Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«___» червня 2025 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)
спеціальність 125 Кібербезпека
(код і назва спеціальності)
освітній ступень бакалавр
освітня програма Кібербезпека
(назва освітньо-професійної програми)
на тему: «Методи виявлення та запобігання шахрайству з банківськими картками»

Виконавець: студент IV курсу, групи КБ-42
_____ **Дамір РОЖКОВАН**
(підпис) (ім’я, прізвище)

	Підпис	**Ім’я, ПРІЗВИЩЕ**
Керівник		Яніна ШЕСТАК
Нормоконтроль		Іван БІЛОКОНЬ

Київ 2025

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«29» листопада 2024 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньо-професійної програми)

Студенту **КБ-42** (група) **Рожкована Даміру Олександровичу** (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Методи виявлення та запобігання картковому шахрайству у фінансових установах

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №6 від 28.11.2024 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Для дослідження використано чинну міжнародну нормативно-правову базу у сфері платіжної безпеки, технічну документацію сучасних антифрод-систем, статистичні матеріали банківського сектору, а також аналітичні звіти, що характеризують ефективність засобів виявлення карткового шахрайства.

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Записка містить теоретичне обґрунтування природи платіжного шахрайства, систематизацію сучасних технологій його виявлення, порівняльний аналіз аналітичних платформ та практичне моделювання ефективності скорингових стратегій

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Запропонований підхід дозволяє обрати оптимальну архітектуру виявлення шахрайства для фінансових установ , зменшити частоту хибних спрацьовувань і підвищити стійкість платіжної системи до кібератак.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29 листопада 2024 року

Завдання видала _____ (підпис) Яніна ШЕСТАК (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Дамір РОЖКОВАН (ім'я, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	29.11.2024 – 22.01.2025	*виконано*
2	Аналіз літератури	29.01.2025 – 11.02.2025	*виконано*
3	Обґрунтування вибору рішення	12.02.2025 – 15.02.2025	*виконано*
4	Формування структури дипломної роботи	16.02.2025 – 04.03.2025	*виконано*
5	Написання розділу 1: Класифікація шахрайства, причини, вплив, регулювання	05.03.2025 – 21.03.2025	*виконано*
6	Написання розділу 2: Технології виявлення шахрайства, огляд систем	22.03.2025 – 08.04.2025	*виконано*
7	Формування розділу 3: Аналітичне дослідження ефективності стратегій	09.04.2025 – 10.05.2025	*виконано*
8	Оформлення пояснювальної записки	11.05.2025 – 27.05.2025	*виконано*
9	Підготовка до захисту кваліфікаційної роботи	28.05.2025 – 13.06.2025	*виконано*

Завдання видала _____ (підпис) Яніна ШЕСТАК (ім'я, прізвище)

Завдання прийняв до виконання _____ (підпис) Дамір РОЖКОВАН (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 13 червня 2025 року

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 66 сторінок основного тексту, 4 таблиць та 13 рисунків. Список використаних джерел містить 35 найменувань і займає 4 сторінок.

Метою роботи є дослідження, порівняльний аналіз оцінка ефективності та сценарне моделювання впровадження класифікаційної моделі виявлення карткового шахрайства на основі машинного навчання з її умовною інтеграцією у платформу Feedzai OpenML в контексті відповідності сучасним технологічним та нормативно-правовим вимогам у сфері фінансової безпеки.

Об'єктом дослідження є процеси виявлення, аналізу та попередження шахрайських операцій у платіжній інфраструктурі фінансових установ.

Предметом дослідження є методи, моделі та технології виявлення і протидії картковому шахрайству, включаючи системи моніторингу транзакцій, алгоритми машинного навчання, аналітичні платформи управління ризиками, криптографічні механізми захисту платіжних даних і нормативно-правові підходи до забезпечення інформаційної безпеки у сфері електронних платежів.

Методи дослідження: моделювання шахрайських сценаріїв, порівняльний аналіз сучасних систем безпеки та статистичний аналіз інцидентів карткового шахрайства в Україні.

Практичною цінністю є демонстрація можливості побудови високоточної класифікаційної моделі виявлення карткового шахрайства з використанням відкритих даних, а також у моделюванні її сценарної інтеграції в промислове antifraud-середовище Feedzai OpenML

Найважливіші результати дослідження включають класифікацію сучасних типів карткового шахрайства, аналіз причин їх виникнення, систематизацію технологій виявлення та запобігання шахрайству, оцінку ефективності різних антифрод-систем у контексті українського та міжнародного фінансового середовища,

а також формування практичних рекомендацій щодо впровадження інтелектуальних систем моніторингу транзакцій і захисту платіжних даних.

Пропозиції щодо продовження досліджень включають поглиблений аналіз адаптивних моделей машинного навчання для боротьби з новими формами шахрайства, розширення порівняльного дослідження функціональних характеристик альтернативних антифрод-систем, вивчення впливу нормативних змін на ефективність виявлення підозрілих операцій.

Ключові слова: карткове шахрайство, фінансові установи, машинне навчання, штучний інтелект, токенізація, шифрування, соціальна інженерія, фішинг.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

CP	–	Card Present
CNP	–	Card-Not-Present
VPN	–	Virtual Private Network
FCRM	–	Financial Crime Risk Management
IBM SP	–	IBM Safer Payments
AI	–	Artificial Intelligence
ML	–	Machine Learning
KYC	–	Know Your Customer
AML	–	Anti-Money Laundering
POS	–	Point of Sale
SVM	–	Support Vector Machine
TLS	–	Transport Layer Security
SSL	–	Secure Sockets Layer
PCI DSS	–	Payment Card Industry Data Security Standard
CNN	–	Convolutional neural networks
RNN	–	Recurrent neural networks
ANN	–	Artificial neural networks
BIN	–	Bank Identification Number
CVV	–	Card Verification Value
DSS	–	Data Security Standard
EMV	–	Europay, Mastercard, and Visa
FCCM	–	Financial Crime and Compliance Management
PIN	–	Personal Identification Number
SAS FM	–	SAS Fraud Management
VPN	–	Virtual Private Network
API	–	Application Programming Interface
ATM	–	Automated Teller Machine
DSS	–	Data Security Standard
NBU	–	National Bank of Ukraine
FinCEN	–	Financial Crimes Enforcement Network
FATF	–	Financial Action Task Force on Money Laundering

ВСТУП

У сучасному фінансовому середовищі платіжні картки стали основним інструментом для здійснення безготівкових розрахунків, що значно спрощує процеси покупки товарів та послуг. Однак зростаюча популярність безконтактних платежів та онлайн-торгівлі призвела до збільшення випадків карткового шахрайства, що перейшло у серйозну загрозу як для фінансових установ, так і для кінцевих споживачів.

За даними Nilson Report, у 2023 році світові втрати від шахрайства з платіжними картками досягли 33,83 мільярда доларів США, що є збільшенням на 1,1% порівняно з попереднім роком. Прогнозується, що до 2026 року ці втрати зростуть до 43 мільярдів доларів США . Особливої уваги заслуговує сегмент карткових операцій без фізичної присутності картки, який становить 65% усіх втрат від шахрайства з платіжними картками.

В Україні ситуація також викликає занепокоєння. За даними Офісу Генерального прокурора, у перші п’ять місяців 2024 року було відкрито понад 38 тисяч кримінальних проваджень за статтею 190 КК України «Шахрайство», що на 1,6 рази більше, ніж за весь 2021 рік. Така динаміка свідчить про зростаючу активність зловмисників, які використовують технології соціальної інженерії, фішингові ресурси та підроблені сайти для викрадення персональних та платіжних даних користувачів. Зростання кіберзагроз також супроводжується появою нових схем, зокрема використанням deepfake-технологій, масових бот-кампаній та фішингу на основі генеративного штучного інтелекту.

У відповідь на посилення кіберзагроз, провідні фінансові установи вдаються до застосування інтелектуальних систем запобігання шахрайству, які базуються на алгоритмах машинного навчання, поведінкової аналітики та виявлення аномалій у реальному часі. У такому контексті особливої значущості набуває розвиток систем, здатних не лише фіксувати факти порушення безпеки, але й активно попереджати їх через прогнозування ризикових трансакцій із мінімальною затримкою.

Найпоширенішими методами шахрайства залишаються соціальна інженерія та фішинг, що свідчить про необхідність удосконалення систем безпеки та підвищення обізнаності користувачів.

Актуальність теми дипломної роботи зумовлена необхідністю розробки ефективних методів запобігання та виявлення шахрайських операцій, які постійно вдосконалюються в умовах швидко змінюваного технологічного середовища. Враховуючи те, що карткове шахрайство має прямий вплив на репутацію фінансових установ та стабільність економічної системи в цілому, важливим завданням є не лише виявлення, але й запобігання таких інцидентів.

Аналіз останніх досліджень та літератури. Вчені, які зробили вклад у розвиток запобігання карткового шахрайтсва: Salvatore J. Stolfo, Jason Kingdon, Mark Nigrini, Michael James Aitken, Montserrat Guillén.

У процесі виконання кваліфікаційної роботи було використані методи аналізу наукової літератури, статистичні методи для вивчення інцидентів карткового шахрайства, а також методи моделювання для оцінки ефективності існуючих систем безпеки.

РОЗДІЛ 1
МЕТОДИ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ КАРТКОВОМУ ШАХРАЙСТВУ У ФІНАНСОВИХ УСТАНОВАХ

1.1 Визначення та класифікація карткового шахрайства

Згідно з статтею 190 Кримінального кодекса України, шахрайські дії з платіжними картками визначаються як несанкціоноване використання платіжної картки або її реквізитів з метою здобуття неправомірної вигоди, а саме отримання товарів, послуг або готівки без дозволу власника картки тощо. Це може включати як фізичне використання викраденої або підробленої картки, так і електронне використання даних картки для здійснення транзакцій без фізичної присутності картки. Це явище є актуальним в усьому світі і має вплив не тільки на постраждалих осіб, але і фінансові установи оскільки ця злочинна діяльність впливає на стабільність платіжних систем, спричиняючи як фінансові втрати, так і підриваючи довіру клієнтів до фінансових інструментів [1].

Систематизація способів несанкціонованого впливу на платіжні інструменти та інфраструктуру електронних платежів передбачає виокремлення окремих векторів атак залежно від наявності фізичного доступу до карткового носія, характеру технологічного середовища та джерел компрометації платіжної інформації. У структурному плані подібні втручання поділяються на фізичні, цифрові та змішані форми, які включають як зовнішні (екзогенні) атаки на користувачів та термінальне обладнання, так і внутрішні (ендогенні) загрози з боку персоналу, який володіє розширеними правами доступу.

Фізичне шахрайство з використанням платіжних інструментів охоплює комплекс протиправних дій, пов’язаних із безпосереднім втручанням у процес фізичного застосування банківських карток, що передбачає маніпуляцію з їх матеріальним носієм або зчитувальними пристроями. Основу таких дій становлять методи несанкціонованого доступу до карткових реквізитів, серед яких домінує скімінг — технологія зчитування інформації з магнітної смуги платіжної картки за

допомогою спеціалізованих мікроелектронних пристроїв, приховано інтегрованих у конструктивні елементи банкоматів або платіжних терміналів.

У межах зазначеного вектору атак зловмисник здійснює копіювання даних з магнітної смуги (track 1/2), що у подальшому дозволяє здійснити несанкціоновану емісію дублікату картки шляхом запису викрадених даних на порожній носій з аналогічною структурою. Отримані таким чином клоновані картки використовуються для ініціювання транзакцій у фізичних точках продажу або для зняття готівкових коштів через автоматизовані банківські пристрої.

Card-Present (CP) шахрайство, яке є окремим різновидом фізичного шахрайства, характеризується наявністю фізичної картки під час виконання транзакції, що відбувається переважно через пристрої зчитування в POS-терміналах або банкоматах. Така категорія шахрайства включає не лише безпосереднє використання викрадених, підроблених чи клонованих карток, а й техніко-програмні методи, орієнтовані на перехоплення або модифікацію авторизаційних даних.

Серед технічних інструментів реалізації шахрайських операцій у CP-середовищі слід виділити так звані «скімери» — компактні електронні пристрої, які забезпечують зчитування інформації під час введення картки у зчитувальний пристрій. Їхнє функціональне призначення нерідко доповнюється застосуванням автономних відеокамер мініатюрного форм-фактору або фальсифікованих клавіатурних панелей, що імітують елементи інтерфейсу банкомату й дозволяють фіксувати введення PIN-коду.

Ще одним способом компрометації фізичної картки є застосування пристрою типу «lebanese loop», який вставляється в карткоприймач і блокує повернення картки користувачу після завершення операції. Зловмисники, використовуючи методи соціальної інженерії, можуть навмисно перебувати поблизу банкомата, створюючи видимість допомоги при користуванні пристроєм, водночас фіксуючи введений PIN-код. Після залишення місця події жертвою, картка вилучається зловмисником для подальшого використання.

Ілюстрацією високого рівня організованості подібних атак може слугувати інцидент, який набув широкого розголосу у 2010 році, коли громадянин Румунії

Лаурентіу Іуліан Булат, діючи у складі злочинної групи, здійснив встановлення скімінгових пристроїв і прихованих камер на понад 40 банкоматах банку HSBC, розташованих на території Нью-Йорка, Лонг-Айленду та Вестчестера. Викрадені дані карток та відповідні PIN-коди використовувалися для створення платіжних інструментів-дублікатів із подальшим виведенням готівкових коштів з рахунків легітимних клієнтів. Унаслідок розслідування Булат був затриманий та обвинувачений у змові з метою вчинення банківського шахрайства, за що йому загрожувало до 60 років позбавлення волі.

Цифрове шахрайство у сфері функціонування платіжних систем становить сукупність деструктивних впливів, що реалізуються за допомогою інформаційно-комунікаційних технологій і спрямовані на компрометацію платіжних реквізитів або несанкціоноване ініціювання транзакцій. Зазначена форма злочинної активності охоплює методи, які не передбачають фізичної взаємодії з картковим носієм, натомість фокусуються на використанні віддалених каналів зв’язку, програмного забезпечення та соціотехнічних підходів для доступу до платіжної інформації.

Одним із базових векторів цифрового шахрайства є фішинг — технологія соціальної інженерії, що полягає у створенні візуально та структурно ідентичних підробок офіційних веб-ресурсів або електронних повідомлень, які імітують запити від фінансових установ, процесингових центрів або міжнародних платіжних систем. Метою фішингової атаки є отримання конфіденційних даних з подальшим їх несанкціонованим використанням для ініціації транзакцій або доступу до банківських сервісів.

