Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук
(повна назва)
Кафедра Штучного інтелекту
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти перший (бакалаврський)

Інтелектуальна система виявлення шахрайства в онлайн-транзакціях з використанням ансамблевих методів машинного навчання
(тема)

Виконав:
здобувач четвертого року навчання,
групи ІТШІ-21-1
Сергій Хрістов
(власне ім'я, прізвище)

Спеціальність 122 Комп'ютерні науки
(код і повна назва спеціальності)
Тип програми освітньо-професійна
Освітня програма Штучний інтелект
(повна назва освітньої програми)
Керівник доц. Анастасія Дейнеко
(посада, власне ім'я, прізвище)

Допускається до захисту

Завідувач кафедри ШІ _____ Олег ЗОЛОТУХІН
(підпис) (власне ім'я, прізвище)

2025 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук

Кафедра Штучного інтелекту

Рівень вищої освіти перший (бакалаврський)

Спеціальність 122 Комп'ютерні науки
(код і повна назва)

Тип програми освітньо-професійна

Освітня програма Штучний інтелект
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«_____» _____ 20 ___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Хрістову Сергію Валерійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Інтелектуальна система виявлення шахрайства в онлайн-транзакціях з використанням ансамблевих методів машинного навчання

затверджена наказом університету від 19 травня 20 25 р. № 378Ст

2. Термін подання студентом роботи до екзаменаційної комісії 25 червня 20 25 р.

3. Вихідні дані до роботи Теоретичний матеріал щодо проблеми шахрайства в онлайн-транзакціях. Теоретичний матеріал щодо існуючих механізмів захисту. Статистичне порівняння існуючих моделей навчання. Прототип інтелектуальної системи для моніторингу онлайн-транзакцій

4. Перелік питань, що потрібно опрацювати в роботі
1) Проблема шахрайства в онлайн-транзакціях
2) Огляд методів виявлення шахрайських транзакцій
3) Експериментальні дослідження та розробка
4) Розробка прототипу інтелектуальної системи

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / терміни виконання етапів роботи	Примітка
1	Отримання завдання на кваліфікаційну роботу	19.05.2025	виконано
2	Аналіз предметної галузі	20.05.2025	виконано
3	Огляд існуючих рішень детекції	22.05.2025	виконано
4	Розробка інтелектуальної системи	27.05.2025	виконано
5	Написання пояснювальної записки	01.06.2025	виконано
6	Перевірка на академічний плагіат	23.06.2025	виконано
7	Нормоконтроль	23.06.2025	виконано
8	Підготовка презентації та доповіді	23.06.2025	виконано
9	Рецензування	23.06.2025	виконано
10	Захист перед ЕК	25.06.2025	виконано

Дата видачі завдання 19 травня 2025 р.

Здобувач _____ _____
(підпис)

Керівник роботи _____ доц. Анастасія Дейнеко
(підпис) (посада, власне ім’я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 54 с., 8 рис., 1 табл., 1 дод., 25 джерел.

АНСАМБЛЕВІ МЕТОДИ, КЛАСИФІКАЦІЯ, МАШИННЕ НАВЧАННЯ, ОНЛАЙН-ТРАНЗАКЦІЇ, ШАХРАЙСТВО, RANDOM FOREST, SMOTE, XGBOOST.

Об’єкт дослідження – процес виявлення шахрайських онлайн-транзакцій у фінансових системах.

Предмет дослідження – застосування ансамблевих методів машинного навчання для виявлення фінансового шахрайства.

Мета роботи – підвищення точності та надійності виявлення шахрайства в онлайн-транзакціях шляхом створення інтелектуальної системи з використанням ансамблевих моделей машинного навчання.

Методи дослідження – аналіз і обробка даних, машинне навчання, ансамблеве навчання (Random Forest, Gradient Boosting, XGBoost, LightGBM), аналіз ефективності моделей за допомогою метрик (Precision, Recall, ROC AUC), балансування даних (SMOTE).

У даній роботі розглядається розробка інтелектуальної системи для виявлення шахрайства в онлайн-фінансових транзакціях. Враховуючи актуальність проблеми, обрано сучасні ансамблеві методи машинного навчання, які забезпечують високу точність класифікації навіть у випадках незбалансованих вибірок. Було проведено повний цикл: від збору та підготовки даних до побудови та оцінювання моделей. Найкращі результати показала модель LightGBM із застосуванням методів балансування даних. Результати дослідження можуть бути використані для впровадження у фінансових установах.

ABSTRACT

Bachelor’s thesis contains: 54 pp., 8 fig., 1 tabl., 1 ann., 25 references.

CLASSIFICATION, ENSEMBLE METHODS, FRAUD, MACHINE LEARNING, ONLINE TRANSACTIONS, RANDOM FOREST, SMOTE, XGBOOST.

The object of research is the process of detecting fraudulent online transactions in financial systems.

The subject of the study is the application of ensemble machine learning methods to detect financial fraud.

Purpose – to increase the accuracy and reliability of fraud detection in online transactions by creating an intelligent system using ensemble machine learning models.

Research methods – data analysis and processing, machine learning, ensemble learning (Random Forest, Gradient Boosting, XGBoost, LightGBM), analysis of model performance using metrics (Precision, Recall, ROC AUC), data balancing (SMOTE).

This paper considers the development of an intelligent system for detecting fraud in online financial transactions. Given the relevance of the problem, modern ensemble machine learning methods have been chosen, which provide high classification accuracy even in cases of unbalanced samples. A full cycle was carried out: from data collection and preparation to model building and evaluation. The LightGBM model using data balancing methods showed the best results. The results of the study can be used for implementation in financial institutions.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

AI – Artificial Intelligence – штучний інтелект;

AUC – Area Under Curve – площа під кривою, метрика, що використовується для оцінювання якості класифікаційної моделі;

CSV – Comma-Separated Values – формат зберігання табличних даних у вигляді текстових файлів із розділенням значень комами;

FN – False Negative – хибно-негативне спрацьовування; випадок, коли шахрайство не було виявлено;

FP – False Positive – хибно-позитивне спрацьовування; випадок, коли звичайна транзакція помилково позначена як шахрайська;

F1-score – зважена середня точність і повнота; метрика, що балансує між false positives і false negatives;

ML – Machine Learning – машинне навчання, підгалузь AI, що передбачає створення алгоритмів, здатних навчатися на основі даних;

Precision – точність –відношення правильних позитивних прогнозів до загальної кількості позитивних прогнозів;

Recall – повнота –відношення правильно виявлених шахрайств до загальної кількості справжніх шахрайств;

RF – Random Forest – ансамблевий алгоритм машинного навчання на основі множини дерев рішень;

ROC – Receiver Operating Characteristic – графік, що відображає співвідношення між повнотою та хибнопозитивними результатами при різних порогах;

SMOTE – Synthetic Minority Over-sampling Technique – метод синтетичного збільшення обсягу класу меншості у незбалансованих вибірках;

TN – True Negative – істинно-негативне спрацьовування; транзакція правильно класифікована як чесна;

TP – True Positive – істинно-позитивне спрацьовування; транзакція правильно ідентифікована як шахрайська;

XGBoost – Extreme Gradient Boosting – потужний ансамблевий алгоритм бустингу рішень, широко застосовуваний для задач класифікації.

ВСТУП

У сучасному цифровому середовищі більшість фінансових операцій здійснюється в Інтернеті, що забезпечує користувачам зручність, швидкість і доступ до платіжних послуг у будь-який час. Однак зростання обсягу онлайн-транзакцій супроводжується збільшенням кількості фінансових шахрайств. Шахрайські операції завдають значних збитків як фізичним особам, так і фінансовим установам, що робить проблему їх своєчасного виявлення особливо актуальною.

Традиційні підходи до виявлення шахрайства, засновані на фіксованих правилах або простому статистичному аналізі, поступово втрачають свою ефективність. Вони не здатні швидко реагувати на нові типи атак і гнучко адаптуватися до змін у поведінці користувачів. У зв'язку з цим відбувся перехід до більш гнучких і потужних підходів, заснованих на машинному навчанні, які дозволяють будувати системи виявлення шахрайства з більш високим рівнем точності, здатні працювати в умовах великих обсягів даних і високої частоти транзакцій.

Останніми роками особлива увага приділяється методам ансамблевого машинного навчання, зокрема таким алгоритмам, як Random Forest, Gradient Boosting, LightGBM та XGBoost. Ці методи базуються на поєднанні декількох слабших моделей, що покращує загальну якість класифікації та зменшує кількість помилок. У випадку виявлення шахрайства, де дані часто є незбалансованими (тобто кількість шахрайських транзакцій становить дуже невелику частку від загальної кількості), ансамблеві підходи демонструють високу надійність та ефективність.

Метою цієї кваліфікаційної роботи є розробка інтелектуальної системи виявлення шахрайства в онлайн-транзакціях з використанням методів ансамблевого машинного навчання. Дослідження охоплює весь цикл побудови такої системи: від аналізу предметної галузі та вивчення

сучасних методів і інструментів до впровадження обраних моделей, обробки даних, збалансування вибірки та оцінки результатів.

Об'єктом дослідження є процес виявлення шахрайських онлайн-транзакцій у фінансових системах. Предметом дослідження є використання ансамблевих алгоритмів машинного навчання для створення ефективної системи класифікації транзакцій з метою виявлення шахрайських дій.

Практичне значення роботи полягає у створенні прототипу системи, який може бути адаптований для впровадження в банках, платіжних платформах та інших фінансових структурах, що працюють з великою кількістю транзакцій. Застосування таких рішень дозволяє зменшити фінансові втрати та підвищити довіру клієнтів до цифрових фінансових послуг.

1 ПРОБЛЕМА ШАХРАЙСТВА В ОНЛАЙН-ТРАНЗАКЦІЯХ

1.1 Втрати від онлайн шахрайства

Онлайн шахрайство стало однією з ключових загроз для сучасної цифрової економіки, суттєво впливаючи на стабільність фінансових систем, довіру споживачів і розвиток електронної комерції. Зі зростанням кількості цифрових транзакцій, поширенням мобільного банкінгу, контактних і безконтактних платіжних сервісів, а також широким використанням персональних пристроїв, кількість шахрайських атак продовжує зростати в геометричній прогресії. За оцінками міжнародних аналітичних центрів, глобальні фінансові втрати від інтернет-шахрайства досягли понад 10 мільярдів доларів у 2023 році, що майже на 25% більше порівняно з попереднім роком. У деяких країнах збитки від кібершахрайства вже перевищують втрати від традиційних економічних злочинів. Крім того, дедалі частіше спостерігається транснаціональний характер атак: злочинці працюють через розподілені мережі, використовуючи анонімні засоби зв’язку, VPN, криптовалюти, що ускладнює ідентифікацію та притягнення до відповідальності.

