт, прибутковість, взаємодія та задоволеність для сегментації. Акцент зроблено на ідеї аналізу споживчої цінності та важливості розуміння сприйнятої цінності, загальних переваг, витрат і суб'єктивних поглядів споживачів.

Теза 2: Останніми роками спостерігається великий інтерес до впровадження методів персоналізованого маркетингу та інструментів інтелектуального аналізу даних у цифрову компанію як стратегію змішаних методів, що включала як якісні, так і кількісні методи дослідження. З точки зору якісних методів, наприклад, у одному з досліджень проводили глибинні інтерв'ю. Кількісні методи використовувалися для збору даних про поведінку споживачів з різних онлайн-джерел, включаючи електронну комерцію Shopee, Instagram, TikTok, WhatsApp та Instagram. Кількісний аналіз цих даних проводиться за допомогою таких методів, як аналіз асоціацій, який виявив взаємозв'язки між продуктами та моделями покупок, системи рекомендацій, які відповідають індивідуальним уподобанням клієнтів, та кластерний аналіз, який виявив групи клієнтів зі схожими уподобаннями та поведінкою. Використовуючи ці методи, дослідники змогли отримати всебічне розуміння того, як споживачі ставляться до індивідуальної маркетингової тактики і як вони поведуться в інтернет-магазинах.

Теза 3: Прогнозування CTR (коефіцієнт кліків) - це розрахунок ймовірності того, що користувач натисне на рекламне оголошення. Цей показник дуже важливий в системах онлайн-реклами. Згідно з традиційною парадигмою оплати за клік, рекламодавці отримують гроші лише тоді, коли глядачі натискають на їхні оголошення, а отже, вищий CTR може збільшити прибутки рекламодавців. Використовуючи сучасні підходи машинного навчання на основі великих обсягів даних, можна отримати більш точний прогноз CTR, що дозволить підвищити ефективність рекламних кампаній і знизити витрати на рекламу. Підходи, які дозволяють видавцям вибирати, яке рекламне зображення показувати конкретному користувачеві на веб-сторінці, щоб максимізувати CTR, користуються високим попитом через необхідність максимізації доходу для видавців. Тому в більшості систем онлайн-реклами основним обов'язком розміщення реклами є передбачення CTR. На прикладі однієї з найбільших рекламних платформ в Інтернеті, Google AdWords, можна продемонструвати, наскільки важливим є показник CTR для систем управління рекламними кампаніями. Моделі дерева рішень, моделі глибокого навчання, моделі машин факторизації та багатовимірні статистичні моделі - це чотири сучасні моделі, доступні для прогнозування CTR. Два найпоширеніші в літературі багатовимірні статистичні методи прогнозування CTR реклами - це логістична регресія та поліноми другого ступеня. Одним з методів, який найчастіше використовується для прогнозування CTR за багатьма факторами, є логістична регресія (LR). Він може повертати число від 0 до 1, що вказує на ймовірність кліка, а також лінійну суміш декількох атрибутів, яка відображає кореляцію між якостями та етикеткою. Однак LR не може врахувати ефекти взаємодії або нелінійні кореляції. У літературі LR часто використовують як еталон для оцінки ефективності рекомендованих моделей прогнозування CTR. Дослідники відзначають, що факторизовані параметри та машини факторизації (МФ) можуть допомогти в оцінці моделі на розріджених даних для прогнозування CTR. МФ та їхні розширення часто використовуються для прогнозування кліків у дослідницькій літературі з реклами. На конкурсі KDDCup 2012 вони продемонстрували, що МФ можуть точно оцінити взаємодію характеристик при прогнозуванні CTR реклами. У 2015 році було представлено стратегію онлайн-навчання для прогнозування CTR, яка використовує алгоритм Follow-TheRegularized-Leader (FTRL-проксимальний) у МФ. Хоча моделі низького порядку прості у створенні, вони не дуже добре справляються з прогнозуванням, особливо в складних рекламних системах. AUC показує, що моделі прогнозування CTR на основі LSTM та RNN перевершують лінійні (наприклад, LR та наївні байєсівські) та нелінійні (наприклад, нейронні мережі та випадкові ліси) моделі. Однак, оскільки LSTM навчаються послідовно, вони вимагають більше