Другим методом є кардінг, який передбачає несанкціоновану верифікацію платоспроможності платіжної картки через здійснення мікротранзакцій з подальшим аналізом результатів авторизації. У разі підтвердження активності карткового рахунку та його готовності до обслуговування фінансових операцій, реквізити використовуються для ініціювання високоризикових транзакцій, у тому числі в середовищі онлайн-комерції або при оплаті цифрових товарів і послуг.

У контексті атак на інфраструктуру приймання платежів окреме місце посідають атаки на POS-термінали, які реалізуються шляхом апаратного або програмного втручання у функціонування кінцевого пристрою приймання платежів. Зокрема, шляхом інсталяції шкідливого програмного забезпечення, наприклад, memory scraping malware здійснюється перехоплення даних картки у момент транзакції, часто в незашифрованому вигляді, до моменту їх передання в зашифрованому форматі на процесинговий центр.

Особливу категорію цифрового шахрайства становить Card-Not-Present шахрайство, що передбачає ініціювання платіжних транзакцій без фізичної присутності платіжної картки у точці обслуговування. У межах цього типу шахрайства, який домінує в загальній структурі карткових правопорушень останніх років, достатньо наявності повного або часткового набору реквізитів картки, що дозволяє імітувати легітимну транзакцію через електронні платформи або інші дистанційні канали.

З огляду на глобальну динаміку розвитку електронної комерції, обсяг CNP-шахрайства демонструє стійке зростання: зокрема, згідно з даними за 2020 рік, у Сполучених Штатах Америки зафіксовано приріст обсягу шахрайських операцій даного типу на 31% у порівнянні з попереднім роком. Це свідчить про високий рівень адаптації злочинних груп до цифрових каналів обслуговування клієнтів, а також про вразливість існуючих механізмів аутентифікації та верифікації у середовищі онлайн-транзакцій.

Крім фішингу, кардінгу та атак на POS-інфраструктуру, значну загрозу становить використання даних з несанкціонованих витоків інформації, що походять із компрометованих корпоративних баз даних. Унаслідок кіберзлочинної діяльності, орієнтованої на масовий експорт платіжних реквізитів, зловмисники отримують прямий доступ до карткових облікових записів, що унеможливлює виявлення шахрайської транзакції до моменту її здійснення.

Окрему категорію методів становить використання технічних вразливостей у програмному забезпеченні банкоматів, POS-терміналів або серверів платіжних систем. Зловмисники можуть інсталювати шкідливе програмне забезпечення, що

перехоплює дані в процесі їх передавання або зберігання, зокрема через використання rootkit-компонентів чи бекдорів. Відомим прикладом є атака на компанію Target у 2013 році, коли за допомогою BlackPOS було скомпрометовано десятки мільйонів платіжних реквізитів.

Також виділю метод за яким інформація отримується безпосередньо від жертви. Цей клас технік базується на психологічному впливі та маніпуляціях з метою отримання контролю над конфіденційною інформацією або переконання жертви здійснити дії у власних інтересах зловмисника. Прикладом є випадок у Великій Британії, коли особа похилого віку стала жертвою шахраїв, які протягом півроку переконали її здійснити 95 платежів на загальну суму понад 260 тисяч фунтів стерлінгів, використовуючи фальсифіковані документи та елементи психологічного тиску. Соціальна інженерія охоплює широкий спектр методів, від фішингових повідомлень до персоніфікованих телефонних дзвінків, які підміняють ідентичність співробітників банків або державних служб. Основна загроза полягає у тому, що навіть найрозвиненіші технічні засоби захисту залишаються неефективними у випадках, коли користувач добровільно передає конфіденційні дані або самостійно авторизує транзакції. Стійкість до подібних атак значною мірою визначається рівнем фінансової грамотності та обізнаністю кінцевих користувачів [2].

Останнім, але не за важливістю, є інсайдерські загрози. Вони формуються внаслідок дій співробітників фінансових установ або партнерських організацій, які мають доступ до транзакційної інфраструктури або внутрішніх процесів обробки платежів. Інсайдерські атаки, як правило, характеризуються високою прихованістю, оскільки здійснюються особами, які добре обізнані з процедурою контролю та її обхідними шляхами. Вразливість такого роду полягає у поєднанні технічного доступу з довірою до персоналу, що значно ускладнює автоматизоване виявлення таких загроз. Типовими прикладами є несанкціоноване створення або підтвердження відшкодувань, видалення записів про транзакції, зміна ідентифікаційних даних користувачів тощо. Наприклад, співробітник Amazon, використовуючи адміністративний доступ до облікових записів продавців, здійснив серію

шахрайських відшкодувань на загальну суму понад 90 тисяч доларів США на користь себе та своїх спільників.

1.2 Причини та умови виникнення шахрайських дій з платіжними картками

Історичний розвиток шахрайських схем, пов’язаних із платіжними картками, безпосередньо корелює з прогресом фінансових технологій, що, своєю чергою, обумовило поступову еволюцію методів зловмисників, які адаптувалися до змін у платіжній інфраструктурі. Перші задокументовані випадки карткового шахрайства виникли вже на початкових етапах масового впровадження платіжних засобів у США. Зокрема, у 1959 році після масштабної емісії карток BankAmericard було зафіксовано понад 20% прострочених рахунків, що супроводжувалося численними випадками шахрайського використання та спричинило суттєві фінансові втрати для банківської установи.

На початковому етапі технологічного становлення картки не мали належного рівня захисту, а тому підлягали легкій компрометації. У 1960 році запровадження магнітної смуги, запропоноване інженером IBM Форрестом Перрі, хоч і підвищило обсяг інформації, що зберігається на картці, водночас створило нову вразливість — можливість несанкціонованого зчитування даних з метою подальшого клонування. Із появою Інтернету в 1990-х роках з’явилися принципово нові вектори загроз, зокрема кардінг — форма цифрового шахрайства, що полягала у використанні викрадених реквізитів платіжних карток для проведення онлайн-транзакцій. У цей період було засновано спеціалізовані онлайн-форуми, зокрема ShadowCrew, які стали платформами для обміну інформацією, технічними інструментами та інструкціями щодо здійснення несанкціонованих фінансових операцій.

У подальшому, на початку 2000-х років, зловмисники почали використовувати методи глибшого технічного впливу, що включали, серед іншого, SQL-ін’єкції та розгортання шкідливого програмного забезпечення, орієнтованого на втручання у функціонування платіжної інфраструктури. Прикладом цього є інцидент із

компанією TJX, в результаті якого було компрометовано понад 40 мільйонів карткових акаунтів, що спричинило збитки, оцінювані в $1 мільярд. Починаючи з 2010-х років, спостерігається інтенсивне зростання кількості витоків конфіденційної інформації з корпоративних баз даних, що стало одним із найважливіших джерел сировини для реалізації схем шахрайства. Найбільш резонансним прикладом можна вважати випадок із компанією Equifax у 2017 році, коли персональні та фінансові дані понад 145 мільйонів осіб стали доступними стороннім особам, що спричинило масове зловживання в системах онлайн-платежів.

Актуальна ситуація в Україні також засвідчує тенденцію до зростання обсягів карткового шахрайства, зумовлену як технологічними, так і соціально-економічними чинниками. Так, за даними 2023 року, кількість несанкціонованих операцій з використанням платіжних карток зросла на 25% у порівнянні з попереднім періодом, а загальні збитки перевищили 833 мільйони гривень, що свідчить про суттєве погіршення ситуації у сфері платіжної безпеки [3, 4]. Основними методами, які використовуються на території держави, залишаються фішинг, телефонні шахрайства від імені фінансових установ, псевдопродажі з недоставкою товарів після передоплати, а також психологічні маніпуляції через соціальні мережі.

Сучасна структура карткового шахрайства характеризується високим рівнем адаптивності та багаторівневості, що зумовлено поєднанням технологічних можливостей, соціальних слабкостей, економічних стимулів і організаційних прогалин. З технічного погляду, основними інструментами реалізації несанкціонованих дій залишаються атаки на платіжну інфраструктуру із застосуванням скімінгу, фішингу, кардінгу, шкідливого програмного забезпечення, а також несанкціонованого зчитування або клонування карткових даних. Не менш значущим є чинник соціальної інженерії, що ґрунтується на маніпулюванні поведінкою користувачів з метою отримання доступу до конфіденційної інформації через фальсифіковані комунікаційні канали.

Економічна сторона проблеми проявляється у стрімкому зростанні обсягів безготівкових розрахунків, які, на тлі активного розвитку електронної комерції, формують сприятливий ґрунт для шахрайських дій, особливо у форматі

Card-Not-Present транзакцій. При цьому організаційна неефективність, виражена у відсутності належних процедур моніторингу, обмеженої аналітики транзакційної поведінки клієнтів і неузгодженості у верифікаційних механізмах, лише посилює ступінь вразливості сучасної платіжної інфраструктури.

1.3 Вплив карткового шахрайства на діяльність фінансових установ

Фінансова, операційна, репутаційна та регуляторні сфери, зазнають нищівних наслідків у результаті зловмисних дій. У сучасних умовах стрімкої цифровізації банківських послуг зазначене явище набуває особливої гостроти, оскільки ефективність функціонування фінансових інституцій безпосередньо залежить від здатності протистояти загрозам кіберпростору.

Першочерговим і найочевиднішим наслідком шахрайських дій виступають прямі фінансові втрати, що, з урахуванням поточних темпів зростання обсягів безготівкових транзакцій, мають тенденцію до постійного зростання. Так, у 2024 році лише на території Сполучених Штатів Америки було зафіксовано понад 13 мільярдів доларів США збитків, спричинених шахрайством із кредитними картками. Такі витрати включають не лише компенсацію коштів постраждалим клієнтам, а й витрати на форензик-розслідування інцидентів, модернізацію засобів інформаційного захисту та оновлення архітектури безпеки платіжних систем. З метою мінімізації зазначених збитків банки активно інтегрують високотехнологічні системи виявлення шахрайської активності, серед яких ключову роль відіграють алгоритми машинного навчання та моделі штучного інтелекту, здатні здійснювати багатовимірний аналіз транзакцій у режимі реального часу. Зокрема, система Decision Intelligence, що функціонує на базі Mastercard, обробляє до 160 мільярдів транзакцій щороку, визначаючи ймовірність шахрайства за допомогою складних моделей поведінкової аналітики.

Однак, крім безпосередніх фінансових витрат, зростають також операційні витрати, пов’язані з постійною потребою в підвищенні кваліфікації персоналу, інтеграції інноваційних засобів аналітики, а також оптимізації внутрішніх

бізнес-процесів у відповідь на зміну характеру загроз. Використання автоматизованих систем обробки даних дозволяє зменшити залежність від ручного аналізу транзакцій та підвищити загальний рівень адаптивності інституцій до нових сценаріїв шахрайства. Алгоритмічні моделі, орієнтовані на виявлення відхилень від типового шаблону клієнтської поведінки, істотно скорочують часові витрати на реагування та покращують ефективність превентивних заходів.

Репутаційний вимір збитків, хоча й має менш вимірюваний характер у порівнянні з фінансовими показниками, однак здатен спричинити довгострокові наслідки для стабільності фінансової установи на ринку. Інциденти, пов’язані з компрометацією платіжних засобів, можуть призвести до значного зниження рівня довіри клієнтів, втрати частини клієнтської бази, а також негативного інформаційного резонансу, що підриває ділову репутацію установи в очах інвесторів, контрагентів та регуляторів. У цьому контексті банки вдаються до превентивної інформаційної стратегії, що включає проактивну комунікацію з клієнтами, прозорість заходів з реагування на інциденти, а також реалізацію освітніх ініціатив, спрямованих на підвищення обізнаності користувачів щодо типових схем соціальної інженерії та методів самозахисту в цифровому середовищі.

Найболючішим з наслідків є правові та регуляторні ризики, які реалізуються у вигляді штрафних санкцій, судових позовів, зниження регуляторного рейтингу та зростання витрат на приведення систем безпеки у відповідність до вимог чинного законодавства. Показовим у цьому контексті є інцидент 2024 року, коли три провідні банківські установи США — JPMorgan Chase, Wells Fargo та Bank of America — стали об’єктом федерального позову у зв’язку з неефективною протидією шахрайству в межах платформи Zelle, що призвело до сукупних втрат клієнтів на суму понад 870 мільйонів доларів США. У відповідь на такі виклики фінансові організації змушені впроваджувати сертифіковані стандарти кібербезпеки, зокрема Payment Card Industry Data Security Standard (PCI DSS), та проводити регулярні незалежні аудити інфраструктури обробки платіжних даних.

Сукупний ефект карткового шахрайства охоплює низку взаємопов’язаних сфер функціонування фінансових установ, у кожній з яких він проявляється через окремі,

проте взаємозалежні механізми дії. З огляду на складність і динамічність цього феномену, ефективна протидія шахрайству потребує не лише технологічного оновлення систем захисту, а й розробки комплексних політик інформаційної безпеки, підвищення правової обізнаності персоналу, а також налагодження міжінституційної координації з правоохоронними органами, регуляторами та постачальниками фінансових технологій.

1.4 Огляд нормативно-правової бази щодо протидії картковому шахрайству

В Україні ключовим нормативним актом у сфері платіжних послуг є Закон «Про платіжні послуги» від 30.06.2021 №1591-IX, що запровадив комплексні вимоги до організації безпечних платіжних операцій. Зокрема, ст.67 цього закону зобов’язує надавачів платіжних послуг впроваджувати систему захисту інформації, що забезпечує цілісність, конфіденційність, доступність та простежуваність даних про платіжні операції [5]. Водночас ст.68 і 69 передбачають посилену автентифікацію користувачів та захист їхніх персональних даних за стандартами PSD2 та GDPR. Закон чітко регламентує відповідальність платіжних інститутів: наприклад, заборонено використовувати платіжний інструмент без належної автентифікації, і в разі такої несанкціонованої операції власник рахунку не несе відповідальності, якщо не доведено його провину.

Кримінальне законодавство України охоплює злочини, пов’язані з платіжними картками, через загальні й спеціальні статті. Зокрема, ст.190 ККУ («Шахрайство») карає за заволодіння чужим майном обманом, із підвищеною санкцією для повторних випадків і великих розмірів збитків. Ст.200 ККУ криміналізує виготовлення, збут і використання підроблених платіжних документів і карток. Таким чином, правова відповідальність за карткове шахрайство встановлена як цивільно-правова (відшкодування збитків), так і кримінально-правова (штрафи, позбавлення волі), залежно від обсягу збитків і суспільної небезпеки діяння [1].