Для кращого розуміння масштабів впливу онлайн шахрайства варто розглянути його основні прояви та механізми. Найпоширенішими є фішинг (виманювання конфіденційної інформації під виглядом легітимних запитів), крадіжка платіжних даних (через злами баз даних, скімінг або шкідливе ПЗ), шахрайські інвестиційні проєкти (ICO, фіктивні біржі), зловмисне використання особистих даних (ідентичність, адреси, документи) та цифровий шантаж (ransomware, sextortion). Особливо загрозливими стали цільові атаки на малі та середні підприємства, які не мають належного технічного захисту та людських ресурсів для оперативного реагування. Водночас зростає кількість інцидентів, пов’язаних із використанням технологій штучного інтелекту – зокрема,

генерації фальшивих голосових повідомлень, підробки відео (deepfake), автоматичного створення переконливих фішингових листів. Такі інструменти дозволяють зловмисникам масштабувати атаки, робити їх персоналізованими та важкодетектованими. Це ставить нові виклики перед системами захисту, які мають не лише ідентифікувати підозрілу активність, але й вміти адаптуватися до мінливих патернів шахрайської поведінки.

На національному рівні втрати від онлайн шахрайства мають відчутний економічний ефект. Наприклад, за даними Національного банку України, лише в секторі електронних платежів у 2022 році було зафіксовано збитків на понад 480 млн грн. Більшість інцидентів пов’язана з соціальною інженерією та фішингом, які стають дедалі складнішими та персоналізованими (таблиця 1.1).

Крім прямих фінансових втрат, онлайн шахрайство завдає також репутаційних збитків компаніям, знижує довіру користувачів до цифрових сервісів та може викликати юридичні наслідки у разі витоку персональних даних. У складних випадках бізнеси вимушені інвестувати в додаткові системи захисту, що збільшує непрямі витрати.

Таблиця 1.1 – Динаміка втрат від онлайн шахрайства у світі

Рік	Глобальні втрати від онлайн шахрайства (млрд $)	Кількість зафіксованих інцидентів (млн)
2020	4.2	23.1
2021	6.4	31.7
2022	8.1	38.9
2023	10.2	45.6

Таким чином, втрати від онлайн шахрайства є не лише індикатором поточної кіберзагрози, а й важливою змінною при плануванні систем управління ризиками у цифровому середовищі.

1.2 Типи шахрайства в онлайн-транзакціях

Шахрайство у сфері онлайн-транзакцій є серйозним викликом для фінансових установ, оскільки охоплює широкий спектр зловмисних дій, що здійснюються як з боку зовнішніх осіб, так і через внутрішні загрози. З розвитком цифрових фінансових сервісів традиційні методи шахрайства доповнюються новими кіберзагрозами, які активно використовують вразливості платіжних систем, соціальну інженерію та автоматизовані атаки.

До поширених типів відносять фішинг, крадіжку облікових даних, зловживання платіжними інструментами, мультиакаунтинг та інсайдерські схеми. Кожна з форм шахрайства має власну логіку реалізації та створює різний рівень ризику, що вимагає застосування адаптивних і спеціалізованих підходів до виявлення таких транзакцій у режимі реального часу.

1.2.1 Внутрішнє шахрайство

Однією з найбільш складних для виявлення форм фінансових зловживань є внутрішнє шахрайство – дії, що здійснюються безпосередньо працівниками фінансових установ з використанням службового доступу. Незважаючи на відносно низьку частоту порівняно з масовими онлайн-атаками, внутрішнє шахрайство завдає значних збитків банкам через високий рівень доступу до критичних даних та інфраструктури. Такі дії можуть включати привласнення коштів, маніпуляції з рахунками клієнтів, несанкціоноване коригування кредитних умов, або незаконне використання персональної інформації.

Поширені приклади внутрішнього шахрайства включають:

– скасування або підміна транзакцій на вразливих або неактивних рахунках, зокрема рахунках літніх клієнтів;

– несанкціоновані зміни параметрів рахунку – модифікація кредитних лімітів, ставок або комісій з метою отримання особистої вигоди;

– використання конфіденційних даних для оформлення фіктивних кредитів, що в подальшому спричиняє збитки банку через відмову клієнта від зобов’язань;

– порушення процедур контролю – зокрема, обходи принципу «чотирьох очей», коли одна особа має змогу як ініціювати, так і схвалити транзакцію;

– співпраця між співробітниками різних відділів, що утворюють внутрішні схеми прикриття шахрайських операцій;

– цілеспрямовані IT-зловживання – надання тимчасових прав доступу до критичних систем з метою проведення підозрілих дій;

– крадіжка або витік клієнтських даних, які потім використовуються для несанкціонованих транзакцій або передаються на чорний ринок.

На відміну від зовнішніх атак, внутрішнє шахрайство складніше виявити за допомогою звичайних правил або класичних сигнатурних методів. У цьому контексті актуальними стають інструменти поведінкового аналізу та інтелектуальні системи, здатні виявляти атипові дії співробітників у транзакційній системі.

До основних стратегій мінімізації ризику внутрішнього шахрайства належать:

– використання персоналізованих облікових записів і журналювання адміністративних дій;

– моніторинг активності персоналу в режимі реального часу;

– поведінкове профілювання транзакцій, зокрема на неактивних або високоризикових рахунках;

– регулярні внутрішні аудити з використанням методів аналізу ризику;

– анонімні канали інформування про підозрілу активність (гарячі лінії, внутрішні портали);

– навчальні програми для персоналу з акцентом на корпоративну етику та відповідальність.

Впровадження таких заходів не лише знижує імовірність шахрайських дій з боку персоналу, а й сприяє підвищенню загального рівня довіри до фінансової установи. З огляду на ризики, які несе внутрішнє шахрайство, його виявлення має бути обов’язковим компонентом будь-якої системи моніторингу транзакцій, зокрема при побудові інтелектуальних рішень із використанням алгоритмів машинного навчання.

1.2.2 Зовнішнє шахрайство

Зовнішнє шахрайство становить одну з ключових загроз у сфері цифрових фінансових операцій. За даними Глобального опитування з питань економічного злочину та шахрайства (PwC, 2020), близько 40% зафіксованих випадків шахрайства були ініційовані сторонніми особами, тоді як ще приблизно 20% стали можливими через змову між внутрішніми і зовнішніми учасниками. Це свідчить про високу складність і масштаб зовнішніх загроз, які мають тенденцію до постійної еволюції та ускладнення методів атак.

Під зовнішнім шахрайством розуміють незаконні дії, що здійснюються клієнтами банку, зловмисниками, афілійованими структурами або третіми сторонами, які не є працівниками фінансової установи, але прагнуть отримати доступ до її ресурсів чи скористатися вразливостями інфраструктури з метою отримання неправомірної вигоди. В умовах активного розвитку онлайн-банкінгу, мобільних додатків і фінансових API зовнішнє шахрайство охоплює дедалі ширший спектр атак – від фальсифікації даних до автоматизованого викрадення коштів.

Основні типи зовнішнього шахрайства:

– фінансові маніпуляції – використання підроблених або викрадених документів для відкриття рахунків, оформлення платіжних інструментів чи ініціації грошових переказів. Сюди входить і шахрайство з чеками, а також спроби проходження KYC-процедур за фіктивними особами;

– кредитне шахрайство – оформлення кредитів або мікропозик на основі недостовірної інформації, зокрема із використанням особистих даних третіх осіб (ідентичне шахрайство). Часто здійснюється через тимчасові SIM-карти, віртуальні адреси або фейкові електронні підписи;

– шахрайство з електронними платіжними засобами – несанкціоноване використання банківських карток, електронних гаманців, зловживання механізмами безконтактної оплати, викрадення CVV-даних, клонування платіжних токенів;

– фішинг і соціальна інженерія – надсилання підроблених електронних листів, повідомлень або посилань, які імітують справжні банківські повідомлення з метою викрадення облікових даних;

– атаки на інтернет-банкінг та мобільні додатки – використання шкідливого ПЗ, троянів, ботів або проксі для перехоплення доступу до онлайн-сервісів клієнта.

Окрім безпосередніх фінансових втрат, зовнішнє шахрайство порушує довіру клієнтів до цифрових сервісів, спричиняє витрати на компенсації, правові процедури та модернізацію систем безпеки. Боротьба з такими загрозами вимагає впровадження багатоетапного захисту, здатного працювати в реальному часі.

Методи виявлення та протидії зовнішньому шахрайству:

а) посилення ідентифікаційних процедур:

– застосування мультифакторної автентифікації (MFA) при вході до акаунтів та здійсненні транзакцій;

– використання біометричних рішень, верифікації фото- та відеоідентифікації, систем відстеження IP-геолокації та пристроїв;

– інтеграція з державними базами даних для перевірки справжності документів;

2) аналітичний моніторинг транзакцій:

– використання машинного навчання для виявлення аномальних транзакцій на основі поведінкових моделей;

– аналіз шаблонів активності клієнтів: середня сума, частота операцій, час доби, тип пристрою;

– rule-based фільтрація підозрілих транзакцій з гнучкими параметрами ризику (наприклад, нестандартна геолокація або новий тип пристрою);

3) співпраця з іншими суб'єктами ринку:

– встановлення інформаційного обміну між банками, платіжними системами та міжбанківськими розрахунковими центрами для виявлення підозрілих сценаріїв;

– активна взаємодія з кіберполіцією, CERT-структурами, а також службами комплаєнсу для розслідування та запобігання шахрайству;

– застосування відкритих реєстрів шахрайських акаунтів (наприклад, blacklists IBAN або BIN), інтегрованих у внутрішні системи перевірки.

Комплексний підхід до виявлення зовнішнього шахрайства передбачає не лише побудову системи моніторингу, але й її адаптивність – здатність реагувати на нові типи атак шляхом оновлення моделей, правил та поведінкових шаблонів. У цьому контексті використання інтелектуальних систем класифікації транзакцій із застосуванням ансамблевих методів машинного навчання (Random Forest, XGBoost, LightGBM тощо) дозволяє ефективно відслідковувати складні шахрайські патерни навіть за умов змінної динаміки вхідних даних.

1.2.3 Цифрове шахрайство

Цифрове шахрайство є одним із найбільш динамічних і небезпечних векторів загроз у фінансовому секторі. У сучасному банківському середовищі це поняття охоплює будь-які шахрайські дії, здійснені з використанням цифрових технологій, включно з атаками на інформаційні системи банку, маніпуляціями в онлайн-каналах обслуговування, крадіжками цифрових ідентифікаторів і використанням шкідливого програмного забезпечення. У контексті онлайн-транзакцій, цифрове шахрайство виявляється особливо небезпечним, оскільки має високий рівень автоматизації, а його сліди часто важко відстежити у реальному часі.