часу і пам'яті на етапі навчання. Деревоподібні моделі використовуються в широкому спектрі обчислювальних рекламних додатків. Gradient Boosting Decision Tree (GBDT) і XGBoost засновані на машині градієнтного бустінгу (GBM), яка продемонструвала великий успіх у прогнозуванні CTR. Для масової реклами у Facebook автори пропонують конкатенацію GBDT та LR для прогнозування CTR, де вихід GBDT слугує входом LR. В результаті GBDT значно підвищує продуктивність LR за рахунок автономного вибору ознак.

Теза 4: Ще один із підходів до вивчення задоволеності та незадоволеності користувачів, використовуючи аналіз текстів. Для цього можна метод латентного семантичного аналізу (LSA), який дозволяє витягти приховані семантичні зв'язки слів та фраз з корпусу документів.

У процесі обробки даних вилучаються зайві слова, об'єднуються пов'язані фрази та визначаються змінні, що вказують на задоволеність і незадоволеність користувачів. Результати дослідження підтверджують важливість тих чи інших елементів, а також допомагають визначити пропозицій чи послуг, які впливають на задоволеність чи незадоволеність користувачів. Далі ці знання використовують для створення фраз на креативах чи квізах, що збільшує зацікавленість користувачів, що в свою чергу збільшує дохід компанії. Оскільки текстова аналітика є відкритою структурою, вона може надавати більш точні звіти про клієнтський досвід, ніж звичайні методи опитування, такі як анкетування або інтерв'ю.

Аналіз великих даних про поведінку та задоволеність клієнтів значно полегшується завдяки застосуванню LSA та текстової аналітики.

Теза 5: Розглянемо приклад коли інтелектуальний аналіз даних в рекламі покращив роботу компанії порівняно з конкурентами. Ретельний аналіз особливої та креативної маркетингової тактики Tesla відрізняє її від традиційних методів, що використовуються в автомобільній індустрії для продажу та реклами. Цифровий маркетинг є основною стратегією, оскільки він не вимагає традиційних витрат на рекламу. Соціальні мережі, такі як Facebook, Instagram, Twitter і YouTube, є основними майданчиками для просування продуктів і бренду Tesla. Тут також проводиться вся реклама та продажі компанії. До 70% продажів компанії, за даними дослідників, здійснюються онлайн.

Працівники компанії проаналізували багато даних про покупців і їхню реакцію на маркетингові ініціативи компанії, використовуючи методи інтелектуального аналізу даних. Зокрема, споживачі були згруповані на основі їхніх інтересів та поведінкових тенденцій за допомогою алгоритмів кластеризації. Це дало змогу визначити, які елементи маркетингових зусиль приваблюють цільову аудиторію та сприяють збільшенню продажів і впізнаваності бренду.

Висновок: Підкреслюю стратегічну цінність інтелектуального аналізу даних у рекламі, особливо в тому, що він допомагає компаніям залишатися конкурентоспроможними на швидко мінливому цифровому ринку, допомагаючи їм передбачати майбутні тенденції, приймати обґрунтовані рішення і так далі. Інтелектуального аналіз даних забезпечує адаптованість маркетингових зусил, поліпшення прогнозів продажів і зміцнення зв'язків з клієнтами, що в результаті сприяє процвітанню і довголіттю організацій.