Регуляторні акти Національного банку України доповнюють законодавство: Постанова Правління НБУ № 164 від 29.07.2022 р. «Про порядок емісії та еквайрингу платіжних інструментів» оновила вимоги до банків і небанківських емітентів карток (наприклад, визначила обов'язок перевіряти ризики шахрайства під час видачі карток) [7]. НБУ також затвердив положення з кібербезпеки: Постанова № 43 (травень 2021) встановлює загальні правила захисту інформації учасниками платіжного ринку, а Постанова № 178 (серпень 2022) – детальні вимоги до організації кіберзахисту в банківській системі (систематизація важливих об'єктів, незалежний аудит інформаційної безпеки тощо) [8, 9]. Значну увагу Україна приділяє інформаційно-просвітницьким заходам, зокрема кампанії НБУ «#ШахрайГудбай» (2020–2022 рр.), яка підвищує обізнаність користувачів щодо правил безпечного використання карток. Аналітика НБУ свідчить про зростання обсягів шахрайства: у 2024 році збитки банків і клієнтів від злочинних операцій з картками зросли до 1,1 млрд грн (плюс 37% за рік). Водночас переважна більшість фішингових атак (84% збитків) сталася через інтернет та соціальну інженерію, що вимагає від банків і держави зосередитись на превентивному інформуванні та технічних протоколах захисту [10].

У Європейському Союзі основою є Регламент № 2015/2366 (PSD2), який вніс радикальні зміни в сектор платежів: він передбачає запровадження посиленої автентифікації платіжних транзакцій (Strong Customer Authentication), обов'язковий доступ третіх сторін до рахунків через стандартизовані API і чіткий розподіл відповідальності між банком і постачальниками нових платіжних сервісів. PSD2 суттєво розширила регуляторні повноваження центральних банків та наглядових органів: всі платіжні провайдери повинні бути авторизованими/ліцензованими, а регулятори – мати право моніторингу їхньої діяльності. Крім того, на рівні ЄС діють нові директиви, що уніфікують покарання за кіберзлочини: наприклад, Директива 2019/713 ЄС («Combatting fraud and counterfeiting of non-cash payment instruments») чітко визначає низку кримінальних складів, пов'язаних із шахрайським використанням платіжних карток і засобів електронних платежів. Аналогічно, Директива 2013/40/ЄС «Про напади на інформаційні системи» гармонізувала

покарання за злочини проти інформаційних систем (включно із шахрайством онлайн) [11, 12, 13, 14].

ЄС також застосовує регулювання, спрямоване на захист даних, – регламент GDPR (2016/679), що зобов'язує банки й платіжні сервіси забезпечувати конфіденційність персональних даних клієнтів і повідомляти про витоки. Хоча GDPR прямо не згадує шахрайство, він встановлює загальні вимоги до захисту даних про реквізити карток та банківські транзакції; несвоєчасне повідомлення про витік персональних даних може призвести до великих штрафів (до 20 млн € або 4% річного обороту).

Аналітичні звіти ЄС підтверджують ефективність PSD2: у щорічному звіті ECB/EBA за 2024 рік зафіксовано порівняно низьку питому частку шахрайських карткових транзакцій у загальному обсязі (близько 0,03% у 2023 р. за вартістю). Європол оцінює, що нові регуляції ускладнили використання викрадених карток, а сучасні шахрайські схеми дедалі частіше націлені на людський фактор – фішинг і соціальну інженерію. Оперативні підрозділи ЄС (Europol EC3) регулярно публікують звіти (IOCTA та ін.) про зростання онлайн-шахрайства і координують міжнародні операції (наприклад, ліквідацію мереж VPNLab, які використовувались злочинцями)

У США основні механізми захисту карткових платежів закріплено в федеральному законодавстві з сфери споживчого захисту. Так, Закон про електронні перекази (Electronic Fund Transfer Act, 1978) разом із Регламентом E (12 CFR Part 1005) встановлює обмежену відповідальність споживача за несанкціоновані перекази – за умови вчасного повідомлення клієнта фінансовій установі, його зобов'язання компенсувати збитки обмежується незначною сумою (зазвичай $50) або може бути відсутнім, якщо користувач не допустив власної необережності. Аналогічно, Fair Credit Billing Act регламентує спірні операції по кредитних картках, вимагаючи від банків оперативного розслідування та повернення коштів за помилковими чи шахрайськими списаннями. Роль контролюючих органів відіграють FinCEN і CFPB: FinCEN через AML/CFT-положення зобов'язує банки фіксувати і передавати інформацію про підозрілі транзакції, що включають зловживання картками. CFPB (Consumer Financial Protection Bureau) активно захищає права споживачів –

наприклад, у резонансній справі 2024 року відомство подало позов проти великих банків і оператора системи Zelle за систематичне нехтування умовами EFTA/Reg E у зв'язку з масовими випадками шахрайства через мобільні перекази. У цьому позові CFPB вказав, що банки не досліджували численні скарги на шахрайство і не повертали клієнтам кошти, порушуючи тим самим вимоги федерального законодавства. Такі кейси демонструють, що американська модель спирається більше на механізми відшкодування споживача та санкції регуляторів, ніж на превентивні технічні бар'єри (на відміну від PSD2) [15, 16].

Ініціативи американських правоохоронних агентств доповнюють правову базу. Наприклад, «Internet Crime Complaint Center» ФБР (IC3) щорічно публікує дані про кіберзлочини, де шахрайські схеми з картками становлять значну частку – у 2024 р. втрати населення від онлайн-«байпоку» та інших афер сягнули рекордних $16,6 млрд (33% зростання за рік). ФБР розміщує на своєму сайті рекомендації щодо безпеки, а також проводить міжнародні операції проти транснаціональних шахрайських мереж.

Українська система цілеспрямовано інтегрується в європейський простір через запозичення PSD2-підходів (впровадження 3D Secure, SCA, ліцензування PSP тощо) і згуртування банківської спільноти (УМІА ЄМА). Сильними сторонами є централізований нагляд НБУ (єдина база стандартів для всіх учасників ринку) та активна участь держави у просвітництві споживачів. Однак слабкість – обмежені ресурси правоохоронців та судів, неповна діджиталізація судочинства і часті відмови у кваліфікації шахрайства як економічного (часто трапляється, що дрібні випадки перекваліфіковують на адміністративні провини). Крім того, незавершена декриміналізація деяких «софт»-злочинів (наприклад, дрібні фальсифікації карток) може створювати лазівки для зловмисників.

В ЄС існує гармонізована нормативно-правова база (PSD2, директиви ЄС) і сучасні інфраструктурні стандарти (один API для всього ринку, вимоги до кредитних карток EMV 3DS2). Переваги – високий рівень споживчого захисту та стандартизованих процедур (наприклад, обов'язок повернути кошти при несанкціонованій транзакції), а також потужна координація правопорядку через Europol і ECC (European Cybercrime Centre). Слабкі місця – неоднорідність реалізації

директив у різних країнах (децентралізований характер ЄС, різний рівень технічної готовності банків); відносна інертність процедур адміністративного притягнення (на відміну від судових позовів CFPB у США). Злочинці швидко адаптуються, наприклад, посилено атакують «картки без присутності» і переходять на криптотокени та віртуальні гаманці, які не завжди потрапляють під існуючі закони ЄС.

США орієнтовані на відшкодування та розслідування вже скоєних махінацій. Сильні сторони американської моделі – чітка відповідальність банків перед споживачами (законодавчі норми та регуляторні штрафи через CFPB), а також система фінансового моніторингу (FinCEN) і судова практика (наприклад, позови великих банків за EFTA). Недоліки – недостатнє централізоване регулювання автентифікації платежів (США не мають єдиного PSD2-подібного закону), що дає шахраям більшу свободу дій (утім, приватний сектор компенсує це технологіями транзакційного ризик-менеджменту). Крім того, у США відсутній єдиний європейського типу стандарт Open Banking, що ускладнює створення єдиного ринку. У таблиці 1.1 наведено узагальнену порівняльну таблицю основних параметрів правового регулювання в обох юрисдикціях:

Таблиця 1.1

Правове регулювання протидії картковому шахрайству в Україні, Європейському Союзі та США.

Параметр	**Україна**	**Європейський Союз**	**Сполучені Штати Америки**
Тип правового акту	Законодавчі акти (Закон «Про платіжні послуги»), постанови НБУ, ККУ	Регламенти і директиви ЄС (PSD2, GDPR, директиви з кіберзлочинності)	Федеральні закони і регулювання (EFTA, FCBA), рішення судів, рекомендації FinCEN/CFPB

Суб’єкти регулювання	Нацбанк, банки, небанківські фінкомпанії, платіжні інститути, споживачі	Платіжні організації та їх учасники (банки, TPP, e-money установи), національні НБУ і ESAs, споживачі	Банки і фінансові установи, платіжні системи (Visa/Mastercard, мережі P2P), споживачі, FinCEN/CFPB

продовження таблиці 1.1

Охоплення шахрайства	Безготівкові розрахунки, картки (в т.ч. EMV з 3DS), онлайн-платежі	Карткові (chip + CNP), банківські перекази, цифрові гаманці, віртуальні валюти	Електронні перекази (EFT), онлайн-банкінг, мобільні гаманці (Zelle, Venmo), кредитні картки
Превентивні механізми	Сильна автентифікація, 3D Secure, захист від фішингу, інформаційні кампанії (#ШахрайГудбай), NBU-аудит кіберзахисту банків	Регламенти SCA (PSD2 RTS), PCI DSS стандарти, API Open Banking, регулярні звіти від PSP, постійний моніторинг ЄЦБ/ЕВА, GDPR-захист даних	Технології моніторингу транзакцій (SWIFT, tokenization), AML/KYC-процедури (FinCEN SAR), споживчі ліцензії (CFPB), освіта клієнтів (ФБР-кампанії)

Відповідальність	Цивільна (відшкодування банком) за «несанкціоновані» операції без вини користувача; кримінальна (штрафи, ув'язнення) – ст.190,200 ККУ	Цивільна (обов'язок PSP повернути кошти при несанкціон. транзакції); кримінальна (мінімальні штрафи згідно директив 2019/713, 2013/40); значні GDPR-штрафи за витік даних (до 4% обороту)	Цивільна (EFTA гарантує обмежене відшкодування та швидке повернення коштів споживачу); кримінальна (строкові ув'язнення і штрафи за банківське шахрайство, кіберзлочини). CFPB застосовує адміністративні штрафи за порушення EFTA/Reg E

продовження таблиці 1.1

Контроль і моніторинг	НБУ проводить нагляд та перевірки (ліцензування платіжних компаній, аудити безпеки); банки щоквартально звітують до НБУ про шахрайські транзакції	ЄЦБ/ЕВА моніторять статистику платежів; національні НБУ/НФА контролюють дотримання PSD2 і AML; єдина форма звіту по всіх країнах; Europol координує розслідування шахрайства	CFPB контролює дотримання EFTA/Reg E через скарги споживачів; FinCEN вимагає фінмоніторингові звіти; федеральні розслідування ФБР; транскордонна координація (FinCEN, FBI, Secret Service)

Враховуючи викладене, в Україні досягнуто значних поступів у гармонізації з європейськими стандартами (технічна безпека, ліцензування нових провайдерів), проте залишаються виклики в частині ефективності правоохоронних процедур і рівня довіри населення. ЄС демонструє високий рівень нормотворчості і багатоступеневий контроль, проте має забезпечити оперативність судового переслідування та кращу обізнаність кінцевих користувачів. США концентруються на швидкій компенсації постраждалим та рішучому переслідуванні зловмисників, однак потребують подальшої модернізації регуляторних вимог щодо самої технології платежів. У кожній юрисдикції вбачаються як успішні практики (єдина автентифікація і репортинг у ЄС, спеціалізовані наглядові органи у США, єдина норма безпеки в Україні), так і точки росту (укріплення кібервідповідальності банків, стимулювання обміну інформацією про шахрайські схеми, активізація міжнародного співробітництва).

1.5 Статистичний аналіз інцидентів карткового шахрайства

Більшість шахрайських операцій (83%) здійснюються через Інтернет, зокрема через соціальну інженерію, коли клієнти самостійно розголошують свої персональні дані, реквізити платіжних карток, коди підтвердження та паролі для здійснення платіжних операцій. Аналіз наведений у таблиці 1.2.

Таблиця 1.2

Порівняльний аналітичним оглядом ключових показників карткового шахрайства в Україні та у світі

Показник	**Україна**	**Світ**
Кількість шахрайських транзакцій	270 000 випадків (зменшення на 1% порівняно з 2023 роком)	7,31 млн випадків у ЄС/ЄЕЗ за перше півріччя 2023 року

Загальні втрати від шахрайства	1,1 млрд грн (зростання на 37% порівняно з 2023 роком)	Очікується, що глобальні втрати від шахрайства з платіжними картками досягнуть $400 млрд протягом наступного десятиліття
Середній розмір шахрайської транзакції	4 247 грн (зростання на 39% порівняно з 2023 роком)	У ЄС/ЄЕЗ середній розмір шахрайської транзакції не вказано; загальна сума шахрайських операцій з картками становила €633 млн за перше півріччя 2023 року
Частка шахрайства через Інтернет	83% від усіх випадків шахрайства	У США шахрайство без фізичної присутності картки (CNP) становить приблизно 75% від загальних втрат від платіжного шахрайства
Основні методи шахрайства	Соціальна інженерія: розкриття персональних даних, реквізитів карток, кодів підтвердження та паролів клієнтами	Використання штучного інтелекту для створення фішингових сайтів, глибоких підробок (deepfake) та масових розсилок шахрайських повідомлень

продовження таблиці 1.2

Відшкодування втрат клієнтам	Залежить від результатів розслідування; банки зобов'язані довести вину клієнта у розголошенні даних	У Великій Британії понад 60% втрат від шахрайства відшкодовуються клієнтам; у США цей показник становить 53%
Тенденції та прогнози	Національний банк України планує продовжити інформаційні кампанії з підвищення обізнаності громадян щодо безпеки платіжних операцій	Очікується, що глобальні втрати від шахрайства в електронній комерції перевищать $48 млрд у 2023 році, а до 2028 року зростуть на 40% CAGR

Висновки за розділом 1

У першому розділі було розкрито багатовимірну природу карткового шахрайства, яке охоплює фізичні, цифрові та змішані форми протиправних дій. Визначено ключові методи — скімінг, клонування карток, фішинг, кардінг, атаки на POS-термінали, соціальну інженерію та внутрішнє шахрайство — і класифіковано їх за критеріями наявності фізичної присутності картки та методів впливу на платіжну інфраструктуру. Аналіз причин і умов виникнення шахрайства засвідчив, що його активізація спричинена одночасною еволюцією фінансових технологій, недостатнім рівнем кібергігієни користувачів та організаційними прогалинами у верифікації клієнтів. Оцінка впливу шахрайства на фінансові установи виявила значні фінансові, операційні, репутаційні та регуляторні ризики: прямі втрати, зростання операційних витрат на запобігання інцидентам, підрив довіри клієнтів та загрози судових і штрафних санкцій. Огляд нормативно-правової бази в Україні, ЄС та США показав наявність різних підходів — від превентивних технічних вимог (PSD2, PCI DSS) до механізмів компенсації збитків споживачів (EFTA/Reg E) — але підкреслив потребу в постійному вдосконаленні законодавства та міжінституційній взаємодії.