Одним із найпоширеніших механізмів цифрового шахрайства залишається фішинг, коли зловмисники створюють підроблені електронні повідомлення або вебсторінки, що імітують офіційні банківські ресурси. Користувачеві пропонується перейти за «безпечним» посиланням, щоб нібито підтвердити свої дані, уникнути блокування рахунку чи переглянути важливе повідомлення. Отримавши облікові дані, зловмисник може увійти до реального банкінгу користувача та здійснити несанкціоновані операції.

Схожий підхід застосовується і у вішингу – шахрайстві на основі телефонного спілкування. Злочинці телефонують клієнтам під виглядом представників банку чи служби безпеки та, використовуючи термінову риторику, змушують їх розголошувати конфіденційну інформацію. Часто використовуються спеціально підготовлені сценарії для підвищення рівня довіри.

Ще однією формою соціальної інженерії є смішинг – обман через SMS-повідомлення. Жертвам надсилають короткі тексти з посиланням на фальшивий сайт банку або запитом на зворотній зв’язок. У результаті клієнт вводить дані для входу або коди підтвердження, що дозволяє шахраям ініціювати транзакції.

Окрім методів, спрямованих безпосередньо на користувачів, існує цілий набір атак на інфраструктуру банку. Зокрема, зломи внутрішніх систем, доступ до баз даних клієнтів, перехоплення платіжних повідомлень або модифікація параметрів транзакцій. Сучасні хакерські атаки часто мають складну багаторівневу архітектуру й використовують цілеспрямоване шкідливе ПЗ, спеціально адаптоване до банківських протоколів.

Окреме місце серед кіберзагроз займають так звані атаки «Man-in-the-Middle», коли шахрай перехоплює комунікацію між двома сторонами транзакції. Імітуючи одного з учасників, він змінює реквізити платежу, перенаправляючи кошти на власний рахунок. У банківських операціях така атака часто реалізується через підробку електронної адреси контрагента або втручання у листування між клієнтом та банком.

Серйозну небезпеку становлять експлойти у мобільних банківських додатках. Уразливості в таких застосунках можуть дозволити зловмисникам отримати доступ до функцій, які дозволяють перерахування коштів, зміну PIN-кодів, або навіть дистанційне керування рахунком користувача. Сюди ж відноситься поширення підроблених застосунків-імітацій, які копіюють зовнішній вигляд справжніх, але крадуть введені користувачем дані.

Поширеною тактикою цифрових атак є DoS-атаки (відмова в обслуговуванні), коли інфраструктура банку перевантажується великою кількістю запитів, що робить сервіси тимчасово недоступними. У деяких випадках це використовується як відволікаючий маневр, поки інша частина системи стає мішенню для цілеспрямованого вторгнення. Такі атаки часто здійснюються із застосуванням бот-мереж – інфікованих пристроїв користувачів, які централізовано керуються зловмисником.

Особливо критичним є те, що нові форми цифрового шахрайства постійно з’являються**.** Вони включають гібридні атаки з використанням глибоких фейків, автоматичну генерацію транзакцій на основі викрадених

шаблонів поведінки клієнтів, а також застосування генеративного штучного інтелекту для обходу перевірок.

Таким чином, цифрове шахрайство в умовах онлайн-фінансів є багатофакторною проблемою, яка вимагає від банків постійної адаптації засобів виявлення загроз. Застосування інтелектуальних систем моніторингу, здатних виявляти неочевидні закономірності, має ключове значення для забезпечення безпеки як окремих транзакцій, так і цифрової банківської системи в цілому.

1.3 Методи виявлення та протидії шахрайству

У контексті стрімкого зростання обсягів онлайн-платежів та активізації кібератак банки стикаються з необхідністю постійного вдосконалення засобів захисту від шахрайства. Виявлення та нейтралізація шахрайських дій стали не лише завданням служб безпеки, а й одним із пріоритетів цифрових стратегій у фінансовій галузі.

Сучасна система протидії шахрайству базується на поєднанні традиційних методів – таких як внутрішній контроль, багаторівнева авторизація та аудит – із інтелектуальними технологіями аналізу транзакцій у реальному часі. Таке поєднання забезпечує як оперативне виявлення підозрілої активності, так і стратегічну стійкість до нових схем зловживань. У наступних підрозділах буде розглянуто найбільш ефективні інструменти, що застосовуються для виявлення та запобігання шахрайству в цифровому банківському середовищі.

1.3.1 Традиційні методи протидії шахрайству

Традиційні підходи до протидії шахрайству в банківській сфері сформували фундамент сучасної системи фінансової безпеки. Попри зростання цифрових загроз, ці методи залишаються актуальними, оскільки

охоплюють широкий спектр управлінських, організаційних і технічних рішень, що спрямовані на мінімізацію ризиків як з боку клієнтів, так і з боку персоналу.

Однією з ключових складових традиційного захисту є система внутрішнього контролю та аудиту. Регулярний аудит операцій, ревізія процедур і перевірка аномальних транзакцій дозволяють виявляти слабкі місця, зловживання службовим становищем або несумісності в обліку. Водночас процедури верифікації клієнтів, що включають перевірку документів, ідентифікацію особи та оцінку платоспроможності, допомагають запобігти шахрайству з використанням фіктивних або викрадених даних.

Фізичні аспекти безпеки, зокрема охорона відділень, контроль доступу до архівів, захист паперової документації та зберігання активів, також залишаються важливою частиною. Окрему увагу приділяють навчанню персоналу – ознайомленню співробітників з типовими схемами шахрайства, внутрішніми політиками реагування та каналами анонімного інформування.

У традиційну модель безпеки входять також обмеження доступу до конфіденційної інформації, вимоги до підтвердження транзакцій за допомогою PIN-кодів, підписів чи фізичних документів, а також регулярне оновлення процедур з урахуванням поточних ризиків.

1.3.2 Використання технологій машинного навчання та штучного інтелекту

У сучасних умовах, коли методи фінансового шахрайства стають дедалі витонченішими, застосування технологій машинного навчання (ML) та штучного інтелекту (AI) відкриває нові можливості для своєчасного виявлення підозрілих дій і запобігання ризикам. Ці технології дозволяють аналізувати великі масиви фінансових та поведінкових даних, виявляти

приховані патерни, а також реагувати на шахрайські дії в режимі реального часу.

Моделі машинного навчання дедалі частіше застосовуються для аналізу транзакційної активності, де системи виявляють аномалії – нетипову частоту, географію чи обсяг операцій. Наприклад, транзакції в нетиповий час доби, в нових регіонах чи за участю незвичних контрагентів можуть автоматично ідентифікуватися як потенційно шахрайські.

Іншим напрямом є побудова графових структур, які відображають зв’язки між клієнтами, рахунками, пристроями та локаціями. Алгоритми виявлення кластерів і відхилень у таких структурах дозволяють виявляти організовані шахрайські мережі, змови або багаторазове використання одних і тих самих схем з різними обліковими даними.

Технології ML також ефективно працюють з неструктурованими даними – наприклад, текстами звернень клієнтів, електронними листами чи публікаціями в соцмережах. Виявлення в них ключових слів або аномальних емоційних контекстів може сигналізувати про шахрайські наміри або фіктивні звернення.

Додатково, моделі верифікації особистості – зокрема розпізнавання обличчя, аналіз біометричних даних або перевірка документів – використовуються для боротьби з крадіжкою ідентичності. Ці моделі здатні адаптуватися до нових спроб обману, оскільки постійно навчаються на нових прикладах.

Штучний інтелект, у свою чергу, забезпечує більш високий рівень автоматизації та контекстного розуміння, включаючи обробку природної мови, прогнозування ризиків та керування сценаріями реагування. AI-системи можуть не лише виявити загрозу, а й автоматично ініціювати відповідні дії – наприклад, блокування транзакції, відправку попереджень клієнту або запуск внутрішнього розслідування.

Також активно впроваджуються віртуальні асистенти та чат-боти, здатні вести контекстно чутливу комунікацію з клієнтами, і водночас фіксувати ознаки шахрайської поведінки або невідповідності у відповідях.

Інтеграція AI-моделей дозволяє здійснювати прогностичний аналіз, на основі якого система формує оцінку ризику для кожного користувача чи транзакції. Це дозволяє не лише реагувати на інциденти, а й запобігати їм заздалегідь.

Таким чином, поєднання технологій машинного навчання та штучного інтелекту створює основу для адаптивної, масштабованої та самонавчальної системи протидії шахрайству, яка значно перевершує традиційні ручні підходи за швидкістю, точністю та здатністю до самовдосконалення. Проте ефективність таких рішень досягається саме в комплексі з класичними методами – тільки багаторівнева інтегрована стратегія дозволяє повноцінно протистояти сучасним загрозам у сфері фінансових транзакцій.

1.3.3 Заходи кібербезпеки

У цифрову епоху, коли банківські операції значною мірою здійснюються через мережу Інтернет, кібербезпека стає критично важливою складовою стратегії протидії шахрайству. Порушення захисту інформаційних систем може призвести до витоку конфіденційних даних, несанкціонованого доступу до рахунків та серйозних фінансових втрат. Тому банки впроваджують комплексні заходи кіберзахисту, які охоплюють як технічні інструменти, так і організаційні політики.

Одним із базових напрямів є зміцнення мережевої інфраструктури. Для цього застосовуються системи виявлення та запобігання вторгненням (IDPS), брандмауери, а також сегментація внутрішніх мереж, що дозволяє локалізувати можливі загрози й обмежити їх поширення. Важливою є також регулярна підтримка актуального стану всіх систем

безпеки: оновлення програмного забезпечення, застосування патчів, тестування на вразливості.

Особливу увагу банки приділяють захисту клієнтських даних. Для цього використовується шифрування як у процесі передавання, так і при збереженні інформації. Впроваджуються багаторівневі механізми аутентифікації – наприклад, комбінація паролів, одноразових кодів та біометричних даних. Такі підходи суттєво ускладнюють несанкціонований доступ навіть у разі викрадення окремих елементів ідентифікації.

Крім технічних заходів, важливу роль відіграє людський фактор. Регулярні навчання співробітників з питань інформаційної безпеки, симуляції фішингових атак та інструктажі щодо дій у разі кіберінциденту формують культуру відповідального ставлення до захисту даних. Водночас банки створюють чіткі процедури реагування на інциденти – з алгоритмами фіксації, локалізації, усунення наслідків і звітності.

Таким чином, заходи кібербезпеки є не лише технологічною потребою, а й стратегічною складовою банківської стабільності. Їх реалізація дозволяє виявляти та нейтралізовувати спроби цифрового шахрайства на ранніх етапах, зберігаючи довіру клієнтів та забезпечуючи стійкість до зовнішніх загроз.