ВИКОРИСТАННЯ ПРАКТИК ІТ-КОМПАНІЙ ДЛЯ ПОСИЛЕННЯ СУСПІЛЬНОЇ КОМП'ЮТЕРНОЇ БЕЗПЕКИ ПІД ЧАС ВІЙНИ 21-ГО СТОЛІТТЯ

*В. І. Скіцько, доцент
Д. Р. Донєв, магістрант
Д. С. Оніщенко, магістрант*

Київський національний економічний університет ім. Вадима Гетьмана

Обґрунтування актуальності проблеми

Україна стала жертвою систематичних кібератак зі сторони країни-агресора, що несе негативний вплив у соціальній, гуманітарній та промисловій сферах. За даними дослідження Державної служби спеціального зв'язку та захисту інформації України, ці атаки викликають непередбачувані наслідки для функціонування держустанов та безпеки громадян [1]. Незважаючи на вжиті заходи, проблема залишається актуальною через людський фактор, який включає в себе недостатню безпекову обізнаність та соціальну інженерію. Зловмисники активно використовують людську необачність, щоб отримати доступ до конфіденційної інформації та порушити стабільний режим функціонування держави. У роботі наведено огляд останніх успішних практик ІТ-компаній та держустанов щодо системного поліпшення обізнаності співробітників у галузі інформаційної безпеки. Найкращі з них пропонується запровадити для держустанов та підприємств критичної інфраструктури з метою запобігання отриманню несанкціонованого доступу до конфіденційних систем державою-агресором і їх компрометації.

Аналіз останніх досліджень і публікацій

Захист ІТ-систем від атак і несанкціонованого доступу є надважливим питанням для компаній. В розвиток цієї галузі інвестуються значні ресурси, бо втрати можуть бути суттєвими. Згідно зі звітом Cybersecurity Business Report, кіберзлочинність, коштувала "понад 6 трильйонів доларів у 2021 році, порівняно з 3 трильйонами доларів у 2015 році" [2]. Тому організації постійно шукають і створюють більш якісні методи збереження безпеки своєї інформації. При цьому, значна кількість інцидентів (як навмисних, так і ненавмисних), пов'язаних з витоками інформації, відбувається через людський фактор [3]. Зазначається, що близько 77% витоків даних у компаніях відбуваються через використання людської неграмотності. Розроблені практики роботи з персоналом треба поширювати на державні об'єкти, які не мають достатньо ресурсів для інвестування у дослідницьку діяльність щодо безпеки. Далі у тексті наведено приклади таких практик з посиланням на оригінальні дослідження.

Формулювання мети роботи

Метою роботи є зібрати набір практик для підвищення обізнаності і вироблення навичок протидії комп'ютерним атакам країни-агресора для українських установ і бізнесів. Підхід має відображати останні дослідження у галузі кібербезпеки і роботи з персоналом. Пропоновані підходи мусять мати підтвердження доцільності свого впровадження на реальних кейсах. Забрані рекомендації допоможуть уникнути значної кількості кіберзлочинів, виробивши "імунітет" серед персоналу, на який спрямовані хакерські атаки.

Виклад основного матеріалу дослідження

Опишемо знайдені нами підходи, які вже довели свою ефективність.

Гейміфікація є новим явищем у сфері розвитку комп'ютерної грамотності. Співробітникам пропонується взаємодіяти зі спеціально розробленою грою, щоб стати більш обізнаними про

загрози та вразливості інформаційної безпеки. Гейміфікація є підходящим рішенням для підвищення рівня знань працівників, оскільки вона персоналізує навчальний контент відповідно до потреб компанії чи підприємства. Інтерактивний прототип гри, представлений під час оцінки впливу вказаного підходу, запропонований працівникам на семінарах показав, що працівники були більш вмотивовані та готові дотримуватися використовуваних методів безпеки, порівняно з групою, яка прослухала серію лекцій з тими самими темами [4]

Метод виявлення порушень використовується для попередження виконання співробітником небажаних дій, разом з тим пояснюючи помилку і потенційні ризики. Цей метод допомагає доносити матеріал на основі порушень працівниками політик компанії (відкриття імейлу з невідомого домену, встановлення на комп'ютер неліцензованих додатків). Він працює за допомогою методу контролю фізичного доступу за допомогою радіочастотної ідентифікації (RFID). Технологія RFID виявить і зареєструє будь-який несанкціонований доступ до інформації з боку працівника. Таким чином, повідомлення про це конкретне порушення буде надіслано саме цьому працівникові. За оцінками оригінального дослідження [5], кількість випадків несанкціонованого доступу в організації різко зменшилася, коли цей метод був адаптований. І в той же час, рівень обізнаності серед співробітників покращився завдяки використанню цього підходу.