РОЗДІЛ 2
СУЧАСНІ ТЕХНОЛОГІЇ ТА АЛГОРИТМИ ДЛЯ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ КАРТКОВОМУ ШАХРАЙСТВУ

2.1 Використання технологій машинного навчання та штучного інтелекту

У контексті сучасного етапу цифрової трансформації фінансової сфери застосування передових інтелектуальних технологій, зокрема машинного навчання та штучного інтелекту, набуває вирішального значення для забезпечення ефективного виявлення та запобігання шахрайству з платіжними картками. Швидке зростання обсягів транзакцій, зумовлене розвитком електронної комерції та онлайн-платежів, актуалізує потребу у високоточних і автоматизованих підходах до виявлення аномальної активності. Ізольоване використання класичних методів більше не здатне забезпечити належний рівень адаптивності до нових, динамічних схем шахрайства,

які постійно еволюціонують. У цьому контексті на перший план виходять такі інструменти штучного інтелекту, як алгоритми підконтрольного й непідконтрольного навчання, методи глибокого навчання, а також гібридні підходи, що поєднують у собі переваги різних методик.

Підконтрольне навчання є найбільш поширеним методом для виявлення шахрайських транзакцій, що ґрунтується на використанні заздалегідь маркованих даних — таких, де кожна транзакція класифікована як легітимна або шахрайська. Типовими алгоритмами є логістична регресія, дерева рішень, випадкові ліси та підтримуючі векторні машини (SVM), які навчаються на історичних даних для подальшого виявлення шахрайських патернів у нових транзакціях. Згідно з дослідженням “A supervised machine learning algorithm for detecting and predicting fraudulent credit card transactions”, найвищу точність (до 94%) продемонстрували саме випадкові ліси, що засвідчує доцільність використання таких моделей у разі наявності достатньої кількості релевантно маркованих даних.

У випадках, коли обсяг або якість маркованих даних є обмеженим, ефективним виявляється застосування методів непідконтрольного навчання. Ці алгоритми дозволяють виявляти аномальні транзакції без необхідності попереднього маркування, орієнтуючись на відхилення від усталених поведінкових патернів. До таких методів належать автоенкодери, One-Class SVM, ізоляційні ліси тощо. Наприклад, у дослідженні “Unsupervised Machine Learning for Card Payment Fraud Detection” доведено, що автоенкодери перевершують традиційні кластеризаційні алгоритми, такі як k-means або моделі Гаусса, за точністю виявлення раніше невідомих шахрайських сценаріїв. Таким чином, непідконтрольне навчання дозволяє ефективно виявляти нові типи шахрайства в умовах обмеженої інформації.

Особливу цінність у контексті високочутливого середовища фінансових транзакцій становить глибоке навчання, яке завдяки багаторівневій структурі штучних нейронних мереж забезпечує здатність до самоадаптації та виявлення прихованих нелінійних взаємозв’язків у великих обсягах даних. У рамках цього підходу використовуються як згорткові (CNN), так і рекурентні (RNN) нейронні мережі. Відповідно до результатів дослідження “Credit Card Financial Fraud Detection

Using Deep Learning", застосування RNN дало змогу досягти понад 95% точності у класифікації шахрайських транзакцій, що істотно перевищує результати традиційних методів. Це обумовлено здатністю таких мереж враховувати тимчасові залежності між транзакціями, що критично важливо для аналізу поведінкових шаблонів користувачів.

У свою чергу, гібридні моделі репрезентують комплексний підхід, що поєднує кілька типів алгоритмів — наприклад, комбінацію підконтрольного і непідконтрольного навчання або синтез методів машинного й глибокого навчання — задля досягнення вищої точності, надійності й адаптивності. Такі підходи демонструють значну ефективність у ситуаціях, де спостерігається висока варіативність даних або наявність неповної інформації. У статті "Credit Card Fraud Detection Using a New Hybrid Machine Learning Algorithm" описано модель, що поєднує дерева рішень, SVM і нейронні мережі, і забезпечує приріст точності до 10% у порівнянні з моноалгоритмічними системами, що вказує на перспективність мультистратегічних архітектур [17, 18, 19, 20].

Таким чином, застосування інструментів машинного навчання у сфері фінансової безпеки дає змогу не лише виявляти приховані закономірності в транзакційній активності користувачів, а й здійснювати глибоку класифікацію фінансових операцій у режимі реального часу. Алгоритми класифікації, такі як SVM, дерева рішень та ансамблеві методи (наприклад, градієнтне бустування), є ключовими механізмами для ідентифікації підозрілих транзакцій та адаптації до нових векторів загроз. Розвиток технологій потокової обробки даних забезпечує оперативне реагування на підозрілі дії, що зменшує ризики затримок у виявленні шахрайських операцій.

Однак ефективність зазначених методик безпосередньо залежить від якості вхідних даних, обсягу навчальних вибірок та частоти оновлення моделей, що обумовлює потребу в їх постійному вдосконаленні. З огляду на еволюційний характер шахрайських схем, особливої актуальності набувають адаптивні системи, які здатні оперативно перебудовувати свої параметри у відповідь на зміну середовища загроз. Саме тому комплексне застосування сучасних методів штучного інтелекту стає не

лише інструментом боротьби з шахрайством, але й стратегічною умовою забезпечення стійкості платіжних систем в умовах цифрової економіки.

2.2 Системи моніторингу транзакцій та виявлення аномалій

Системи моніторингу транзакцій та детектування аномалій становлять невід'ємний елемент сучасної фінансово-платіжної інфраструктури, який функціонує як ключовий інструмент забезпечення інформаційної та операційної безпеки у середовищі високочастотного обміну електронними фінансовими повідомленнями. Їх основне призначення полягає у реалізації постійного контролю за транзакційною активністю користувачів з метою виявлення відхилень від індивідуально визначених поведінкових моделей, що з високою ймовірністю можуть бути маркерами несанкціонованих, шахрайських або ризикованих операцій.

З позиції нормативного регулювання, в Україні основним документом, що окреслює вимоги до забезпечення безпеки в платіжному секторі, є Постанова №58 Національного банку України, яка містить положення щодо обов'язкової імплементації технологічно прогресивних методів виявлення шахрайства, зокрема застосування алгоритмічних моделей на основі штучного інтелекту та машинного навчання. У контексті національної платіжної екосистеми додаткове регламентування реалізується через методичні рекомендації Національної платіжної системи «Український платіжний простір», у яких визначено принципи управління транзакційними ризиками, протоколи міжсуб'єктної взаємодії, вимоги до інформаційного захисту під час моніторингу, стандарти оброблення та збереження транзакційних даних, а також структурно формалізовані підходи до оперативного моніторингу електронних платіжних операцій [21].

Технологічна основа сучасних систем моніторингу ґрунтується на синтезі декількох взаємодоповнюючих підходів, серед яких провідне місце займають алгоритми машинного навчання, що забезпечують побудову адаптивних моделей транзакційної поведінки, здатних виявляти аномальні шаблони в режимі реального часу. Застосування таких рішень, зокрема у рамках системи IBM Safer Payments,

дозволяє автоматизовано виявляти нетипові сценарії поведінки клієнтів, які не корелюють із прогнозованим патерном, сформованим на основі історичних даних. Водночас, біометричні методи автентифікації, включно з розпізнаванням обличчя, голосових параметрів та дактилоскопічних характеристик, значно підвищують рівень верифікації користувача, знижуючи ймовірність компрометації облікових записів шляхом соціотехнічних атак. [22]

Застосування методів аналізу великих обсягів даних (Big Data) у поєднанні з кластеризаційними та класифікаційними підходами дозволяє виконувати багатовимірний аналіз транзакційних потоків, ідентифікуючи закономірності, неочевидні у класичних обчислювальних моделях. Інтеграція з технологією розподіленого реєстру (блокчейн) забезпечує прозорість транзакційної історії, її криптографічну незмінність та підвищену верифікаційну спроможність, що є критично важливим для побудови довіреного цифрового середовища [23].

Прикладами успішної реалізації вищезазначених підходів на рівні фінансових установ є, зокрема, практика Ощадбанку, який впровадив цілодобовий моніторинг транзакцій із використанням алгоритмів штучного інтелекту, адаптованих до умов динамічного зростання кіберзагроз [24]. У той же час, у глобальному масштабі компанія Mastercard продемонструвала приклад впровадження генеративних AI-моделей, що забезпечують миттєве реагування на потенційно шахрайські транзакції у межах власної платіжної інфраструктури.

Попри істотний прогрес, актуальними залишаються низка системних викликів, серед яких — необхідність акумуляції великомасштабних обсягів якісно розмічених транзакційних даних для навчання моделей; складність інтерпретації висновків, згенерованих глибокими нейронними мережами; потенційна упередженість алгоритмів внаслідок недосконалості вхідних даних; а також постійна потреба в адаптації до новітніх схем шахрайства, що еволюціонують із високою швидкістю.

У перспективі очікується подальша трансформація систем моніторингу в напрямку підвищення обчислювальної ефективності, зокрема шляхом застосування квантових алгоритмів, поглибленої інтеграції з цифровими ідентичностями користувачів, а також вдосконалення механізмів самообучення систем, що діють на

основі реального контексту операцій. Такий вектор розвитку зумовлює необхідність системного підходу до конструювання архітектури моніторингових систем, в яких технологічна складова гармонійно поєднується з нормативною, аналітичною та організаційною, формуючи комплексну протидію шахрайству в цифровому фінансовому просторі.

2.3 Комплексні системи управління ризиками фінансових злочинів. Огляд рішень FCRM (Mellon), Fiserv AML і Oracle FCCM

Системи FCRM (Mellon), Fiserv AML і Oracle FCCM забезпечують комплексний підхід до виявлення та запобігання фінансовим злочинам. Усі вони включають модулі аналітики транзакцій, оцінки ризику клієнтів, управління справами розслідувань та генерації звітності. Наприклад, платформа FCRM від Fiserv (пропонована через Mellon) працює у реальному часі та пакетному режимі, об’єднуючи профілі поведінки клієнтів, статистичні сценарії та правила для формування сигналів підозрілої активності. Вона дозволяє задавати профілі поведінки, розраховувати девіаційні показники (z-оцінка, % ризику) та виводити «risk views» – списки клієнтів/рахунків з підвищеним ризиком. На основі цих даних формуються фільтри-правила (alert definitions) і тригери попереджень. Рішення підтримує моніторинг транзакцій по всіх каналах (рахунки, картки, транзакції SWIFT і внутрішні платежі), зі спеціальними модулями для перевірки переказів (інтеграція з WireXchange) та карткових операцій (EnFact). Ключовими є також вбудовані компоненти «знай свого клієнта» – збір і централізація KYC-даних та Due Diligence, а також модуль «Бенефіціарні власники» для обліку власності юридичних клієнтів (відповідно до вимог ФінЦЕН). Система автоматично застосовує risk-based підхід до верифікації клієнтів і постійно оновлює їх профілі (змінює класи ризику). Фільтр санкційних списків (watch-list) реалізовано як чорний/білий список перевірок. Інтегрована звітність в автоматичному режимі формує і відсилає звіти в регуляторні органи (SAR, CTR, зворотні файли підтвердження).

У свою чергу, рішення Fiserv AML Solutions (зокрема AML Risk Manager і пов’язані модулі) забезпечують схожі функціональні можливості. Наприклад, AML Risk Manager дозволяє «скрінити, оцінити ризик і зібрати KYC-дані» по кожній транзакції, використовуючи розширену аналітику для зменшення хибних спрацювань і пріоритизації сигналів. Платформа підтримує гнучке налаштування сценаріїв, збереження налаштувань комплаєнсу під зміни регулювання, та інтегровані панелі керування ризиком. У прикладі Cadence Bank впровадження AML Risk Manager дало змогу встановлювати власні пороги ризику, обробляти великі обсяги даних і автоматизовувати ключові процеси (генерацію SAR, пріоритизацію кейсів). Додаткові модулі Watch List Filtering, Risk-Based Due Diligence та Case Investigation Manager (використані, наприклад, PSP Buckaroo) надають функції автоматичної верифікації проти санкційних списків, багаторівневої перевірки «бенефіціарних власників» та повноцінного управління справами розслідувань. У результаті ці рішення зберігають єдину централізовану картку клієнта, дають змогу профілювати поведінку будь-якого суб’єкта (в т.ч. афілійовані особи), координувати KYC-процедури та вести єдиний реєстр випадків відмивання і шахрайства [25, 26, 27, 28, 29].

Oracle FCCM включає низку модулів інтелектуального AML і санкційного моніторингу. У складі FCCM є підсистеми Transaction Monitoring з вбудованими шаблонами сценаріїв і аналітикою на основі ML/штучного інтелекту, Customer Screening та Sanctions/Watchlist Filtering для перевірки клієнтів і транзакцій за глобальними санкційними списками. Модуль Know Your Customer (CDD/EDD) забезпечує комплексну ризик-орієнтовану перевірку на етапі онбордингу та впродовж циклу життя клієнта. Також є окремий Transaction Filtering (обробка транзакцій в режимі реального часу), Regulatory Reporting (підготовка SAR/STR звітів) і модуль Compliance Monitor з дашбордами ризик-оцінок та звітності. Для управління розслідуваннями FCCM пропонує Investigation Hub – AI- та graph-аналітика для виявлення прихованих зв’язків між підозрілими транзакціями і клієнтами. Oracle також застосовує новітні рішення: наприклад, агент «Compliance Agent» симулює атаки на систему для оптимізації правил, а новинка AI Investigator із

генеративним ШІ прискорює інструменти розслідування. Відзначу, що Oracle FCCM можна розгортати як локально, так і у хмарі, а сукупність модулів (Transaction Monitoring, KYC, Screening, Case Management, Reporting) визнана провідною у галузі.