1.4 Особливості шахрайства в онлайн-транзакціях

Шахрайство в онлайн-транзакціях є одним із найдинамічніших і найнебезпечніших викликів для сучасних фінансових установ. На відміну від традиційних форм шахрайства, де зловмисники вдаються до фізичних дій або безпосереднього втручання у фінансові процеси, онлайн-шахрайство здійснюється через цифрові канали з використанням складних технічних засобів та високого рівня анонімності. Ця категорія шахрайства охоплює широкий спектр дій, спрямованих на незаконне отримання доступу

до рахунків, маніпулювання платіжними системами або викрадення персональних і фінансових даних з метою їх подальшого використання.

Однією з ключових особливостей шахрайства в онлайн-транзакціях є висока швидкість виконання операцій. Транзакції можуть здійснюватися в режимі реального часу, що значно ускладнює своєчасне виявлення шахрайської активності. Навіть незначна затримка у реагуванні з боку банку може призвести до втрати значних сум коштів. Зловмисники, користуючись вразливостями систем, можуть за лічені секунди переказати кошти через кілька посередників або використати підставні рахунки, після чого встановити відстеження руху практично неможливо.

Іншим важливим аспектом є використання спеціалізованих автоматизованих скриптів і ботів, що здатні масово виконувати транзакції або генерувати запити до серверів банківських систем. Такі дії часто маскуються під поведінку легітимного користувача, що суттєво ускладнює їх виявлення за допомогою простих порогових правил або класичних механізмів верифікації. Крім того, сучасні шахрайські схеми нерідко передбачають імітацію транзакційної активності клієнта: зловмисники ретельно копіюють часові патерни, географічні точки доступу, середні суми операцій тощо, що дозволяє їм залишатися непоміченими для стандартних систем моніторингу.

Також слід враховувати, що більшість шахрайських дій в онлайн-просторі здійснюється без фізичної присутності або контакту з працівниками банку, що значно ускладнює верифікацію особи. Атаки часто будуються на компрометації облікових даних (логінів, паролів, OTP-кодів), які отримуються за допомогою фішингу, соціальної інженерії або шкідливого програмного забезпечення. Унаслідок цього виникає необхідність побудови систем, здатних автоматично розпізнавати аномальні шаблони поведінки навіть тоді, коли шахрай використовує справжні облікові дані користувача.

Ще однією критичною особливістю є високий рівень анонімності злочинців. Використання віртуальних приватних мереж (VPN), TOR, тимчасових адрес електронної пошти, а також численних акаунтів-фантомів значно ускладнює ідентифікацію зловмисника та джерела шахрайських транзакцій. У багатьох випадках шахрайські дії здійснюються з територій, де банківська юрисдикція має обмежений вплив або взагалі відсутня, що унеможливлює ефективне правове переслідування.

Окрему увагу слід приділити масштабованості шахрайства в онлайн-середовищі. Якщо у традиційних умовах зловмисники були обмежені фізичним доступом або необхідністю персонального втручання, то в онлайн-банкінгу можлива паралельна атака на тисячі облікових записів за допомогою автоматизованих інструментів. Це зумовлює потребу у впровадженні систем виявлення, здатних обробляти великі обсяги даних у режимі реального часу, швидко виявляти аномалії та ініціювати превентивні дії ще до завершення шахрайської транзакції.

Отже, специфіка онлайн-шахрайства потребує нових підходів до побудови систем захисту, орієнтованих на швидкість, масштабованість, точність та здатність до самонавчання. Саме тому зростає інтерес до застосування інтелектуальних методів виявлення шахрайства, зокрема заснованих на ансамблевих моделях машинного навчання, які можуть ефективно працювати з високорозмірними транзакційними даними та адаптуватися до постійно змінюваних схем атак. У подальших розділах буде детальніше розглянуто особливості побудови таких моделей, їх архітектуру, принципи роботи та результати експериментального дослідження.

1.5 Проблеми автоматичного виявлення шахрайства в онлайн-транзакціях

Автоматичне виявлення шахрайства в онлайн-транзакціях є однією з найбільш критичних задач у сучасній банківській сфері. Попри широке

впровадження інструментів аналітики та алгоритмів машинного навчання, системи протидії шахрайству стикаються з низкою викликів, які обумовлені як технологічними обмеженнями, так і поведінковими характеристиками самих зловмисників. Розуміння цих проблем є необхідною умовою для побудови ефективних захисних систем, здатних оперативно реагувати на нові типи загроз.

Однією з основних проблем є висока динаміка та еволюція шахрайських схем. Шахраї постійно змінюють свої тактики, використовуючи нові канали зв’язку, обхідні шляхи автентифікації, атаки через мобільні застосунки або API. Схеми, які виявлялися ефективними ще декілька місяців тому, можуть повністю втратити актуальність у поточному середовищі. У таких умовах традиційні фільтри або жорстко закодовані правила не дають очікуваного результату, а системи, побудовані на основі машинного навчання, потребують постійного оновлення та донавчання на нових даних.

Ще однією важливою проблемою є дисбаланс у даних. У більшості реальних банківських систем частка шахрайських транзакцій є дуже низькою – зазвичай менше 1%. Це створює серйозні труднощі для алгоритмів машинного навчання, оскільки моделі можуть схилятися до «оптимальної», але непотрібної стратегії – класифікувати всі транзакції як легітимні. Застосування традиційних метрик точності в таких умовах не дає об'єктивного уявлення про якість класифікатора, тому необхідно використовувати спеціалізовані метрики, як-от precision, recall, F1-score, area under ROC/PR curve. Також потрібне застосування методів балансування класів, таких як oversampling, undersampling, SMOTE або генеративні підходи.

Важливим обмеженням є неоднорідність та складність вхідних даних. Транзакційні дані можуть мати різні формати, джерела та частоту оновлення. Окрім класичних числових ознак (сума, час, валюта, місцезнаходження), сучасні системи повинні опрацьовувати текстову

інформацію (наприклад, призначення платежу), графові структури зв’язків між користувачами, метадані з пристроїв, IP-адреси, тип браузера, а також поведінкові патерни. Інтеграція таких різнорідних даних у єдиний вектор ознак вимагає складного препроцесингу, нормалізації, побудови ембедингів та агрегування у реальному часі.

Ще один виклик – обмеженість пояснюваності моделей. Багато сучасних алгоритмів, зокрема ансамблеві або нейронні мережі, виступають як «чорні ящики», результат яких важко пояснити кінцевому користувачу або службі безпеки банку. У випадках автоматичного блокування транзакцій необхідна можливість обґрунтувати причину відхилення. Це особливо важливо в контексті фінансової відповідальності, судових спорів або перевірок регулятора. У зв’язку з цим, навіть при високій точності моделей, банки нерідко змушені застосовувати менш складні, але більш інтерпретовані алгоритми (логістична регресія, дерева рішень) або використовувати XAI-технології (Explainable AI), такі як SHAP, LIME, attention heatmaps.

Реактивність системи – ще один критичний аспект. Через високу швидкість проведення онлайн-транзакцій системи виявлення шахрайства повинні працювати з мінімальними затримками. При цьому вони повинні встигати не тільки проаналізувати нову транзакцію, але й, за необхідності, зробити запит до історичних даних клієнта, збудувати поведінкову модель та зіставити її з поточним шаблоном. Забезпечення такої низької латентності часто вимагає складної інфраструктури — швидких баз даних, розподілених обчислень та кешування обробки профілів користувачів.

Крім технічних труднощів, автоматичні системи виявлення шахрайства також зіштовхуються з юридичними та етичними обмеженнями. Наприклад, використання персональних або чутливих даних (геолокація, біометрія, історія пристроїв) часто потребує згоди користувача або проходження регуляторних процедур. Надмірно жорсткі системи фільтрації можуть призвести до високої кількості false positives, що

спричиняє незадоволення клієнтів, погіршення користувацького досвіду та втрату довіри до банку. Баланс між точністю виявлення та збереженням лояльності клієнтів є ключовим завданням у проектуванні таких систем.

Окремо варто згадати про ускладнення перевірки гіпотез та налаштування моделей. У звичайних задачах машинного навчання можна експериментувати з різними архітектурами, гіперпараметрами, наборами ознак та метриками. Проте у сфері фінансової безпеки доступ до реальних транзакційних даних обмежений через конфіденційність і комерційну таємницю. Це створює потребу у використанні синтетичних або анонімізованих датасетів, які не завжди відображають усю складність реального середовища.

Таким чином, побудова ефективної системи автоматичного виявлення шахрайства в онлайн-транзакціях є складною багаторівневою задачею, яка виходить за межі звичайної класифікації. Вона потребує не лише глибоких технічних рішень, а й розуміння специфіки предметної галузі, користувацької поведінки, правових рамок та ризиків. У наступних розділах буде представлено аналіз підходів, що базуються на ансамблевих моделях машинного навчання, які демонструють високу ефективність в умовах високої динаміки загроз та обмеженості достовірних міток у вхідних даних.

Ще одним критичним викликом є нестабільність ознак та концепт-дрейф. У сфері онлайн-транзакцій користувацька поведінка змінюється не лише під впливом шахраїв, але й через сезонні фактори, зміну платіжних звичок або впровадження нових технологій. Це призводить до того, що модель, навчена на історичних даних, може швидко втратити релевантність. Наприклад, під час розпродажів або святкових періодів обсяги транзакцій та їх географія суттєво змінюються, що ускладнює розпізнавання аномалій. Для боротьби з цим явищем необхідне регулярне оновлення моделей, моніторинг стабільності розподілів ознак, використання методів online learning або drift detection.

Обмежена кількість позитивних прикладів також ускладнює розробку ефективних моделей. Оскільки реальні шахрайські транзакції трапляються рідко, навіть великі банки можуть мати лише декілька тисяч прикладів у вибірці, у той час як легітимних транзакцій – мільйони. Це перешкоджає повноцінному використанню глибоких моделей, які потребують великої кількості даних для навчання, і підштовхує до застосування методів transfer learning, semi-supervised learning або генерації синтетичних зразків через GAN чи інші моделі.

Варто також підкреслити проблему обмеженого часу на прийняття рішення. Система має ухвалити рішення про легітимність транзакції протягом декількох секунд або навіть мілісекунд. Це виключає можливість ручної верифікації або довготривалих обчислень. У таких умовах моделі мають бути не лише точними, а й достатньо легкими, щоб їх можна було розгорнути у продакшн-середовищі без затримок. Рішенням можуть бути попередньо скомпільовані моделі (ONNX, TorchScript), використання моделей лайт-класу (наприклад, LightGBM), або мікросервісна архітектура з кешуванням.