Покращення загальних ІТ-знань працівників є однією з найвпливовіших передумов інформаційної безпеки. ІТ-знання працівників стосуються загальних знань основних ІТ-додатків, що використовуються у повсякденній роботі, таких як комп'ютери, системи електронної пошти та Інтернет. Рівень загальних ІТ-знань позитивно впливає на рівень ІСА працівників [6]. Чим більше працівники знають про інформаційну безпеку та ІТ, тим більше вони обізнані з питаннями інформаційної безпеки. Таким чином, організаціям рекомендується підвищувати рівень ІТ-знань працівників, щоб запобігти ненавмисним порушенням. Цю думку також підтверджують емпіричним шляхом інші публікації з цієї теми, які в поточній роботі не наводяться.

Висновки даного дослідження й перспективи подальшого розвитку

Проблема кібербезпеки в Україні є актуальною та серйозною, зокрема через систематичні кібератаки та людський фактор, який допускає вразливості в інформаційній безпеці. Дослідження виявило підходи призначені для підвищення кіберграмотності та свідомості персоналу, які можуть стати ефективними засобами протидії комп'ютерним атакам. Перспективи подальшого розвитку включають імплементацію практик, які вже успішно використовуються ІТ-компаніями, зокрема в сфері гейміфікації та методів виявлення порушень. Запропоновані підходи для підвищення обізнаності та навичок протидії кібератакам може слугувати основою для розробки програм та навчальних ініціатив у держустановах та підприємствах критичної інфраструктури. Дослідження також підкреслило важливість інвестування у кібербезпеку як приватними, так і державними підприємствами, оскільки витрати на боротьбу з кіберзагрозами значно перевищують можливі втрати внаслідок кіберзлочинності. У майбутньому, з урахуванням постійного розвитку технологій та методів атак, необхідно посилювати зусилля у вдосконаленні систем кіберзахисту та поширювати свідомість щодо кібербезпеки серед різних шарів суспільства.

Використання інноваційних підходів, таких як гейміфікація, може сприяти збільшенню відповідальності та обізнаності персоналу, зменшити ризик людських помилок та створити ефективний механізм протидії кіберзагрозам в Україні.

```
# --- Code from preprocessing ---

#!/usr/bin/env python

# coding: utf-8

# In[1]:

import matplotlib.pyplot as plt

get_ipython().run_line_magic('matplotlib', 'inline')

import numpy as np

import pandas as pd

pd.set_option('display.max_rows', None)

pd.set_option('display.max_columns', None)

import seaborn as sns

from sklearn.preprocessing import StandardScaler

import statsclf_models.api as sm

# Load raw_dataset

# In[2]:

transactions_raw_data_main = pd.read_csv('raw_data/creditcard.csv', header=0)

# Work on null values

#

# - Possible solutions if there were any null values:

#   - applying tree-based / kNN clf_models to fill NA values

#   - replacing null values with mean/mode values

#   - dropping features with 99% null values

#   - replacing null values with "-1" value == creating an isolated category

# In[3]:

display(
```

```

'Found {0} null values in transactions raw_dataset'.format(
    transactions_raw_data_main.isnull().sum().sum()
)
)
# ### Work on duplicated transactions
#
# - Drop duplicated rows
# - There is no need to store duplicated rows, even if they are Class=1 ('rare' target)
# In[4]:
display(
    'Duplicated rows, Class values frequency:',
    transactions_raw_data_main.loc[
        transactions_raw_data_main.duplicated(),
        'Class'
    ].value_counts()
)
transactions_raw_data_main = transactions_raw_data_main.drop_duplicates()
# ### Features normalization
#
# - All features except 'Amount' one are already normalized - fix this by applying StandardScaler to 'Amount' feature
# In[5]:
std_scaler = StandardScaler()
normed_amount = std_scaler.fit_transform(
    transactions_raw_data_main['Amount'].values.reshape(-1, 1)
)