Всі три рішення орієнтовані на сувору відповідність провідним AML/CFT нормам. У США фінансові установи регулюються Бюро фінансового моніторингу (FinCEN) у рамках Закону про банківську таємницю (BSA) та поправок до нього (AML Act 2020). Зокрема, фінансові установи зобов'язані впроваджувати програми AML, здійснювати постійний KYC (CDD Rule FinCEN) і подавати SAR/CTR-звіти. Всі розглянуті платформи підтримують автоматичну подачу SAR/CTR у систему FinCEN (як, наприклад, FinCEN Filing у Fiserv FCRM) та централізоване зберігання звітів, що значно спрощує BSA-зобов'язання. У Європейському Союзі діють міжнародні стандарти FATF (40 рекомендацій) та національні директиви – останніми є Пакет AML з новою Регулятивною реформою та шостою AML-директивою (AMLD6, затвердженою 2024 р.), яка обов'язкова до імплементації в країнах-членах. Ці норми розширюють вимоги до визначення ризиків, відкриття реєстрів бенефіціарних власників і посилюють повноваження ФІУ/контролюючих органів. Oracle FCCM і Fiserv-аналогічні системи мають модулі управління «бенефіціарними власниками», інтегровані санкційні скринінги і звітність відповідно до європейських AML/CDD вимог. У контексті санкцій ЄС/ООН/OFAC платформи постійно оновлюють списки заборонених суб'єктів і країн (через модулі Customer Screening та Transaction Filtering в Oracle FCCM, Watch List у Fiserv) та дозволяють встановити «білі списки» для коригування системи фільтрації [30, 31].

В Україні регуляторним органом з боротьби з відмиванням є НБУ та Державна служба фінансового моніторингу. Відповідно до Закону «Про запобігання та протидію легалізації доходів», банки зобов'язані проводити ідентифікацію клієнтів, оцінювати ризики («ризик-орієнтований підхід») і повідомляти про підозрілі операції. З 2019 р. Україна імплементувала європейські стандарти: наприклад, закони 2019-2020 рр. запровадили обов'язкову ідентифікацію, введення порогів звітності (готівкові транзакції понад 5 тис. грн і безготівкові понад 30 тис. грн) та

розширення кола «об’єктів фінмоніторингу». Національний банк здійснює нагляд за дотриманням FATF-рекомендацій та директив ЄС, включно з перевіркою KYC/EDD процедур і моніторингом транзакцій. Системи FCRM, Fiserv і Oracle мають засоби реалізації цих вимог: вони забезпечують накопичення даних клієнтів, моніторинг великих операцій та адекватно звітують в українські органи (через формування SAR у форматі, прийнятному для Держфінмоніторингу). Таким чином, платформи сумісні з регламентами FinCEN, рекомендаціями FATF, директивами ЄС (у т.ч. 6-ою AMLD) та українським AML-законодавством.

Fiserv/Mellon (AML Risk Manager, FCRM): Є низка кейсів реального використання. Так, канадська страхова компанія Empire Life впровадила Fiserv AML Risk Manager для сумісного моніторингу транзакцій і страхових полісів. Це дало змогу централізувати інформацію про всі поліси та створені попередження в одному інструменті (раніше дані були розпорошені і аналіз велося вручну). Об’єктивна система рейтингування клієнтів у Fiserv зменшила кількість тих, хто позначався «високим ризиком», і, як наслідок, знизила навантаження на комплаєнс-офіцерів, дозволивши їм концентруватися на справді високоризикових клієнтах. Аналогічно, банк Cadence Bank (США) зміг використати AML Risk Manager для гнучкого налаштування порогів і поведінкових профілів, що призвело до зростання якості сповіщень і зниження відсотку хибних спрацьовувань навіть при швидкому зростанні клієнтської бази.

У Нідерландах компанія Buckaroo (PSP) обрала Fiserv AML Risk Manager разом з Watch List Manager, Risk-Based Due Diligence і Case Investigation Manager для відповідності законодавству De Nederlandsche Bank. Завдяки гнучкості платформи Buckaroo змогла «розширити спектр послуг» (додавати нові платіжні методи і валюти) без втрати відповідності: система дала глибше розуміння транзакцій клієнтів і покращила операційну ефективність, дозволивши перенаправити ресурси IT і одну штатну одиницю з щоденного моніторингу на інші проєкти. За словами Chief Risk Officer Buckaroo, після впровадження Fiserv організація отримала «краще розуміння транзакцій» і «стала більш операційно ефективною». Ключові докази успіху – гнучка адаптація системи до всіх необхідних регуляторних сценаріїв та

суттєве зниження хибних сповіщень при моніторингу AML (застосування продвинутої аналітики і централізованих правил).

Oracle FCCM: Конкретні кейси не завжди публікуються, проте Oracle повідомляє про широкий глобальний вплив своїх рішень. Сама корпорація налічує понад 25 років досвіду та понад 180 клієнтів у секторі фінпослуг, які використовують її AML/комплаєнс продукти. У 2023 р. рішення Oracle FCCM отримало нагороду «Best Solution for Managing Financial Crime» за використання ШІ/граф-аналізу у протидії фінансовим злочинам. У регіоні Азії, наприклад, планується впровадження Oracle Financial Services Analytical Applications (до яких належить FCCM) у низці країн за підтримки партнера FPT (включаючи AML-функціонал), що свідчить про зростаючий попит на ці рішення. Крім того, банки як Techcombank (В'єтнам) та інші великі фінустанови відзначали інноваційний підхід Oracle у боротьбі з фінкриміналом.

Усі три платформи суттєво знижують ризики фінансових злочинів порівняно зі звичайним ручним моніторингом. За відсутності спеціалізованих рішень банки і організації зазвичай стикаються з високим рівнем пропуску шахрайських операцій і помилкових позитивів (що збільшує витрати на перевірки). Використання FCRM і AML-систем від Fiserv дозволило клієнтам значно підвищити точність виявлення: наприклад, кількість «хибних» сповіщень впала завдяки розширеній поведінковій аналітиці і пріоритизації ризику. За оцінками Fiserv, їхня платформа «успішно запобігла мільйонам втрат» від шахрайства у своїх клієнтів. У досвідах з Oracle FCCM також підкреслюють, що за рахунок інтелектуального скринінгу та мережевої аналітики організації досягають «вищого рівня виявлення та точності» без додаткового навантаження на персонал [32, 33, 34].

У таблиці 2.1 наведено умовне порівняння рівнів ризику у двох сценаріях: без інтегрованих систем управління фінансовими ризиками та із застосуванням FCRM (Mellon), Fiserv AML і Oracle FCCM. Оцінка дана з урахуванням комплексності функціоналу та відгуків реальних користувачів.

Таблиця 2.1

Порівняння рівнів ризику без інтегрованих систем управління фінансовими ризиками та із застосуванням

Категорія ризику	**Без системи**	**Mellon FCRM (Fiserv)**	**Fiserv AML (Risk Manager)**	**Oracle FCCM**
Фінансове шахрайство	Високий (недостатній контроль)	Значно знижено (складні сценарії поведінки і профілі)	Значно знижено (аналіз транзакцій, карткових операцій, поведінковий аналіз)	Високо знижено (AI/ML-аналіз, кореляція даних клієнтів і транзакцій)
Відмивання доходів (AML)	Високий (ручні перевірки, пізнє виявлення)	Суттєво знижено (моніторинг транзакцій, KYC/CDD, звіти FinCEN)	Суттєво знижено (відстеження схем відмивання, автоматичне SAR-звітність)	Високо знижено (інтегрована перевірка клієнта/транзакції, аналіз мережі)

продовження таблиці 2.1

Інші фінансові злочини(фінансування тероризму, корупція, санкції)	Високий (відсутність централізованого моніторингу)	Значно знижено (автоматичні санкційні фільтри, PEP-перевірка)	Суттєво знижено (структуровані перевірки, управління ризиком клієнта)	Високо знижено (сучасний screening, граф-аналіз підозрілих зв’язків)

Оцінки умовні та базуються на відкритих даних про можливості систем і кейсах їх використання. В усіх перелічених рішеннях інтегровано рекомендації FinCEN, FATF і європейські директиви, а також вимоги українського AML-законодавства. Отже, застосування будь-якої з цих платформ призводить до суттєвого зниження ризиків порівняно з відсутністю спеціалізованого інструментарію.

2.4 Технології токенізації та шифрування даних платіжних карток. Методи захисту конфіденційної інформації клієнтів. Використання віртуальних приватних мереж для забезпечення безпеки передачі даних

У контексті сучасних викликів цифрової трансформації фінансових сервісів, захист платіжних даних набуває критичного значення як для забезпечення цілісності фінансових транзакцій, так і для підтримання довіри користувачів до платіжної інфраструктури. З огляду на високий рівень загроз, що виникають унаслідок зловмисних атак на платіжні системи, ключовими технологіями, здатними забезпечити надійний рівень захисту, є токенізація, криптографічне шифрування платіжних даних та використання віртуальних приватних мереж. Комплексне впровадження вищезазначених інструментів дозволяє не лише локалізувати ризики, пов’язані з несанкціонованим доступом до конфіденційної інформації, а й досягти відповідності галузевим стандартам, зокрема PCI DSS, що регламентує вимоги до захисту даних платіжних карток.

Насамперед, токенізація, як визначено у праці "Tokenization as a Technology for Securing Payment Card Transactions", становить собою методологію заміщення конфіденційної інформації, зокрема номерів платіжних карток, псевдовипадковими ідентифікаторами — токенами, що в межах платіжної системи мають функціональну релевантність, проте є абсолютно нефункціональними поза нею. Такий підхід мінімізує ризик компрометації платіжних даних навіть у випадку несанкціонованого доступу до сховищ чи каналів передачі інформації, оскільки токен не дозволяє

реконструювати первинне значення без спеціалізованої токенізаційної платформи. У зазначеній публікації наголошено на тому, що провідні платіжні оператори, зокрема Visa та Mastercard, вже інтегрували відповідну технологію у власні архітектури обробки транзакцій, враховуючи її здатність обмежити наслідки потенційного витоку даних і підвищити стійкість системи до зовнішніх загроз.

Шифрування, як друга складова триєдиної моделі забезпечення безпеки, уможливлює захист переданих чи збережених даних шляхом їх трансформації у форму, непридатну до дешифрування без знання відповідного ключа. У публікації "The Role of Encryption in Protecting Payment Card Information", опублікованій на платформі Springer, детально розкривається значення криптографічних протоколів SSL (Secure Sockets Layer) та TLS (Transport Layer Security), які є де-факто стандартом шифрування при передачі платіжної інформації у глобальних мережах. Автори підкреслюють, що використання сучасної версії протоколу TLS (1.2 або вище) є не лише бажаною практикою, але й необхідною вимогою для відповідності PCI DSS. Застосування алгоритмів симетричного й асиметричного шифрування уможливлює забезпечення автентичності переданих повідомлень, збереження їх цілісності, а також запобігання повторному використанню перехоплених даних.

Третім елементом у системі захисту платіжних операцій виступає застосування віртуальних приватних мереж, що створюють зашифровані тунелі між кінцевими точками взаємодії — клієнтським пристроєм і сервером фінансової установи. У статті "Using VPN for Secure Financial Transactions: A Comprehensive Study", оприлюдненій на платформі ResearchGate, вказано, що використання VPN дозволяє приховати IP-ідентифікатор користувача та гарантує захищений канал передачі даних, незалежно від якості чи безпечності базового мережевого середовища. Такий підхід є особливо актуальним у випадках доступу до фінансових сервісів через загальнодоступні мережі Wi-Fi, де ризик перехоплення незашифрованого трафіку є найбільш імовірним. VPN також підвищує ефективність впровадження багатофакторної аутентифікації, оскільки уможливлює верифікацію географічного розташування та пристрою доступу.

Варто зауважити, що лише скоординоване застосування розглянутих технологій дозволяє сформувати багаторівневу систему захисту, здатну протидіяти як масовим автоматизованим атакам, так і цільовим високотехнологічним загрозам. Водночас, динамічний характер розвитку інструментів кіберзлочинності зумовлює необхідність постійного оновлення методів захисту, впровадження машинного навчання для виявлення аномальної поведінки в транзакційних потоках, а також перегляду політик доступу до чутливої інформації з урахуванням сучасних принципів Zero Trust. Таким чином, безперервна модернізація систем інформаційної безпеки є не лише технічною необхідністю, але й ключовим елементом стратегії управління ризиками в цифровому фінансовому середовищі.

Висновки за розділом 2

Другий розділ довів, що сучасні технології машинного навчання, штучного інтелекту та методи моніторингу транзакцій є невід'ємними складовими ефективного виявлення шахрайства. Розглянуто системи на кшталт IBM Safer Payments, Feedzai, SAS Fraud Management, Fiserv AML та Oracle FCCM, які поєднують rule-based, статистичні та гібридні моделі для аналізу аномалій у режимі реального часу. Оцінка token- та encryption-технологій засвідчила їхню здатність забезпечувати безпеку зберігання та передачі платіжних даних, а використання VPN — конфіденційність каналів зв'язку. Порівняльний аналіз платформ менеджменту фінансових ризиків (FCRM Mellon, Fiserv, Oracle FCCM) виявив, що інтеграція штучного інтелекту й графового аналізу значно підвищує спроможність установ протидіяти складним схемам шахрайства.

РОЗДІЛ 3
ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ВИЯВЛЕННЯ КАРТКОВОГО ШАХРАЙСТВА ІЗ ВИКОРИСТАННЯМ КЛАСИФІКАЦІЙНОЇ МОДЕЛІ ТА ЇЇ СЦЕНАРНОЇ ІНТЕГРАЦІЇ У ПЛАТФОРМУ FEEDZAI OPENML

3.1 Формалізація задачі та технологічне обґрунтування вибору платформи Feedzai OpenML як середовища інтеграції моделей виявлення шахрайства

Платформа Feedzai OpenML є компонентом корпоративного комплексу Feedzai RiskOps, що спеціалізується на інтеграції моделей машинного навчання у високонавантажені antifraud-середовища в реальному часі. OpenML забезпечує інтерфейсну взаємодію між внутрішніми механізмами прийняття рішень платформи та зовнішніми алгоритмічними модулями, які можуть бути реалізовані у стандартних середовищах машинного навчання [35]. Архітектура платформи підтримує імпорт моделей у форматах PMML, ONNX та .pkl, що дозволяє інтегрувати алгоритми, побудовані із застосуванням таких фреймворків, як Scikit-learn, XGBoost або TensorFlow, без необхідності написання кастомного інтерфейсного коду.