Протидія адаптивним атакам – ще один виклик. Шахраї можуть навмисно тестувати межі системи: змінювати поведінку, щоб обійти фільтри, або навіть виконувати adversarial атаки на моделі машинного навчання, навмисно генеруючи приклади, які вводять модель в оману. Це особливо актуально для публічних API або платіжних платформ із відкритим інтерфейсом. Для захисту від таких сценаріїв застосовують методи adversarial training, побудову ансамблів моделей з різною чутливістю або системи додаткової перевірки на основі поведінкової біометрії.

Недостатня узгодженість між підсистемами також може стати джерелом вразливості. У великих банках різні елементи інфраструктури – системи автентифікації, транзакційного моніторингу, клієнтської підтримки – можуть функціонувати незалежно. У результаті між ними відсутня єдина картина подій, що унеможливлює ефективне об'єднання

даних та ускладнює виявлення складних шахрайських схем. Проблему вирішують шляхом впровадження централізованих платформ моніторингу або Data Lake архітектур, які агрегують та синхронізують події в реальному часі.

Також не слід ігнорувати людський фактор у побудові моделей. Неправильно обрані ознаки, некоректна валідація, недооцінка категоріальних змінних або надлишкова фільтрація «сумнівних» прикладів можуть призвести до переобучення або упередженої поведінки моделі. Відомі випадки, коли моделі демонстрували дискримінацію за регіоном, віком чи типом пристрою через некоректну інтерпретацію кореляцій. Це потребує особливої уваги до етичного аудиту моделей, fairness-аналізу та використання explainable AI підходів.

Нарешті, проблема реальної інтеграції моделей у бізнес-процеси – ще один бар’єр. Навіть найточніша модель виявлення шахрайства не матиме цінності, якщо вона не інтегрована у життєвий цикл транзакції, не має каналу для втручання або не супроводжується політиками реагування. Ефективна реалізація потребує не лише технічної розробки, але й узгодження з юридичним відділом, службою підтримки, відділом ризиків, а також побудови звітності для подальшого аудиту.

Таким чином, автоматичне виявлення шахрайства в онлайн-транзакціях є мультидисциплінарною задачею, що вимагає поєднання сучасних технологій, операційного досвіду, обчислювальних ресурсів та гнучкої адаптації до динамічних умов. Розробка ефективної системи виявлення шахрайства повинна спиратися на поетапне впровадження: від попереднього аналізу даних до побудови архітектури, навчання моделей, контролю їх стабільності та постійного моніторингу у продакшн-середовищі. Тільки такий підхід дозволить зменшити збитки, підвищити довіру клієнтів та забезпечити відповідність сучасним вимогам фінансової безпеки.

2 ОГЛЯД МЕТОДІВ ВИЯВЛЕННЯ ШАХРАЙСЬКИХ ТРАНЗАКЦІЙ

2.1 Методи машинного навчання

Методи машинного навчання відіграють ключову роль у побудові ефективних систем виявлення шахрайства в онлайн-транзакціях. Вони здатні самостійно розпізнати як і звичайні незаконні схеми, так і складні та неочевидні закономірності в даних. Це особливо важливо в умовах, коли шахраї змінюють свої тактики, а традиційні підходи швидко втрачають актуальність.

У 2023 році, за даними Національного банку, було здійснено 7 397,2 мільйона безготівкових операцій на суму 3 980,0 млрд грн. У більшості випадків завдання виявлення шахрайства формується як бінарна класифікація, де кожна транзакція має значення: шахрайська (1) або легітимна (0). Навчальна вибірка складається на основі історичних даних із логів транзакцій, тож основна мета моделі – навчитись розділяти ці два класи з максимальною точністю та мінімізувати при цьому кількість хибно-позитивних та хибно-негативних рішень і важливим фактором є можливість моделі працювати з великим об’ємом даних.

Основні типи алгоритмів:

– логістична регресія. Це базовий статистичний метод, що широко використовується як базова модель через свою простоту, швидкість і інтерпретованість. Логістична регресія обчислює ймовірність належності об’єкта до класу 1 на основі лінійної комбінації ознак. Проте вона обмежена в здатності моделювати нелінійні залежності;

– дерева рішень. Дерева рішень розбивають простір ознак на підмножини на основі умовних переходів, що ґрунтуються на значеннях атрибутів. Вони добре працюють з категоріальними та числовими даними, а також забезпечують високу інтерпретованість;

– метод опорних векторів. Цей метод шукає гіперплощину, яка максимізує відстань між класами. Добре працює в задачах з високою розмірністю, проте чутливий до вибору гіперпараметрів і масштабів даних. Через високу обчислювальну складність рідко застосовується у великих транзакційних системах у реальному часі;

– наївний баєсівський класифікатор. Простий і швидкий у реалізації, базується на застосуванні теореми Байєса під припущенням незалежності ознак. Попри спрощення, може бути ефективним на слабоструктурованих даних, але зазвичай поступається сучасним ансамблевим моделям за точністю.

Кожна з вище перелічених моделей має свої переваги та недоліки, але ми стикаємося з проблемами, які повинні бути вирішеними одночасно. По-перше, є висока нерівноважність класів у даних – кількість шахрайських транзакцій зазвичай на кілька порядків менша за кількість легітимних. Це призводить до складнощів у навчанні моделей і підвищує ризик хибно-негативних результатів. Крім того, шахрайські дії часто маскуються під звичайну поведінку користувача, що знижує ефективність традиційних систем навчання. По-друге, Шахрайські схеми постійно змінюються, тому модель дуже швидко застаріває, що потребує постійного перенавчання моделі. Також для таких система важливо приймати рішення в режимі реального часу, мому необхідно шукати компроміс між точністю та швидкодією моделі.

2.2 Ансамблеві методи

Ансамблеві методи стали однією з найефективніших категорій моделей машинного навчання для вирішення задач виявлення шахрайства. Їхня ефективність пояснюється здатністю поєднувати велику кількість простих (базових) моделей у складну систему, яка демонструє високу узагальнюючу здатність, тобто добре працює не лише на навчальних, але й

на нових, невідомих даних. У порівнянні з окремими моделями, ансамблі, як правило, мають вищу узагальнюючу здатність та кращу стійкість до шумів. У своїй основі ці методи спираються на дві стратегії: бутстрепне агрегування (bagging) та послідовне навчання (boosting), що визначає відмінності між конкретними реалізаціями.

2.2.1 Поняття Bagging та Boosting

Bagging – це техніка ансамблевого навчання, яка базується на ідеї зменшення варіації моделі шляхом побудови кількох незалежних базових моделей (часто дерев рішень) на випадкових підмножинах даних, після чого об'єднуються їхні передбачення.

Принцип роботи bagging полягає в наступному: на основі початкового набору даних випадково з поверненням (тобто з можливим повторенням одних і тих самих прикладів) формуються кілька нових підмножин даних. Кожна з цих підмножин використовується для тренування окремої моделі. Це називається Bootstrap. Після цього всі моделі використовуються для прогнозування, а їхні результати агрегуються – у задачах класифікації, як правило, шляхом більшості голосів (majority voting).

Головна перевага bagging полягає в тому, що він знижує варіативність моделі, тобто зменшує ризик перенавчання, не збільшуючи значно упередження. Це досягається завдяки тому, що кожна модель бачить дещо інший розподіл даних, і в результаті модель загалом стає більш стійкою до випадкових коливань у даних.

Типовим представником методів bagging є Random Forest, де використовується набір дерев рішень, кожне з яких будується на випадковій підмножині об'єктів та ознак. Random Forest зберігає здатність моделювати складні нелінійні зв’язки, але при цьому зменшує надмірну чутливість окремих дерев до шуму (рисунок 2.1).

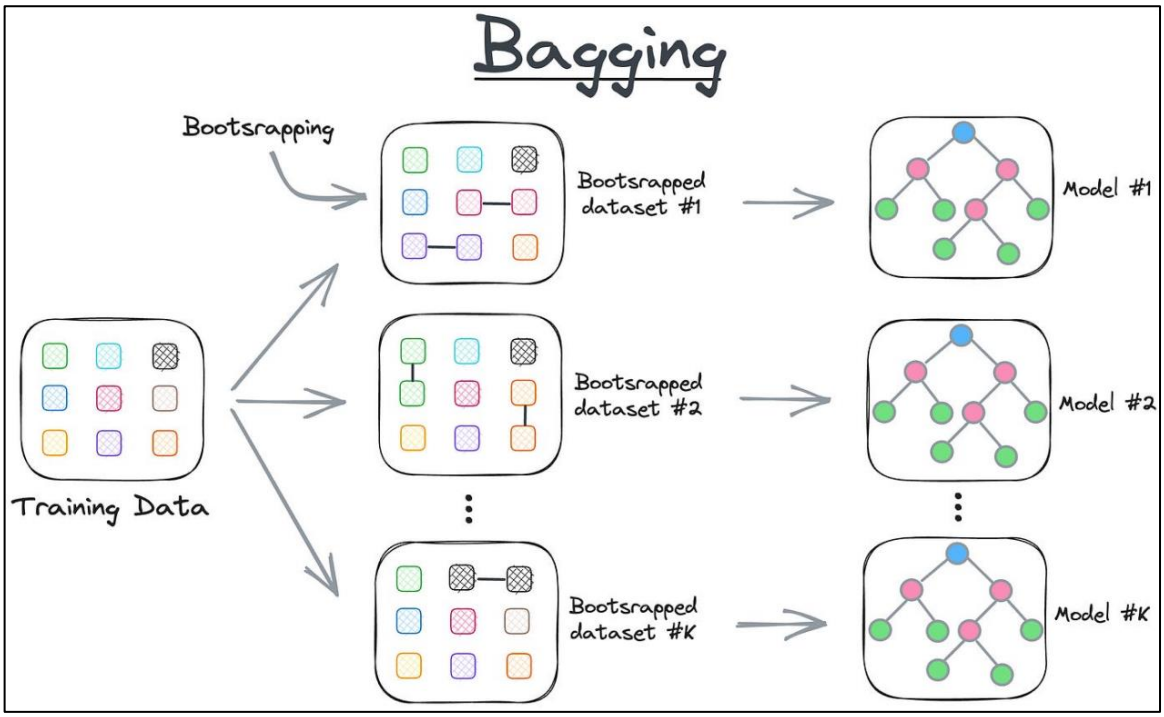

Рисунок 2.1 – Принцип роботи методу bagging

У задачах виявлення шахрайства bagging добре працює в умовах, коли система має справу з великою кількістю ознак, але хоче уникнути перенавчання на незначущі патерни. Також цей підхід дозволяє ефективно використовувати паралельні обчислення, що пришвидшує процес навчання.