```

```

transactions_raw_data_main['Amount'] = normed_amount

# In[6]:

display(

    'Normalized "Amount" feature stats:',

    transactions_raw_data_main['Amount'].describe()

)

# ### Log/sqrt/...-transformations

# In[7]:

# def overview_sqrt_skew_kurt(f_name):

#     plt.title('raw')

#     sns.distplot(

#         transactions_raw_data_main[f_name],

#         kde=True,

#         bins=50

#     )

#     plt.show()

#     plt.title('sqrt-transformed')

#     sns.distplot(

#         np.sqrt(transactions_raw_data_main[f_name] + 1),

#         kde=True,

#         bins=50

#     )

#     plt.show()

#     display(transactions_raw_data_main[f_name].skew(),
transactions_raw_data_main[f_name].kurt())

#     display(np.sqrt(transactions_raw_data_main[f_name] -
transactions_raw_data_main[f_name].min()).skew(),
np.sqrt(transactions_raw_data_main[f_name]).kurt())

```

```

# In[8]:

# V_features_to_transform = [

#   'V1', 'V2', 'V3', 'V5', 'V6', 'V7', 'V8', 'V10', 'V17', 'V20', 'V21', 'V23', 'V28'

# ]

# for col_name in V_features_to_transform:

#   transactions_raw_data_main[col_name] = np.log(transactions_raw_data_main[col_name] + 1)

# ### Work on correlations

#

# - Try to remove features which have weak correlation with target and weak cross-correlations

# In[9]:

target_pearson_correlations = transactions_raw_data_main.drop(columns=['Time']).corr()['Class']

# In[10]:

weak_correlation_feature_names = target_pearson_correlations[

    target_pearson_correlations.abs() < 0.001

].index

display(

    'Found {0} features with weak cross-correlation AND weak correlation with target:'.format(

        len(weak_correlation_feature_names)

    )

)

# In[11]:

transactions_raw_data_main_no_weak_corrs = transactions_raw_data_main.drop(

    columns=weak_correlation_feature_names

)

# ### Work on encoding by Information Value metric

#

```

- About IV:

- <https://medium.com/@sundarstyles89/weight-of-evidence-and-information-value-using-python-6f05072e83eb>

- https://www.listenraw_data.com/2015/03/weight-of-evidence-woe-and-information.html

In[12]:

```
good_client_label = 0
```

```
bad_client_label = 1
```

In[13]:

```
def get_range_woe_iv(all_feature_values: pd.DataFrame, range_values: pd.DataFrame) -> tuple:
```

```
    """
```

```
    Note: if in certain group there are no good / no bad clients - return WOE=0 and IV=0
```

```
    """
```

```
    # Number of good/bad clients for the whole group
```

```
    total_target_vc = all_feature_values['Class'].value_counts()
```

```
    total_bad_clients = total_target_vc[bad_client_label]
```

```
    total_good_clients = total_target_vc[good_client_label]
```

```
    # Number of good/bad clients for the current range
```

```
    group_target_vc = range_values['Class'].value_counts()
```

```
    try:
```

```
        group_bad_clients = group_target_vc[bad_client_label]
```

```
    except KeyError:
```

```
        return 0, 0 # better to return 0 rather than np.nan or np.inf
```

```
    try:
```

```
        group_good_clients = group_target_vc[good_client_label]
```

```
    except KeyError:
```

```
        return 0, 0 # better to return 0 rather than np.nan or np.inf
```

```
# Calculate "event pct" / "non event pct"

good_clients_distr = group_good_clients / total_good_clients

bad_clients_distr = group_bad_clients / total_bad_clients

# Calculate WOE and IV

woe = np.log(good_clients_distr / bad_clients_distr)

iv = (good_clients_distr - bad_clients_distr) * woe

return woe, iv
```

In[14]:

```
def recursive_get_range_woe_iv(all_feature_values: pd.DataFrame,
                               cur_possible_ranges: list,
                               cur_ranges_storage: list,
                               all_ranges_storage: list) -> list:
```

```
"""
```

Get:

- all possible combinations of ranges
- WOE and IV values on them

The ranges are saved in "global" all_ranges_storage.