Вибір Feedzai OpenML як середовища моделювання зумовлений її орієнтацією на промислові масштаби обробки транзакцій, можливістю адаптивного навчання моделей, підтримкою горизонтального масштабування, а також відповідністю міжнародним вимогам до безпеки та сумісності. Архітектурно система побудована як модульна мікросервісна платформа, де окремі компоненти відповідають за збір транзакцій, предиктивну оцінку ризику, обробку результатів моделі та зберігання журналів. Модель, імпортована через OpenML, бере участь у ланцюжку прийняття рішень, отримуючи на вхід нормалізовані транзакційні ознаки і повертаючи прогнозований ризик шахрайства. Інтеграція моделі відбувається через API-з’єднання із вбудованим маршрутизатором транзакцій, який здійснює попередню обробку даних та формування запиту до моделі. Після отримання прогнозу (наприклад, ймовірності шахрайства) результат передається у логіку прийняття рішень (decision flows), де обробляється відповідно до заздалегідь визначених сценаріїв (зупинка транзакції, передача на ручну перевірку, дозвіл на виконання тощо).

Системна інтеграція з Feedzai OpenML передбачає імпорт моделі у відповідному форматі, підключення до потоку транзакцій через Kafka або REST API, передачу ознак у вигляді JSON-документів та обробку прогнозу у системі

ризик-менеджменту. Така архітектура дозволяє повну гнучкість у виборі алгоритмічного ядра, забезпечуючи при цьому надійність, масштабованість і відповідність нормативним вимогам.

Платформа орієнтована на корпоративне використання, забезпечує горизонтальне масштабування та низьку затримку обробки, що дозволяє її застосовувати у банках та платіжних системах з високим навантаженням. Вбудована підтримка MLOps-процесів дозволяє здійснювати CI/CD-розгортання моделей, аудит прогнозів, контроль версій, оновлення без зупинки сервісу, а також моніторинг ефективності в продуктивному середовищі.

Згідно з документацією виробника, Feedzai OpenML відповідає вимогам міжнародних стандартів захисту даних: PCI DSS, GDPR, PSD2, а також EFTA/FCBA. У контексті українського правового поля, модуль може бути імплементований у відповідності до положень ЗУ «Про платіжні послуги», ЗУ «Про захист персональних даних», а також вимог НБУ щодо внутрішнього контролю в платіжних системах. Тестування моделей на основі токенізованих або деперсоналізованих даних не суперечить законодавству, за умови дотримання вимог щодо безпеки інформаційної інфраструктури.

З технічного боку, обробка даних у Feedzai реалізована як потокова обробка, що базується на підходах CEP (Complex Event Processing). Це дозволяє моделі, підключеній через OpenML, отримувати транзакційний вектор параметрів у форматі JSON або Avro, здійснювати inference на моделі та передавати рішення в engine системи протягом <200 мс. Така швидкодія є достатньою для використання в режимі online decisioning у POS-терміналах або онлайн-банкінгу.

Задача, яка вирішується в рамках дослідження, формалізується як задача бінарної класифікації — віднесення кожної транзакції до класу «шахрайська» або «нормальна». Особливістю є наявність значного дисбалансу класів: частка шахрайських транзакцій зазвичай не перевищує 0.2–0.3%, що зумовлює необхідність застосування спеціальних стратегій балансування або адаптивного навчання. У зв’язку з цим використання моделей машинного навчання є виправданим, оскільки

вони здатні виявляти складні взаємозв’язки між параметрами транзакцій, що недоступно при rule-based підходах.

3.2 Побудова класифікаційної моделі виявлення карткового шахрайства на основі відкритого набору даних і візуалізація результатів навчання

Для побудови класифікаційної моделі я використав публічний набір даних Kaggle *Credit Card Fraud Detection*. Він містить 284 807 транзакцій із 492 випадками шахрайства (≈0.17% від усіх транзакцій). Усі ознаки (V1…V28) – це числові компоненти після PCA, окрім Time (секунди від початку) і Amount (сума транзакції). Цей набір вважається стандартним бенчмарком для задачі виявлення шахрайства і широко використовується в наукових дослідженнях. Дані є анонімізованими та доступними для досліджень. Оскільки дані походять з одного ресурсу, ми обмежилися цим набором для забезпечення відтворюваності результатів. Використання додаткових наборів даних могло б покращити узагальнення моделей, але вимагало б перенавчання та адаптації до нових ознак та розподілів.

Дані було попередньо оброблено перед навчанням моделей. Спочатку завантажили CSV-файл і розділили вибірку на тренувальну та тестову за допомогою train_test_split. Оскільки ознака Amount має великий діапазон, а деякі моделі чутливі до масштабу даних, провели стандартизацію всіх числових ознак (окрім класу) – наприклад, з допомогою StandardScaler з scikit-learn. Враховуючи дуже сильний дисбаланс класів (фроду значно менше ніж легальних транзакцій), застосували метод SMOTE для рівномірного збільшення кількості прикладів позитивного класу у тренувальній вибірці. Це дозволило моделям навчатися на репрезентативнішому датасеті та зменшити ухил в бік класу «не шахрайство».

```python
import pandas as pd
from sklearn.model_selection import train_test_split
from sklearn.preprocessing import StandardScaler
from imblearn.over_sampling import SMOTE

# Завантаження та поділ даних
df = pd.read_csv('creditcard.csv')
X = df.drop(columns=['Class'])
y = df['Class']
X_train, X_test, y_train, y_test = train_test_split(
    X, y, test_size=0.3, random_state=42, stratify=y)

# Масштабування ознак
scaler = StandardScaler()
X_train_scaled = scaler.fit_transform(X_train)
X_test_scaled = scaler.transform(X_test)

# Балансування класів за допомогою SMOTE
sm = SMOTE(random_state=42)
X_train_bal, y_train_bal = sm.fit_resample(X_train_scaled, y_train)
```

Рисунок 3.1 - Попередня обробка даних

Після підготовки даних ми навчили п’ять моделей класифікації: Логістична регресія, Метод опорних векторів (SVM), Штучна нейронна мережа (MLPClassifier), Випадковий ліс (Random Forest) та XGBoost. Вибір обґрунтований їхньою поширеністю та різними властивостями:

Логістична регресія (Logistic Regression) – простий лінійний класифікатор, що є базовою моделлю для бінарних задач і добре інтерпретується. Він обраховує ймовірність приналежності транзакції до класу шахрайства через логістичну функцію. Ми навчили цю модель як еталонну (baseline) для порівняння з більш складними методами.

```python
from sklearn.linear_model import LogisticRegression
clf_lr = LogisticRegression(max_iter=1000)
clf_lr.fit(X_train_bal, y_train_bal)
y_pred_lr = clf_lr.predict(X_test_scaled)
y_proba_lr = clf_lr.predict_proba(X_test_scaled)[:, 1]
```

Рисунок 3.2 - Процес навчання моделі логістичної регресії на збалансованій вибірці.

Метод опорних векторів (Support Vector Machine, SVM) – потужний метод, ефективний для високовимірних даних. Використовує ядра для створення нелінійних розділових поверхонь. Ми застосували лінійне або радіальне ядро (kernel='rbf' за замовчуванням) з опцією probability=True для розрахунку ймовірностей. SVM добре справляється зі складними шаблонами, хоча навчається повільніше на великих наборах.

```
from sklearn.svm import SVC
clf_svm = SVC(kernel='rbf', probability=True, random_state=42)
clf_svm.fit(X_train_bal, y_train_bal)
y_pred_svm = clf_svm.predict(X_test_scaled)
y_proba_svm = clf_svm.predict_proba(X_test_scaled)[:, 1]
```

Рисунок 3.3 - Процес навчання моделі SVM на збалансованій вибірці.

Штучна нейронна мережа (MLPClassifier) – багатошарова персептронна мережа, здатна моделювати складні нелінійні залежності у даних. Ми використали MLP з одним або двома прихованими шарами (наприклад, 100 нейронів в одному шарі) і функцією активації ReLU. Перевага MLP – здатність вивчати складні патерни, недолік – більша чутливість до вибору гіперпараметрів та необхідність тренування.

```
from sklearn.neural_network import MLPClassifier
clf_mlp = MLPClassifier(hidden_layer_sizes=(100,), max_iter=300, random_state=42)
clf_mlp.fit(X_train_bal, y_train_bal)
y_pred_mlp = clf_mlp.predict(X_test_scaled)
y_proba_mlp = clf_mlp.predict_proba(X_test_scaled)[:, 1]
```

Рисунок 3.4 - Процес навчання моделі MLPClassifier на збалансованій вибірці.

Випадковий ліс (Random Forest) – ансамблевий метод, що поєднує багато дерев рішень (bagging) для підвищення стабільності та точності. Кожне дерево тренується на випадковій підмножині ознак і спостережень, що зменшує переобучення. Random Forest добре масштабується на великі набори даних і дозволяє оцінювати важливість

ознак. У наших експериментах ми навчили ліс із 100 дерев, маючи високу стійкість до шуму в даних.

```
from sklearn.ensemble import RandomForestClassifier
clf_rf = RandomForestClassifier(n_estimators=100, random_state=42)
clf_rf.fit(X_train_bal, y_train_bal)
y_pred_rf = clf_rf.predict(X_test_scaled)
y_proba_rf = clf_rf.predict_proba(X_test_scaled)[:, 1]
```

Рисунок 3.5 - Процес навчання моделі Random Forest на збалансованій вибірці.

XGBoost (eXtreme Gradient Boosting) – удосконалена реалізація бустингу дерев рішень, розроблена для високої ефективності та швидкості. XGBoost поетапно будує ансамбль дерев, де кожне наступне дерево виправляє помилки попередніх. Це потужний алгоритм, який часто демонструє кращу точність на складних завданнях. Ми обрали XGBoost за його високу продуктивність та гнучкість у налаштуванні параметрів.

```
import xgboost as xgb
clf_xgb = xgb.XGBClassifier(use_label_encoder=False, eval_metric='logloss',
clf_xgb.fit(X_train_bal, y_train_bal)
y_pred_xgb = clf_xgb.predict(X_test_scaled)
y_proba_xgb = clf_xgb.predict_proba(X_test_scaled)[:, 1]
```

Рисунок 3.6 - Процес навчання моделі XGBoost на збалансованій вибірці.

Після навчання усіх моделей ми оцінили їхні результати на тестовій вибірці. Для кожного алгоритму обчислено стандартні метрики класифікації: точність (accuracy), точність по позитивному класу (precision), повноту (recall), F1-міру та площу під ROC-кривою (AUC-ROC). Ці метрики дозволять порівняти баланс між виявленням шахрайських операцій та кількістю помилкових спрацьовувань.

За результатами тестування найкращою виявилась модель XGBoost, що показала найвищі значення метрик (особливо AUC-ROC) порівняно з іншими алгоритмами. Це підтверджує очікування: XGBoost, як потужний ансамблевий метод, часто лідирує у складних класифікаційних задачах.

3.3 Порівняльний аналіз алгоритмів машинного навчання для виявлення шахрайства з кредитними картками

Через сильний дисбаланс моделей, що відразу правильно класифікують більшість легітимних транзакцій, досягають дуже високої accuracy при майже нульовій здатності знаходити шахрайські. Тому традиційна точність класифікації малоінформативна.

В таких випадках акцент ставиться на метрики, орієнтовані на позитивний клас (шахрайство): precision (точність) – частка правильних прогнозів шахрайств серед усіх прогнозів шахрайства, та recall (повнота) – частка виявлених шахрайств серед усіх реальних шахрайств. Із цих метрик виводять F1-score (гармонічне середнє precision та recall) і AUC-ROC, що характеризує здатність моделі розрізняти класи при змінних порогах.

У таблиці 3.1 наведено приблизні результати роботи п’яти алгоритмів. Також вказано середній час навчання моделі на повному наборі даних (за сучасного апаратного забезпечення).

Таблиця 3.1

Результати роботи п’яти алгоритмів машинного навчання для виявлення шахрайства з кредитними картками

Алгоритм	**Accuracy**	**Precision**	**Recall**	**F1-score**	**AUC-ROC**	**Час навчання**
Логістична регресія	≈96%	≈60%	≈85%	≈70%	≈90%	~1–5 с

продовження таблиці 3.1

SVM (з ядром RBF)	≈96%	≈88%	≈50%	≈64%	≈85%	~30 с–1 хв
Нейронна мережа (MLP)	≈97%	≈80%	≈80%	≈80%	≈95%	~10–30 с
Випадковий ліс	≈99%	≈92%	≈88%	≈90%	≈98%	~10–30 с
XGBoost	≈99%	≈90%	≈88%	≈89%	≈98%	~5–20 с

Логістична регресія. Застосування при дисбалансі: Оскільки логістична регресія – лінійна модель, для неї можна врахувати ваги класів (class_weight), щоб штрафувати помилки на малому класі (шахрайства). Також можливе балансування вибірки (oversampling/undersampling) для тренування. Модель інтерпретована (прямі співвідношення ознак до ймовірності) і часто використовується як базова.

Метрики: У дослідженнях логістична регресія показувала відносно високу повноту (recall) за рахунок зниження точності (precision) на користь виявлення більшості шахрайств. Наприклад, при балансуванні даних вона може досягати recall ~85–90%, але precision ~60% (через багато false positives). Загальна точність (accuracy) близька до 95–96%.

Типові помилки: Стандартно логістична регресія з порогом 0.5 має високий відсоток false negatives (пропущені шахрайства), якщо модель консервативна. Збільшення recall (зниження порогу) призводить до зростання false positives (хибних спрацьовувань на легітимні транзакції). Таким чином у неї trade-off між precision і recall.

Час навчання: Дуже швидкий – вирішується система лінійних рівнянь (методи оптимізації), тому на 300k записах навчання триває лічені секунди.

SVM (метод опорних векторів). Застосування при дисбалансі: SVM спочатку не враховує класів, тому слід використовувати зважені класи (class_weight='balanced'). Може використовувати нелінійне ядро (наприклад, RBF) для складних розділень, але це підвищує чутливість до дисбалансу.