Boosting – це інша стратегія ансамблювання, яка навпаки зменшує упередження моделей, поступово нарощуючи складність композиції за рахунок послідовного навчання. Ідея boosting полягає в тому, щоб навчати моделі послідовно – кожна наступна модель намагається скоригувати помилки, зроблені попередніми.

На першому етапі навчається проста модель на початковому наборі даних. Далі помилки цієї моделі аналізуються, і наступна модель фокусується саме на прикладах, де були допущені помилки. Таким чином, кожна наступна модель отримує інформацію про те, де її попередники були слабкими, і намагається ці слабкі місця виправити. В результаті виходить сильна модель – комбінація багатьох слабких прогнозів, які доповнюють один одного (рисунок 2.2).

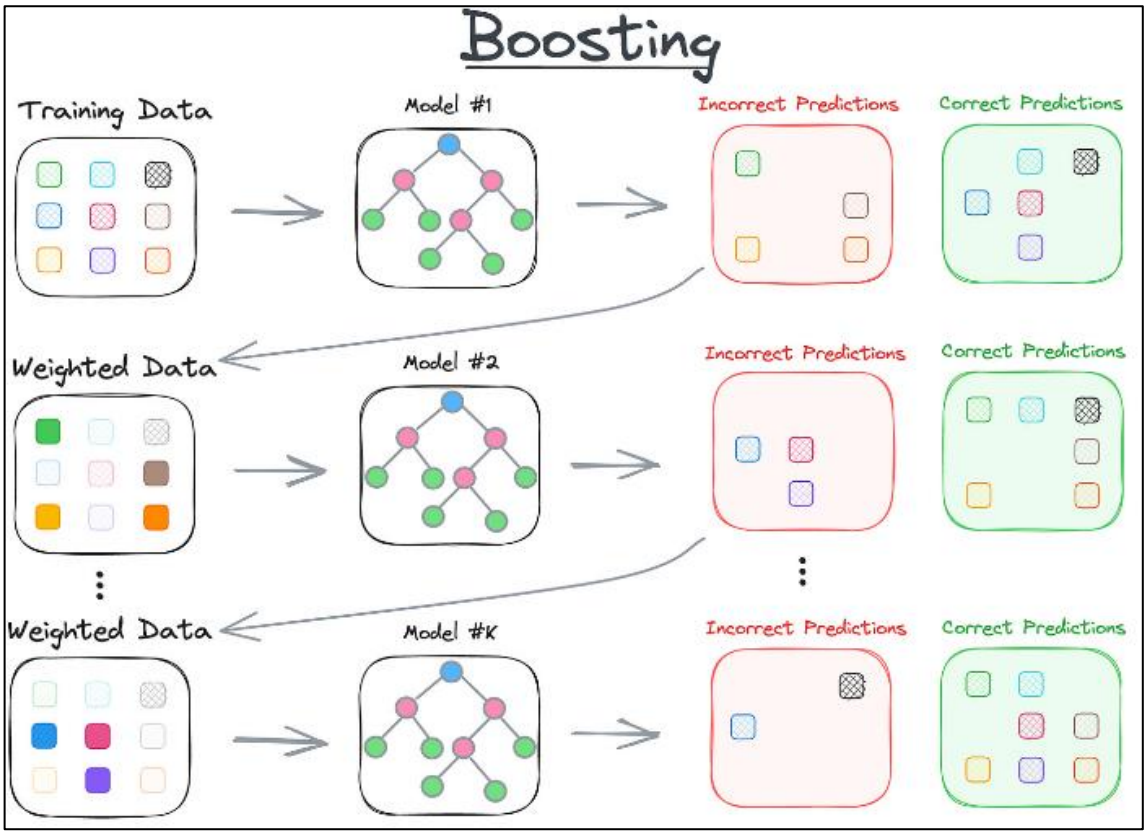

Рисунок 2.2 – Принцип роботи методу boosting

У підсумку, bagging робить модель стабільнішою та менш чутливою до шуму за рахунок паралельного навчання і зменшення дисперсії, а boosting підвищує точність за рахунок послідовного усунення помилок і зменшення упередження.

2.2.2 Random Forest

Random Forest – це класичний приклад методу bagging, де велика кількість дерев рішень навчаються паралельно. Кожне дерево створюється на випадковій підмножині навчального набору даних, причому випадково обираються як приклади (спостереження), так і ознаки, які використовуються під час побудови дерева. Це дозволяє зменшити кореляцію між деревами, що в підсумку призводить до більш стабільної та надійної моделі.

Після навчання всі дерева «голосують» за підсумкове рішення, а результат визначається як більшість голосів. Основна перевага Random Forest полягає у високій стійкості до перенавчення та хорошій інтерпретованості, оскільки можна легко оцінити важливість кожної ознаки. Цей метод добре працює з табличними даними різних типів і здатен ефективно обробляти відсутні значення. Проте, попри універсальність, він не завжди забезпечує найвищу точність і може бути менш чутливим до слабких патернів у даних порівняно з boosting моделями. Також із зростанням кількості дерев зростають вимоги до обчислювальних ресурсів.

2.2.3 Gradient Boosting

На відміну від Random Forest, Gradient Boosting реалізує ідею послідовного навчання, коли кожна нова модель навчається на помилках попередньої. Після першого дерева оцінюється похибка класифікації, і наступне дерево намагається компенсувати цю похибку. Цей процес повторюється багато разів, поки не буде досягнуто стабільного покращення.

Суть методу полягає у мінімізації певної функції втрат, зазвичай логарифмічної або квадратичної, шляхом додавання нових слабких моделей, що рухаються в напрямку градієнта похибки. Основною перевагою Gradient Boosting є висока точність моделювання навіть на складних, нерівномірних даних.

Цей метод здатен вловлювати складні залежності, які не доступні для простих дерев. Водночас він має серйозні обмеження: процес навчання є повільним, потребує значної кількості часу і ресурсів, а також вимагає тонкого налаштування гіперпараметрів, таких як глибина дерев, кількість ітерацій та швидкість навчання. Якщо ці параметри підібрані невдало, модель може легко перенавчитися або навпаки – виявитися недостатньо потужною.

2.2.4 XGBoost (eXtreme Gradient Boosting)

Модель XGBoost є вдосконаленням класичного бустингу, в якому було реалізовано кілька важливих оптимізацій. По-перше, вона використовує регуляризацію для зменшення ризику перенавчення, що робить її більш стійкою до шумових даних. По-друге, алгоритм навчання реалізований таким чином, що дозволяє паралельно обробляти окремі вузли дерев, завдяки чому досягається значне пришвидшення. Крім того, XGBoost ефективно працює з відсутніми значеннями, автоматично знаходячи оптимальні напрямки для їх обробки у дереві.

Також реалізована підтримка роботи з великими об’ємами даних як на CPU, так і на GPU, що розширює можливості практичного застосування. Основною перевагою XGBoost є баланс між точністю, продуктивністю та гнучкістю налаштувань. Саме тому ця модель часто використовується як еталонна в практиці Data Science і є однією з найуспішніших у конкурсах на платформах на зразок Kaggle. Проте, як і в будь-якому бустинговому методі, процес налаштування може бути складним, а модель – важкою для інтерпретації.

2.2.5 LightGBM

Найновішим представником серед розглянутих методів є LightGBM, розроблений компанією Microsoft для вирішення проблем продуктивності традиційного boosting. Головною його інновацією є використання leaf-wise росту дерев замість level-wise, як це реалізовано в інших бібліотеках. Завдяки цьому деревам дозволяється рости в глибину там, де спостерігається найбільше зменшення функції втрат, що забезпечує більш точну модель при меншій кількості дерев. Додатково модель використовує histogram-based підхід для дискретизації числових ознак, що значно зменшує обчислювальні витрати. Ще однією сильною стороною є вбудована

підтримка ознак категорій без необхідності ручного кодування, що спрощує попередню обробку даних. Завдяки всім цим оптимізаціям LightGBM демонструє дуже високу швидкість навчання, низьке споживання пам’яті та конкурентну точність. Особливо ефективною ця бібліотека є при роботі з великими наборами даних або у випадках, коли критично важлива швидка обробка. Проте, оскільки leaf-wise ріст може призводити до надмірної складності дерев, існує ризик перенавчення на малих або шумних даних. Крім того, модель менш інтерпретована, ніж класичні дерева або логістична регресія, що створює додаткові труднощі при роботі в регульованих сферах, таких як фінансовий сектор.

3 ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ ТА РОЗРОБКА

3.1 Критерії оцінювання

Процес створення інтелектуальної системи класифікації було реалізовано у декілька етапів, які охоплювали підготовку вхідних даних, балансування вибірки, вибір і навчання моделей, а також оцінку якості класифікації на основі ключових метрик. Основна мета полягала в побудові моделі, здатної точно і стабільно розпізнавати об’єкти класу меншості в умовах значного дисбалансу.

У процесі розробки і оцінки інтелектуальної системи класифікації дуже важливо правильно підібрати критерії, за якими буде визначатися якість роботи моделей. У рамках цієї роботи застосовуються такі ключові метрики:

– precision (точність). Precision показує, яка частка прикладів, що були класифіковані як позитивні, насправді є позитивними. Інакше кажучи, це відношення істинно позитивних передбачень до всіх позитивних, передбачених моделлю;

– recall (повнота, чутливість). Recall відображає здатність моделі виявити всі об’єкти позитивного класу, тобто показує, яку частку всіх реальних позитивних прикладів модель змогла правильно розпізнати;

– F1-score. F1-score є гармонічним середнім між Precision і Recall. Це метрика, яка враховує одночасно і точність, і повноту, особливо коли важливо зберігати баланс між обома;

– ROC AUC. ROC AUC – це площа під кривою «чутливість – специфічність» (TPR vs. FPR). Вона показує загальну здатність моделі відділяти позитивні приклади від негативних незалежно від порогу прийняття рішення. Значення ROC AUC = 0.5 означає випадкове передбачення (модель не краща за випадкову), значення близьке до 1 означає, що модель добре відрізняє класи. ROC AUC важлива тим, що

дозволяє оцінити модель за всіма можливими порогами одночасно, а не лише для конкретного значення. Це дає загальне уявлення про роздільну здатність моделі і допомагає уникати надлишкової оптимізації на конкретній точці.

У задачі з дисбалансом класів, коли приклади меншості є значно рідкіснішими, звичайна точність (accuracy) не підходить як основна метрика. Модель може просто передбачати всі приклади як більшість і при цьому мати, наприклад, 90% accuracy, не розпізнавши жодного прикладу меншості. Тому було обрано F1-score як головну метрику для порівняння, оскільки вона збалансовано оцінює здатність моделі виявляти важливий клас. Recall важливий як гарантія того, що ми не пропускаємо критичні об'єкти, Precision – щоб не "зашумляти" результат зайвими хибними тривогами, а ROC AUC – як загальний показник роздільної здатності класифікатора.