The final ranges are also returned as recursive_get_range_woe_iv returning value

```
"""
```

```
for idx, next_range in enumerate(cur_possible_ranges):
```

```
    # Find out WOE and IV for each range.
```

```
    woe_first, iv_first = get_range_woe_iv(
```

```
        all_feature_values,
```

```
        all_feature_values.loc[
```

```
            (all_feature_values['col_name'] >= cur_possible_ranges[0]) &
```

```
            (all_feature_values['col_name'] <= next_range).....
```

Звіт подібності

метадані

Назва організації
Kyiv National Economic University named after Vadym Hetman KNEU

Заголовок
Ідентифікація ризиків онлайн-оплат за допомогою алгоритмів машинного навчання

Автор
Науковий керівник / Експерт
Онщенко Діана СергіївнаШевченко Анатолій Іванович

підрозділ
кафедра інформаційних систем в економіці

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.



Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв		4
Інтервали		0
Мікропробіли		0
Білі знаки		0
Парафрази (SmartMarks)		13

Подібності за списком джерел

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Колір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз			Копію тексту
ПОРЯДКОВИЙ НОМЕР	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)	
1	Прогнозування CTR рекламних кампаній методами інтелектуального аналізу даних 3/15/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)	31	0.24 %
2	http://csc.knu.ua/uk/filer/canonical/1506499576/411/	24	0.18 %

3	Розробка інтегрованої інформаційної системи нарахування заробітної плати на карткові рахунки 6/19/2020 Kyiv National Economic University named after Vadym Hetman KNEU (кафедра інформаційних систем в економіці)	20 0.15 %
4	Прогнозування CTR рекламних кампаній методами інтелектуального аналізу даних 3/15/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)	19 0.15 %
5	Прогнозування фродових транзакцій 3/15/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)	16 0.12 %
6	Корпоративні цінні папери на ринку капіталів 5/25/2020 Kyiv National Economic University named after Vadym Hetman KNEU (кафедра корпоративних фінансів і контролінгу)	16 0.12 %
7	http://csc.knu.ua/uk/filer/canonical/1506499576/411/	12 0.09 %
8	http://www.repository.hneu.edu.ua/bitstream/123456789/23300/1/%D0%A0%D0%9F%D0%94%D0%9D%202019-120%20%D0%91%D0%86%20%D0%9A%D0%BE%D1%80%D0%BE%D0%BB%D1%8C%D0%BE%D0%B2.pdf	11 0.08 %
9	Прогнозування фродових транзакцій 3/15/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)	11 0.08 %
10	http://csc.knu.ua/uk/filer/canonical/1506499576/411/	10 0.08 %
з бази даних RefBooks (0.00 %)		
ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ (ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ))
з домашньої бази даних (0.28 %)		
ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ (ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ))
1	Розробка інтегрованої інформаційної системи нарахування заробітної плати на карткові рахунки 6/19/2020 Kyiv National Economic University named after Vadym Hetman KNEU (кафедра інформаційних систем в економіці)	20 (1) 0.15 %
2	Корпоративні цінні папери на ринку капіталів 5/25/2020 Kyiv National Economic University named after Vadym Hetman KNEU (кафедра корпоративних фінансів і контролінгу)	16 (1) 0.12 %
з програми обміну базами даних (0.90 %)		
ПОРЯДКОВИЙ НОМЕР	ЗАГОЛОВОК	КІЛЬКІСТЬ (ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ))
1	Прогнозування CTR рекламних кампаній методами інтелектуального аналізу даних 3/15/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)	59 (3) 0.45 %

2	Прогнозування фродових транзакцій 3/15/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)	59 (7) 0.45 %
з Інтернету (0.56 %)		
ПОРЯДКОВИЙ НОМЕР	ДЖЕРЕЛО URL	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	http://csc.knu.ua/uk/filer/canonical/1506499576/411/	62 (5) 0.48 %
2	http://www.repository.hneu.edu.ua/bitstream/123456789/23300/1/%D0%A0%D0%9F%D0%94%D0%9D%202019-120%20%D0%91%D0%86%20%D0%9A%D0%BE%D1%80%D0%BE%D0%BB%D1%8C%D0%BE%D0%B2.pdf	11 (1) 0.08 %
Список прийнятих фрагментів (немає прийнятих фрагментів)		
ПОРЯДКОВИЙ НОМЕР	ЗМІСТ	КІЛЬКІСТЬ ОДНАКОВИХ СЛІВ (ФРАГМЕНТІВ)