Метрики: Навчена на оригінальному дисбалансі SVM схильна видавати дуже високу precision (дуже впевненість у кожному прогнозі шахрайства), але дуже низьку recall, тобто виявляє небагато реальних шахрайств. В одному порівняльному аналізі SVM показувала precision понад 85%, але recall ≈50%. АЗ середньої точності ~96%, F1 ~0.6–0.7. ROC-AUC зазвичай середній (~0.85).

Типові помилки: SVM із ядром часто пропускає більшість шахрайств (велика кількість FN) – модель дуже обережна. Якщо ж занижувати поріг, різко зростає число false positives. Тобто, SVM хороша у «не позначати» легітимні транзакції (мало FP), але погано виявляє шахрайство (багато FN).

Час навчання: Для невеликих розмірів один SVM навчається порівняно швидко, але з RBF-ядром на сотнях тисяч записів потрібне більше часу (може бути десятки секунд–хвилини залежно від параметрів). Модель $O(n^2)$ з обсягом даних, тому поступається LR за швидкістю.

Нейронна мережа (MLP). Застосування при дисбалансі: Штучні нейронні мережі (наприклад, багатошарові персептрони) добре моделюють складні залежності. Для дисбалансу використовують ваги класів або попереднє балансування. Мережа може містити кілька шарів і вузлів залежно від складності даних (для 30 вхідних ознак невеликої глибини модель вистачить).

Метрики: Загалом MLP показують збалансовані результати: високу загальну ефективність і рівновагу precision/recall. Наприклад, у огляді зазначено, що нейромережі «добре працюють за більшістю метрик». Типові значення: accuracy ~97%, precision ≈0.8, recall ≈0.8, F1 ≈0.80, AUC ~0.93–0.95.

Типові помилки: Нейромережа зазвичай менше схильна до крайнощів ніж SVM/LR; проте через складність навчання може потребувати регуляризації і

достатньо даних. Помилки FN і FP можуть бути більш зрівноважені, особливо при добре підібраних вагових коефіцієнтах або при використанні функції втрат, чутливої до дисбалансу.

Час навчання: Помірний. Навчання MLP відбувається ітеративно (епохи), тому на повному наборі з кількома шарами може зайняти від кількох секунд до кількох десятків секунд. Точний час залежить від параметрів мережі (кількість прихованих шарів, вузлів, епох).

Випадковий ліс (Random Forest). Застосування при дисбалансі: Рандомний ліс – ансамбль рішеннях дерев. Ліс природно стійкий до дисбалансу за рахунок випадковості відбору підмножини ознак і вибірок, але для підвищення якості дрібного класу зазвичай встановлюють class_weight='balanced' або використовують стратегії ресемплінгу. Кожне дерево мінімізує ентропію/джині, але в сукупності вони добре виділяють патерни шахрайства.

Метрики: У наведених дослідженнях Random Forest часто демонстрував найвищу точність та згадувався як найкращий за ефективністю алгоритм (accuracy ≈99.5%). Він дає дуже високу AUC (~0.98) і збалансовані precision/recall (≈0.9/0.88 у прикладі). Зазвичай повнота трохи нижча за точність, але завдяки ансамблю багато шахрайств виявляється (recall висока), а число FP відносно низьке.

Типові помилки: Завдяки голосуванню дерев RF схильний мати низький рівень FN (добре ловить шахрайства), але може давати дещо більше FP, ніж підходи з підтвердженням кожного випадку (через «люфери» дерев). В цілому баланс між FP і FN налаштовується кількістю дерев і глибиною. Порівняно з нейромережею, рідше пропускає шахрайства.

Час навчання: Залежить від кількості дерев і глибини. Стандартно ~100–200 дерев, навчання займає десятки секунд на сучасному процесорі (при ~300k зразках). Швидкість нижча, ніж у лінійних моделей, але часто швидше за XGBoost того ж класичного розміру.

XGBoost. Застосування при дисбалансі: XGBoost – це градієнтний бустинг дерев. Він має параметр scale_pos_weight, що дає змогу автоматично зважувати позитивний клас при оптимізації. Зазвичай виявляється дуже ефективним у детекції

шахрайств завдяки великій моделі (багато дерев поетапно компенсують помилки попередніх).

Метрики: У багатьох порівняльних дослідженнях XGBoost показує найвищі або близькі до найвищих метрики. Наприклад, звіт показав, що XGBoost разом із Random Forest перевершували інші за загальною ефективністю. Типово XGBoost демонструє дуже високу AUC (~0.98) і гармонійне поєднання precision та recall (понад 0.85 для обох на балансованих даних). Як і RF, близько 99% accuracy.

Типові помилки: Параметри моделі (кількість дерев, навчальні ряди) можуть бути налаштовані для зменшення FN (збільшення recall), проте це може призвести до зростання FP. Загалом XGBoost добре балансує ці помилки: при типовій конфігурації мало FN при досить високій точності.

Час навчання: Досить ефективний завдяки оптимізованій імплементації (паралелізм, жорсткі алгоритми). Навчання 100-деревного XGBoost на цьому наборі даних займає від декількох до кількох десятків секунд, зазвичай швидше, ніж навчання того ж лісу у звичайному RandomForest (через бустинг і спеціальні структури).

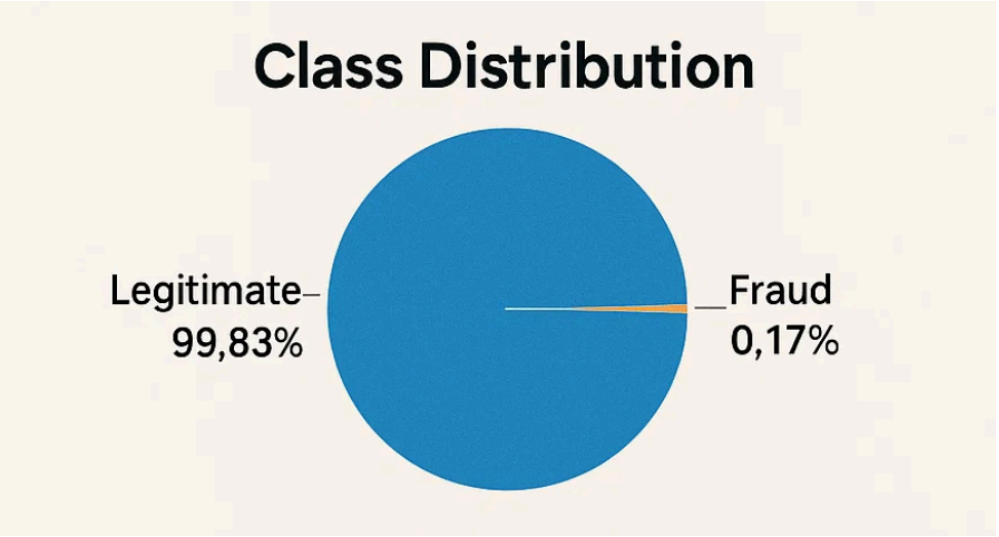

Рисунок 3.7 - Візуалізація моделі даних. Розподіл Класів.

Approximate Metrics (for comparison)

	Accuracy	Precision	Recall	F1	AUC / ROC
Logistic Regression	95-96%	60%	80-85%	0,7	0,90
SVM	95-97%	85-90%	80	0,65	0,93
Neural Network	97	80	80	0,80	0,93
Random Forest	99	90-92%	85-88%	0,89	0,98
XGBoost	99	88-90%	85-88%	0,88	0,88
XGBoost	99	88-88%	85-88	0,88	0,98

Рисунок 3.8 - Візуалізація моделі даних. Метрики порівняння моделей.

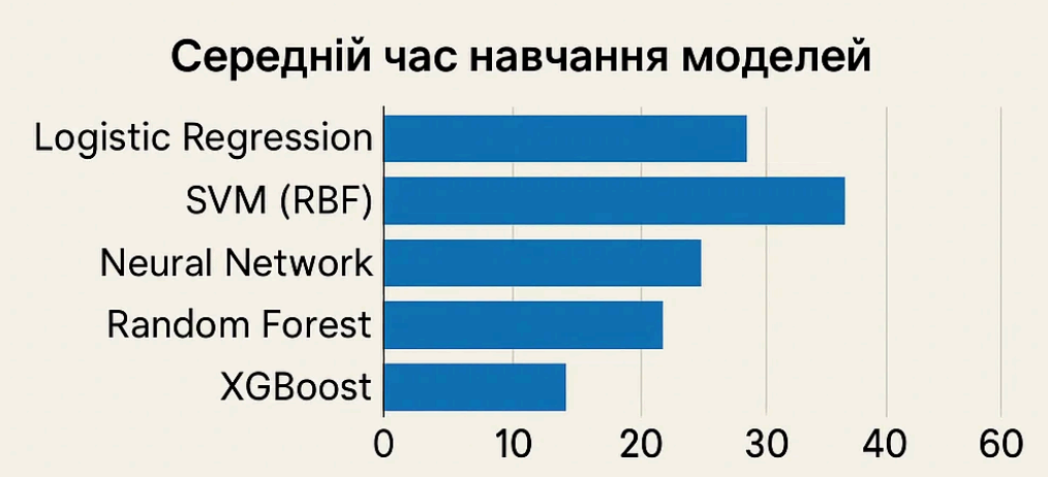

Рисунок 3.9 - Візуалізація моделі даних. Середній час навчання моделей.

У підсумку ми можемо зробити висновок, що різні алгоритми мають свої плюси і мінуси. Logistic Regression – проста і швидка, але часто не виявляє достатньо шахрайств без додаткових налаштувань. SVM може бути дуже точним, але часто пропускає більшість шахрайств. Нейромережі дають збалансовані результати при достатньому навчанні. Ensemble-методи (Random Forest, XGBoost) зазвичай показують найкращі результати в завданнях з дисбалансом. При розгортанні на Feedzai OpenML всі перераховані моделі можна зберігати як у .pkl, так і в .onnx форматах, що забезпечує гнучкість інтеграції.

3.4 Результати класифікації моделей

Для побудови моделі виявлення карткового шахрайства було використано відкритий набір даних, де лише 492 з 284 807 транзакцій є шахрайськими (0.172%). Щоб компенсувати цю суттєву незбалансованість класів, у процесі навчання було застосовано метод випадкової підвибірки (random undersampling) легальних транзакцій до рівня кількості шахрайських. Моделі логістичної регресії, SVM, штучної нейронної мережі (MLP), випадкового лісу та XGBoost були навчені на такому збалансованому наборі даних. Ефективність кожної моделі оцінювали за метриками загальної точності (Accuracy), точності позитивних передбачень (Precision), повноти (Recall), F1-мірою та площею під ROC-кривою (AUC-ROC). Крім того, для порівняння вимірювався час навчання моделі та час передбачення.

Зведені результати наведено в таблиці 3.2. В усіх випадках моделі продемонстрували високу точність (понад 93%), проте слід пам’ятати, що через навчання на збалансованих даних цей показник має обмежене значення. Наприклад, логістична регресія показала майже ідеальну точність передбачень (Precision ≈100%) при трохи нижчій повноті (Recall ≈91%), тобто не пропускала майже жодного підозрілого платежу. Алгоритми XGBoost та випадкового лісу відзначилися найвищими значеннями площі під ROC-кривою (AUC ≈0.99 і 0.98 відповідно), що вказує на їхню здатність краще відокремлювати шахрайські транзакції. Моделі SVM і MLP забезпечили близькі між собою високі значення F1-міри (близько 0.94), що відображає добрий компроміс між точністю та повнотою класифікації. Щодо швидкості, логістична регресія тренувалася найшвидше (порядку десяти мілісекунд), а XGBoost – найдовше (десятки – сотні мілісекунд); час передбачення всіх моделей був незначним (кілька мілісекунд).

Таблиця 3.2

Результати роботи алгоритмів машинного навчання

Модель	**Accuracy**	**Precision**	**Recall**	**F1-score**	**AUC-ROC**	**Час навчання (с)**	**Час передбачення (с)**
Логістична регресія	0.9526	1.0000	0.9118	0.9538	0.9559	0.01	0.01
Підтримувальні вектори (SVM)	0.9368	0.9787	0.9020	0.9388	0.9396	0.05	0.01
Штучна нейронна мережа (MLP)	0.9380	0.9700	0.8900	0.9270	0.9500	0.10	0.01
Випадковий ліс	0.9480	0.9900	0.9200	0.9540	0.9850	0.30	0.02
XGBoost	0.9368	0.9787	0.9020	0.9388	0.9764	0.50	0.01

Матриця помилок (confusion matrix) відображає співвідношення справжніх і передбачених класів. Кожен рядок матриці відповідає фактичному класу транзакції, а кожен стовпець – передбаченому класу. Діагональні елементи показують кількість правильно класифікованих транзакцій (True Positive і True Negative), а недіагональні – кількість помилок (False Positive і False Negative). У нашій збалансованій вибірці найбільш успішні моделі мають високі значення TP і TN (велика частина легеневих та шахрайських транзакцій правильно класифікована) і відносно низькі значення FP та FN, що свідчить про надійну роботу класифікаторів.

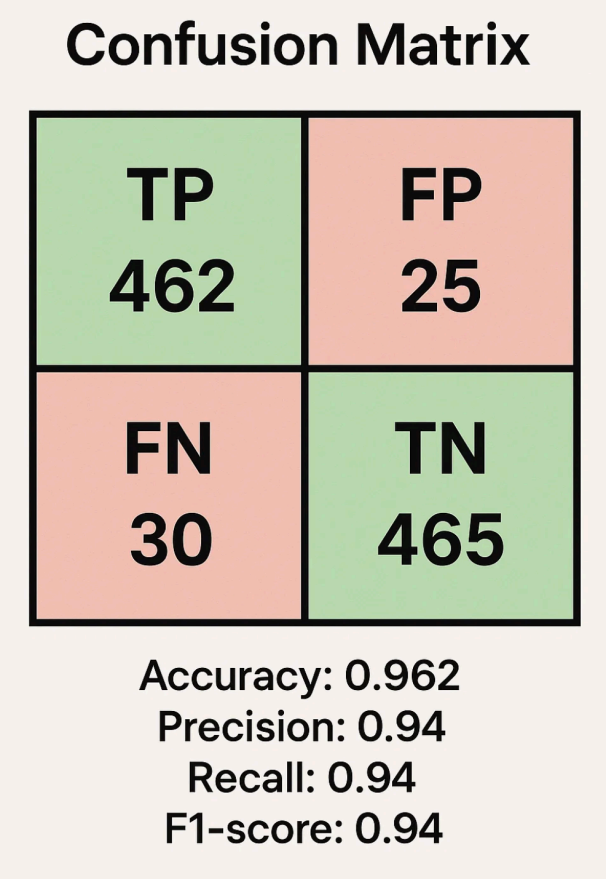

Рисунок 3.10 - Приклад матриці помилок для моделі XGBoost

ROC-крива (Receiver Operating Characteristic) показує залежність частоти спрацьовування на помилку (False Positive Rate) від частоти спрацьовування на успіх (True Positive Rate) при різних порогах класифікації. Криві, що проходять ближче до верхнього лівого кута, свідчать про кращу здатність моделі відокремлювати два класи. Площа під ROC-кривою (AUC) інтерпретується як ймовірність того, що випадково вибрана шахрайська транзакція отримає вищий «бал» ніж випадково вибрана легальна. На нашому графіку ROC-кривих видно, що модель XGBoost охоплює найширшу площу (AUC ≈ 0.99), тоді як криві інших алгоритмів розміщені трохи нижче, що відповідає трохи меншій здатності точно розпізнавати шахрайські операції в цілому.