На початковому етапі було синтезовано набір даних за допомогою функції make_classification, який містив 10 000 прикладів з 20 ознаками.

П’ятнадцять ознак були інформативними, а п’ять – надлишковими. Класи були розподілені нерівномірно: 90% прикладів належали до більшості, 10% – до меншості. Це дозволило змоделювати ситуацію, наближену до реальних прикладних задач, наприклад, виявлення шахрайства або рідкісних відмов систем. Вибірка була розділена на навчальну і тестову частини у співвідношенні 70:30.

З метою забезпечення коректної роботи моделей було проведено масштабування числових ознак за допомогою StandardScaler. Масштабовані дані навчальної вибірки були використані для подальшого балансування за допомогою методу SMOTE (Synthetic Minority Over-sampling Technique). SMOTE дозволяє синтетично створити нові приклади меншості шляхом інтерполяції між наявними об’єктами цього класу, що дає змогу досягти симетричного розподілу без дублювання.

В результаті цього кроку структура вибірки була вирівняна, і кожен клас мав однакову кількість прикладів. Це дало змогу зменшити упередженість моделей до класу більшості та покращити здатність виявляти важливі, але рідкісні об’єкти.

3.2 Вибір алгоритмів

У моделюванні були використані п’ять ансамблевих алгоритмів: Random Forest, XGBoost, LightGBM, Bagging та Gradient Boosting. Random Forest був сконфігурований зі 100 деревами та фіксованим генератором випадковості.

XGBoost працював з деактивацією енкодера міток та метрикою втрат 'logloss'. Модель LightGBM використовувалась із параметрами за замовчуванням, що вже забезпечували високі показники навіть без ручного налагодження. Bagging та Gradient Boosting реалізовували відповідні класичні підходи, також з 100 базовими оцінювачами.

Навчання всіх моделей відбувалося на синтетично збалансованій навчальній вибірці. Тестування здійснювалося на початковій тестовій множині, що була масштабована тими ж параметрами. Після тренування було обчислено основні метрики: точність (Precision), повноту (Recall), F1-міру та площу під ROC-кривою (ROC AUC). Крім того, було враховано час тренування кожної моделі, що дозволяло зіставити обчислювальні витрати.

Результати показали, що застосування SMOTE дозволило значно покращити Recall майже у всіх моделей. Особливо помітне зростання повноти призвело до підвищення F1-score, що є ключовою метрикою у випадку задач із критично важливим класом меншості.

Усі моделі також демонстрували стабільні значення ROC AUC, що свідчило про хорошу здатність відокремлювати класи. Найкращі результати загалом були досягнуті моделлю LightGBM, яка забезпечила найвищу F1-міру та одночасно мала мінімальний час навчання (рисунок 3.1).

Без SMOTE

	Model	Precision	Recall	F1-score	ROC-AUC	Train Time (s)
1	XGBoost	0.887	0.851	0.869	0.968	0.21
2	LightGBM	0.834	0.846	0.840	0.962	0.10
0	Random Forest	0.852	0.757	0.802	0.964	3.51
3	Bagging	0.806	0.771	0.788	0.956	16.86
4	Boosting	0.662	0.817	0.731	0.948	6.83

Після SMOTE

	Model	Precision	Recall	F1-score	ROC-AUC	Train Time (s)
1	XGBoost	0.981	0.751	0.851	0.964	0.19
2	LightGBM	0.972	0.694	0.810	0.964	1.32
4	Boosting	0.977	0.609	0.750	0.943	3.61
3	Bagging	0.959	0.609	0.745	0.948	10.33
0	Random Forest	0.985	0.569	0.721	0.957	2.10

Рисунок 3.1 – Точність та час роботи моделей без та після балансування

Крім числових результатів, було побудовано графіки F1-score та ROC AUC для візуального порівняння моделей, а також матриці помилок для кожного алгоритму. Візуальний аналіз підтвердив покращення здатності моделей розпізнавати клас меншості після балансування (рисунки 3.2–3.3).

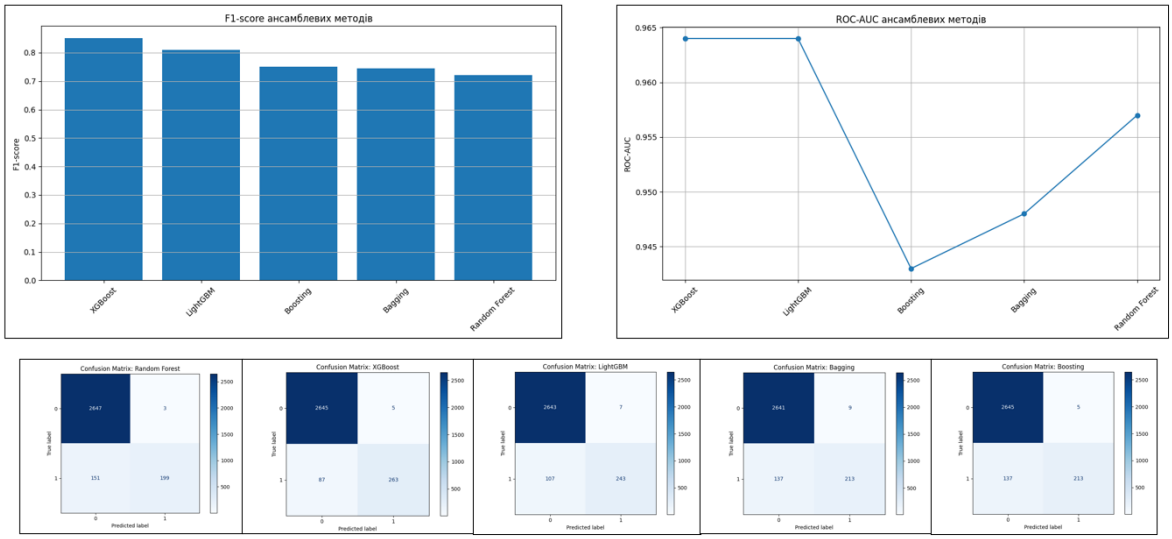

Рисунок 3.2 – Графіки порівняння роботи та матриці помилок для кожного алгоритму без балансування

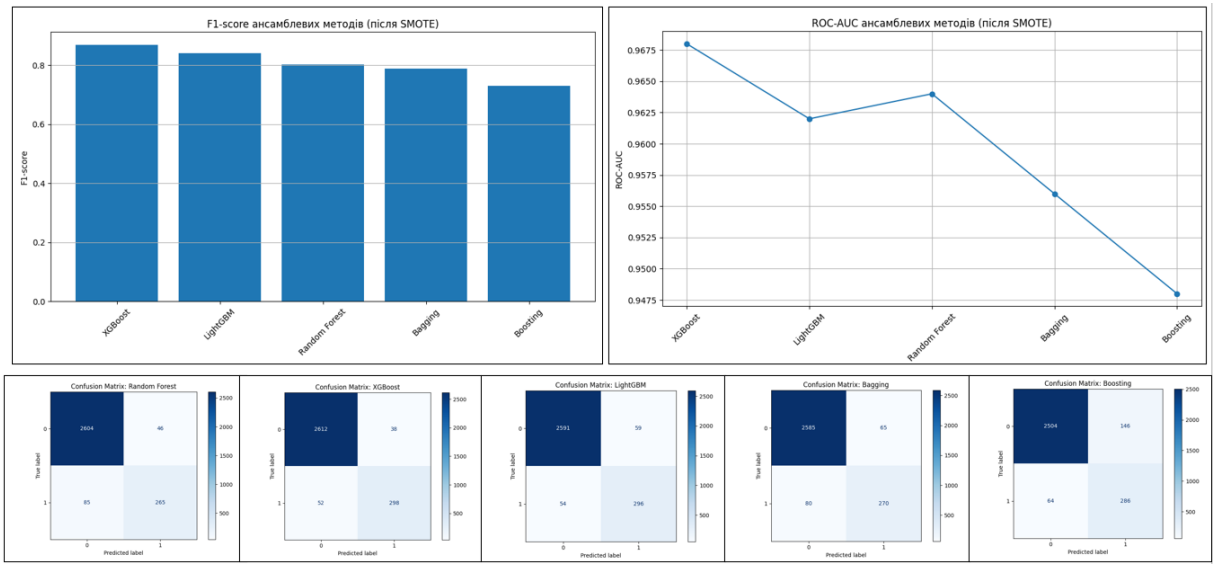

Рисунок 3.3 – Графіки порівняння роботи та матриці помилок після використання SMOTE

Таким чином, включення SMOTE у процес побудови моделей виявилося критично важливим для досягнення прийнятної якості класифікації. Найбільш придатною до впровадження у фінальну систему було визнано модель LightGBM, яка забезпечила найкраще поєднання точності, повноти, швидкості та стабільності при роботі на збалансованому наборі даних.

4 РОЗРОБКА ПРОТОТИПУ ІНТЕЛЕКТУАЛЬНОЇ СИСТЕМИ

Процес створення прототипу інтелектуальної системи виявлення шахрайства полягав у побудові повнофункціонального клієнтського застосунку, який виконує симуляцію обробки фінансових транзакцій у режимі реального часу.

Основна мета цього етапу полягала у візуалізації та демонстрації роботи моделі машинного навчання на практиці. Прототип поєднує в собі простоту запуску, автономність, а також наочність, що є ключовими критеріями для оцінки поведінки системи на ранніх етапах проєктування.

Візуальна частина реалізована з використанням HTML, CSS та JavaScript, що забезпечує кросплатформенність і можливість демонстрації без потреби у серверній інфраструктурі. Вебсторінка виконує функцію інтерактивного моніторингового інтерфейсу, в якому змодельовано як саму модель виявлення шахрайства, так і вхідний потік транзакцій. У верхній частині інтерфейсу розташований заголовок із назвою системи та коротким описом її можливостей.

Далі слідує блок, присвячений продуктивності моделі, в якому виведено метрики оцінки якості – точність, повнота, F1-міра та AUC-ROC. Значення цих метрик базуються на попередньому тренуванні моделі LightGBM, і на етапі прототипу подаються як фіксовані, що дозволяє користувачу сформувати уявлення про ефективність застосованого підходу.

Центральна частина інтерфейсу займає область з ключовими статистичними показниками (рисунок 4.1).

Тут виводиться загальна кількість опрацьованих транзакцій, окремо підраховується кількість нормальних і шахрайських транзакцій, а також динамічно обчислюється рівень шахрайства у відсотках. Ці показники оновлюються в режимі реального часу по мірі обробки нових транзакцій.

У нижній частині реалізовано панель керування, яка містить кнопки запуску та зупинки моніторингу.

Рисунок 4.1 – Статистичні показники роботи програми

При натисканні кнопки «Start Monitoring» активується симуляція – система починає генерувати випадкові транзакції з різними параметрами. Кожна транзакція проходить через алгоритм, що імітує поведінку навченої моделі LightGBM. У цьому алгоритмі передбачено набір ознак, які мають найбільший вплив на класифікацію: сума транзакції, час доби, вік користувача, частота попередніх операцій, ризик за геолокацією та ризик за типом пристрою.

На основі цих даних модель розраховує ймовірність того, що транзакція є шахрайською. Якщо значення перевищує умовний поріг (0.5), транзакція класифікується як підозріла (рисунок 4.2).

Рисунок 4.2 – Приклад Створеної Транзакції

Особливістю цієї логіки є введення елементів припущення та глибшої імітації реального середовища – навіть за високої кількості транзакцій загальний рівень шахрайства підтримується на рівні нижче одного відсотка, що відображає статистику реального світу. У деяких випадках у систему навмисне додаються транзакції з високим скором, аби протестувати реакцію інтерфейсу на виявлення шахрайства.

Кожна оброблена транзакція відображається у вигляді картки в журналі. Цей журнал оформлений як вертикальний список, де кожна транзакція має унікальний ідентифікатор, позначку часу, суму, торгову точку, місце здійснення, а також оцінку ризику у вигляді відсотка. Для зручності сприйняття шахрайські транзакції виділяються червоним кольором і анімаційним ефектом «пульсації», тоді як нормальні – зеленим або нейтральним. Крім того, виводиться рівень впевненості моделі в кожному рішенні, що дає додаткову інформацію для інтерпретації.

Одночасно з оновленням журналу система динамічно оновлює графік, що відображає зміни рівня шахрайства у часі. Графік реалізований з використанням бібліотеки Chart.js і дозволяє відстежувати обидва параметри – відсоток шахрайства та обсяг транзакцій – на двох різних шкалах. Це дозволяє оцінити вплив частоти операцій на рівень аномалій та змоделювати навантаження на систему.

Прототип спроєктований таким чином, щоб легко адаптувати його до роботи з реальними даними. Кожна його компонента, від симуляції до візуалізації, має відповідник у реальних банківських чи фінансових системах. У подальших етапах система може бути розширена за рахунок підключення серверної частини, бази даних транзакцій, REST API або потокових систем типу Kafka. Але вже на етапі прототипу вона дозволяє провести повноцінну оцінку реакції моделі на змінні вхідні дані, дослідити параметри ризику та оцінити інтерфейс з точки зору кінцевого користувача.

Таким чином, створений прототип не лише демонструє інтелектуальні можливості системи виявлення шахрайства, а й виконує роль експериментального середовища для тестування гіпотез, візуалізації результатів та підготовки до інтеграції у складніші архітектури.

ВИСНОВКИ

У межах цієї кваліфікаційної роботи було розроблено повноцінну інтелектуальну систему для виявлення шахрайських транзакцій у режимі реального часу. Робота охопила весь цикл створення системи – від теоретичного аналізу сучасних методів виявлення фінансового шахрайства до побудови робочого прототипу, який імітує поведінку реального застосунку в галузі банківських технологій.

На початковому етапі було проведено огляд основних підходів до боротьби з шахрайством, серед яких особливу увагу приділено алгоритмам машинного навчання, здатним адаптуватися до складних, нестабільних та сильно незбалансованих даних. Обґрунтовано вибір моделі LightGBM як оптимального компромісу між швидкістю обробки, точністю класифікації та можливістю масштабування на великі обсяги транзакцій. Модель було налаштовано з урахуванням реалістичних показників поширення шахрайства (менше одного відсотка) та використано найбільш релевантні ознаки, включаючи розмір транзакції, час доби, ризик за локацією, частоту операцій тощо.

Практична частина проєкту завершилася створенням інтерактивного прототипу, що дозволяє візуалізувати процес класифікації транзакцій у режимі реального часу. Інтерфейс розроблений з урахуванням сучасних вимог до зручності, доступності та наочності. Особливістю системи є наявність повноцінного модуля статистики, журналу подій, графічного моніторингу показників моделі та симуляції роботи системи без використання серверної інфраструктури. Це робить її зручною для демонстрації, тестування та подальшої інтеграції з реальними сервісами.

Результати моделювання показали високу точність і стабільність у виявленні потенційно шахрайських транзакцій навіть за низького рівня їхньої поширеності. Система демонструє адаптивну поведінку при зміні

вхідних параметрів, що є важливою перевагою в умовах постійної еволюції шахрайських схем.

Загалом, робота довела доцільність використання сучасних методів машинного навчання у сфері фінансової безпеки та підтвердила ефективність створеної системи на етапі прототипування. Вона може слугувати основою для подальших досліджень і розгортання промислових рішень, зокрема із підключенням до потокових сервісів, баз даних, а також побудовою повноцінного бекенду для обробки реальних транзакцій.

Подальший розвиток системи передбачає її інтеграцію з платіжними шлюзами, реалізацію механізмів самооновлення моделі на основі нових даних, застосування методів пояснюваного штучного інтелекту для підвищення прозорості прийняття рішень, а також впровадження додаткових кіберзахисних заходів для забезпечення безпеки самої системи. Таким чином, результати дипломної роботи не лише мають теоретичну та практичну цінність, а й відкривають перспективи для впровадження інтелектуальних рішень у критично важливі сфери фінансів та цифрової безпеки.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Ngai E. W. T., Hu Y., Wong Y. H., Chen Y., Sun X. Застосування технологій інтелектуального аналізу даних для виявлення фінансового шахрайства: класифікаційна структура та огляд літератури. *Decision Support Systems.* 2011. Т. 50, № 3. С. 559–569.

2. Bhattacharyya S., Jha S., Tharakunnel K., Westland J. C. Інтелектуальний аналіз даних для виявлення шахрайства з кредитними картками: порівняльне дослідження. *Decision Support Systems*. 2011. Т. 50, № 3. С. 602–613.

3. Mohiuddin M., Yousuf M. A., Zaman M., Rahman M. M. Виявлення шахрайства з кредитними картками за допомогою методів машинного навчання. *Information Security Journal*. 2020. № 29(3). С. 103–112.

4. Carcillo F., Dal Pozzolo A., Le Borgne Y. A., Caelen O., Mazzer Y., Bontempi G. Поєднання неконтрольованого та контрольованого навчання для виявлення шахрайства з кредитними картками. *Information Sciences.* 2019. Т. 479. С. 590–603.

5. Delamaire L., Abdou H., Pointon J. Шахрайство з кредитними картками та методи його виявлення: огляд. *Banks and Bank Systems*. 2009. Т. 4, № 2. С. 57–68.

6. Roy A., Sun J., Mahoney W., Alsharif Y., Gangopadhyay A. Глибоке навчання для виявлення шахрайства в транзакціях з кредитними картками. *Informatics.* 2018. Т. 5, № 4. С. 36.

7. Jakobsson M., Myers S. Фішинг та методи протидії: Розуміння проблеми електронного викрадення ідентичності. *Hoboken*: Wiley, 2006. 320 с.

8. Phua C., Lee V., Smith K., Gayler R. Огляд досліджень з виявлення шахрайства на основі інтелектуального аналізу даних. *arXiv preprint* arXiv:1009.6119. – 2010. URL: https://arxiv.org/abs/1009.6119 (date of access: 10.06.2025)

9. Breiman L. Random forests. *Machine Learning*. 2001. Vol. 45, Issue 1. P. 5–32.

10. Chen T., Guestrin C. XGBoost: масштабована система деревного бустингу. *Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. 2016. С. 785–794.

11. Chawla N. V., Bowyer K. W., Hall L. O., Kegelmeyer W. P. SMOTE: синтетичний метод надвибірки для класифікації незбалансованих даних. *Journal of Artificial Intelligence Research*. 2002. Vol. 16. P. 321–357.

12. Jurgovsky J., Granitzer M., Ziegler K. Класифікація послідовностей для виявлення шахрайства з кредитними картками. *Expert Systems with Applications.* 2018. Vol. 100. P. 234–245.

13. Zhang C., Ma Y. Ансамблеве машинне навчання: методи та застосування. *Berlin: Springer*, 2012. 340 с.

14. Aggarwal C. Outlier Analysis. *New York: Springer*, 2017. 456 с.

15. Lu Y., Liu F. Модель виявлення фінансового шахрайства на основі ансамблевого стекування. *IEEE Access*. 2020. Vol. 8. P. 84246–84255.

16. Dal Pozzolo A., Caelen O., Johnson R., Bontempi G. Calibrating probability with undersampling for unbalanced classification. *2015 IEEE Symposium Series on Computational Intelligence (SSCI)*. 2015. P. 159–166.

17. West J., Bhattacharya M. Інтелектуальне виявлення шахрайства в електронних платежах: огляд. *Information Systems*. 2016. Vol. 54. P. 44–62.

18. Sudjianto A., Yuan M., Zhang A., Kern D., Nair S., Cela J. Uncertainty quantification and interpretability in machine learning for fraud detection. *Banking Research Journal.* 2021. Vol. 38(1). P. 17–32.

19. Mahmoudi S., Duman E. Detecting credit card fraud by modified Fisher discriminant analysis. *Expert Systems with Applications*. 2015. Vol. 42. P. 2510–2516.

20. Bolón-Canedo V., Alonso-Betanzos A., Sánchez-Maroño N. Feature selection and ensemble classification for credit scoring. *Intelligent Systems.* 2014. Vol. 29(1). P. 3–12.

21. Bauder R. A., Khoshgoftaar T. M. A survey of data sampling and class imbalance in fraud detection. *Journal of Big Data*. 2018. Vol. 5(1). 42 с.

22. Kaggle. Credit Card Fraud Detection Dataset. URL: https://www.kaggle.com/mlg-ulb/creditcardfraud (date of access: 10.06.2025)

23. Aleskerov E., Freisleben B., Rao B. Cardwatch: система виявлення шахрайства на основі нейромереж. *Proceedings of the IEEE/IAFE*. 1997. P. 220–226.

24. Arshad S. Z., Khan S., Ahmad Z. Fraud detection in online payment systems using machine learning. *Journal of Computer Networks and Communications*. 2021. Vol. 2021. Article ID 6672978.

25. Sahoo S., Liu C., Hoi S. C. Fraud detection in e-commerce transactions using sequential behavior modeling. *Proceedings of the 41st International ACM SIGIR Conference*. 2018. P. 957–960.