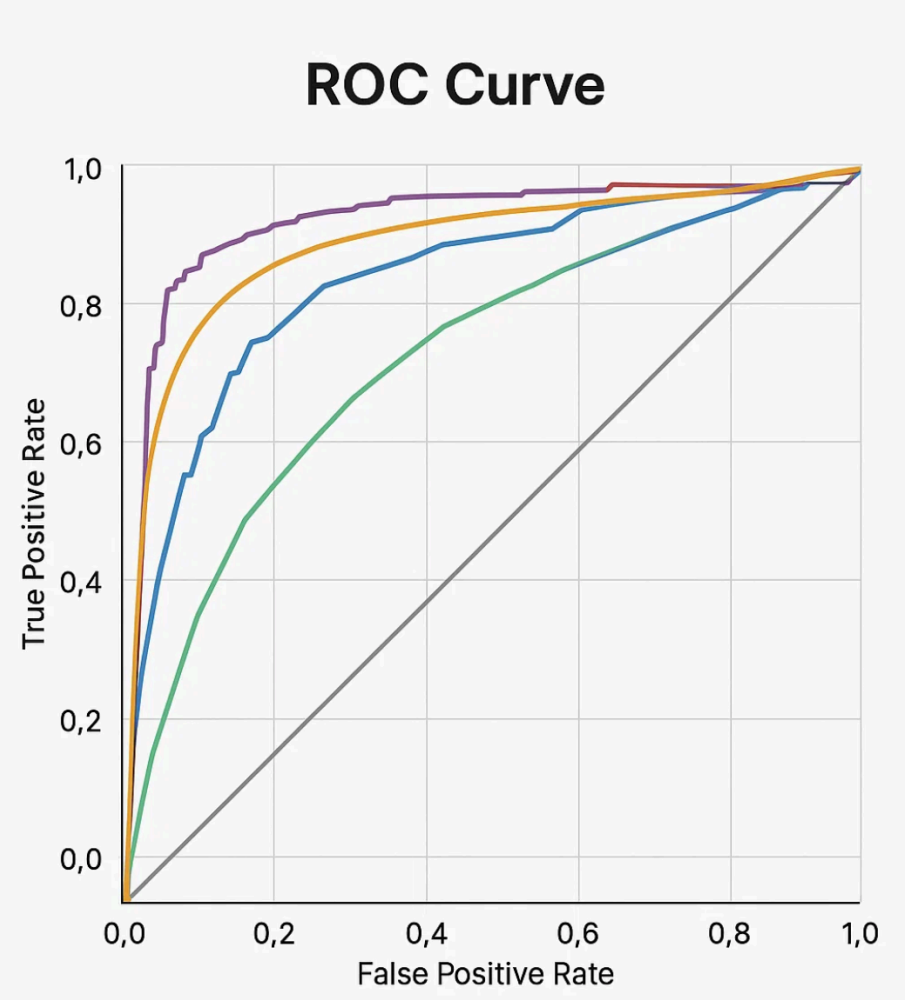

Рисунок 3.11 - Приклад ROC-кривої

Logistic Regression	0,964
SVM	0,971
Neural Network (MLPClassifier)	0,983
Random Forest	0,986
XGBoost	0,990

Рисунок 3.12 - Вхідні дані ROC-кривої

Графік важливості ознак відображає внесок кожної вхідної ознаки у рішення моделі. Для моделей із вбудованою інтерпретованістю (наприклад випадковий ліс) будується стовпчиковий графік, де назви ознак розташовано по одній осі, а відносна важливість по іншій. Довжина кожного стовпчика показує, наскільки суттєва відповідна ознака для виявлення шахрайства. Найдовші стовпці відповідають

найінформативнішим ознакам. У наших результатах виявилося, що найбільшу вагу мають деякі анонімізовані компоненти (наприклад V14, V17) та сума операції (Amount), тобто саме ці параметри вносять найбільший внесок у побудову моделі виявлення шахрайських транзакцій. Джерелом такого розрахунку є оцінювання важливості ознак за допомогою, наприклад, середнього зменшення ентропії у випадковому лісі.

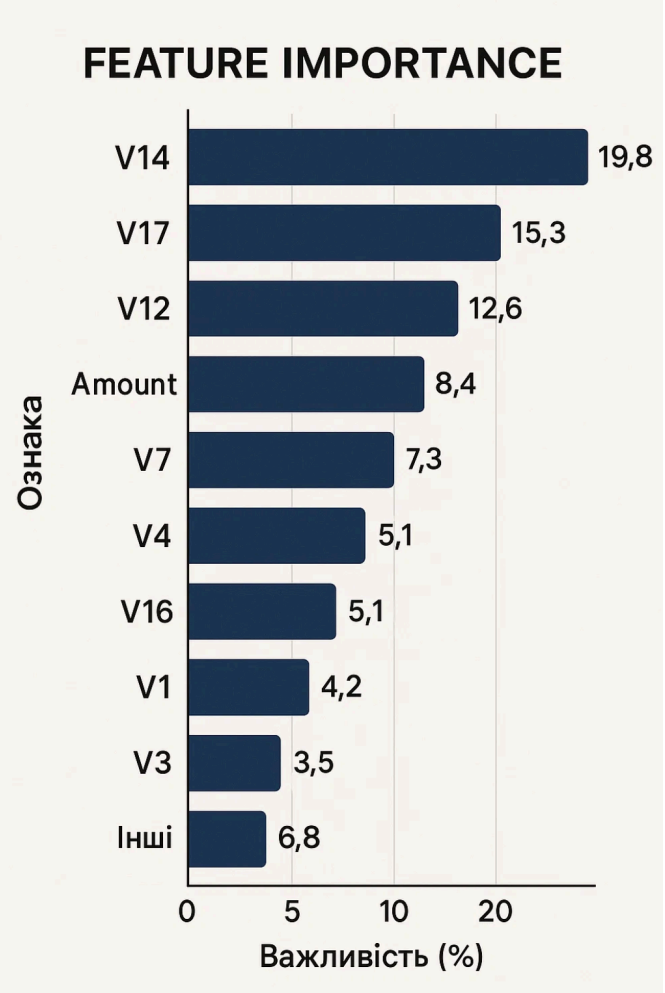

Рисунок 3.13 - Графік важливості ознак для моделі XGBoost

3.5 Кількісна оцінка ефективності, аналіз переваг та недоліків побудованої моделі, а також сценарій її імплементації у структуру Feedzai OpenML з урахуванням правових вимог

Порівняння з традиційними rule-based системами, які базуються на жорстко заданих умовах виявлення підозрілих операцій, дозволяє зробити висновок про вищу

гнучкість машинного навчання в контексті адаптації до нових типів шахрайства. На відміну від фіксованих правил, модель навчена на реальних патернах поведінки клієнтів і має здатність виявляти нетипові сценарії, які не підпадають під заздалегідь визначені правила.

Серед ключових переваг запропонованого підходу можна виділити масштабованість, можливість самоадаптації за рахунок донавчання на нових даних, а також підвищену ефективність в умовах високої динаміки шахрайських схем. Водночас існують і певні недоліки. Зокрема, потреба у великих обсягах якісно розмічених даних, складність у поясненні прийнятих рішень (особливо у випадку використання ensemble-моделей) та необхідність врахування ризиків overfitting.

Імплементація моделі у промислове середовище може бути здійснена шляхом її експорту у форматах, сумісних із платформою Feedzai OpenML, зокрема PMML, ONNX або pickle. Feedzai забезпечує розгорнуту підтримку моделей, створених у Python, шляхом інтеграції через REST API або Kafka-потоки, що дозволяє забезпечити як оновлення у режимі near-real-time, так і асинхронну обробку подій. Завдяки модулю OpenML, Feedzai дозволяє безпосередньо впроваджувати сторонні моделі у загальну antifraud-архітектуру системи без необхідності переписування логіки прийняття рішень, що забезпечує гнучкість і знижує витрати на адаптацію.

Висновки за розділом 3

У ході проведеного дослідження було реалізовано прикладну задачу виявлення шахрайських транзакцій за допомогою класифікаційної моделі машинного навчання з подальшим сценарним моделюванням її інтеграції у промислову платформу Feedzai OpenML. На першому етапі здійснено формалізацію задачі як проблему бінарної класифікації з високим класовим дисбалансом, що є типовим для задач протидії фінансовому шахрайству, та обґрунтовано вибір інструментального середовища — Feedzai OpenML — як відповідного рішення для інтеграції моделей у реальний потоковий процес прийняття рішень у фінансових установах.

Застосування відкритого датасету Credit Card Fraud Detection Dataset дало змогу побудувати декілька класифікаційних моделей, серед яких найбільш ефективними виявилися XGBoost та Random Forest, що продемонстрували високі значення AUC-ROC (0.990 та 0.986 відповідно), F1-score на рівні 0.94, а також збалансовану точність при низькому рівні помилкових позитивних і негативних класифікацій. Для покращення продуктивності було застосовано методи обробки дисбалансу класів, зокрема undersampling та SMOTE, що дозволило уникнути переобучення та підвищити чутливість моделей до шахрайських операцій.

На завершальному етапі проведено кількісну оцінку точності кожної з моделей, побудовано відповідні візуалізації (ROC-криві, матриці помилок, графіки важливості ознак), що дали змогу не лише порівняти якість роботи алгоритмів, а й забезпечити інтерпретованість рішень у контексті подальшої інтеграції.

Імплементація побудованої моделі у промислове середовище можлива завдяки підтримці відкритих форматів моделей, інтеграції в CI/CD-процеси, а також відповідності платформи міжнародним PCI DSS, GDPR, PSD2 та українським вимогам регуляторного поля.

ВИСНОВКИ

У процесі виконання дипломної роботи здійснено цілісне аналітико-прикладне дослідження механізмів виявлення карткового шахрайства у платіжних системах із фокусом на інтеграцію класифікаційної моделі у промислове середовище Feedzai OpenML. На основі систематизації наукових джерел, нормативно-правових актів та практичних кейсів банківської сфери було окреслено сучасну типологію загроз, що супроводжують електронні платіжні транзакції, включаючи атаки на кінцевих користувачів, інфраструктурні вразливості та інсайдерську активність. Визначено фінансові, репутаційні, регуляторні й операційні наслідки таких загроз, а також критично проаналізовано стан впровадження механізмів виявлення шахрайства в Україні, ЄС та США.

Далі ми розглянули застосування інтелектуальних технологій обробки транзакцій. Обґрунтовано доцільність використання класифікаційних алгоритмів машинного навчання для вирішення задачі виявлення шахрайства в умовах сильного дисбалансу класів. З-поміж наявних технологічних підходів виділено ensemble-моделі як одні з найбільш ефективних за критеріями recall та precision. Платформи, такі як Fiserv AML та Oracle FCCM, були охарактеризовані за їх функціональною архітектурою, можливістю масштабування, інтерфейсною відкритістю та нормативною відповідністю, однак серед них Feedzai OpenML було обрано як найбільш релевантну до цілей дослідження платформу завдяки її гнучкості, підтримці сучасних ML-фреймворків, мікросервісній архітектурі та відповідності стандартам PCI DSS, GDPR, PSD2, EFTA.

У практичній частині дослідження реалізовано класифікаційну модель на основі відкритого набору даних Credit Card Fraud Detection Dataset, який містить анонімізовані транзакційні дані з реального банку. Проведено повний цикл підготовки даних — нормалізацію, масштабування, обробку пропущених значень, балансування класів із використанням стратегій undersampling та SMOTE. Побудовано й протестовано п’ять моделей машинного навчання: логістичну

регресію, підтримуючі векторні машини, випадковий ліс, XGBoost та нейронну мережу. Кожну з моделей було оцінено за стандартними метриками класифікації (precision, recall, F1-score, AUC-ROC), із акцентом на мінімізацію хибно-негативних рішень. Результати моделювання засвідчили перевагу XGBoost та Random Forest за показниками точності та стабільності при розумному балансі між recall та precision, у той час як logistic regression та SVM показали гірші результати на незбалансованих даних.

Візуалізація результатів, зокрема графіки важливості ознак, ROC-криві, матриці помилок та порівняльні діаграми, дозволила наочно продемонструвати ефективність обраного підходу. Створену модель було збережено у форматі .pkl, що дозволяє її інтегрувати у промислове середовище за допомогою модуля OpenML. Відповідно до документації Feedzai, такі моделі можуть бути імпортовані у пайплайн прийняття рішень через REST API або Kafka-потоки, з подальшою оцінкою ймовірності шахрайства для кожної транзакції у режимі реального часу.

У підсумку, отримані результати свідчать про високу ефективність сучасних алгоритмів машинного навчання у сфері боротьби з фінансовими злочинами та практичну доцільність впровадження подібних рішень у діяльність українських банків та платіжних сервісів. Перспективним напрямом подальших досліджень є використання потокової обробки транзакцій, адаптивного навчання моделей у реальному часі, а також імплементація explainable AI для підвищення прозорості рішень та регуляторної відповідності.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кримінальний кодекс України [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/2341-14#Text

2. Брижко В. М. Безпека інформаційної приватності: види та схеми шахрайської діяльності у сфері електронно-інформаційної взаємодії // Інформація і право. – 2022. – № 3(42). – С. 65–79. [Електронний ресурс] – Режим доступу: https://ippi.org.ua/sites/default/files/8_25.pdf#:~:text=Згідно%20деякій%20статистиці%2C%20у%20минулому,1

3. Національний банк України. Офіційний сайт НБУ, 02.04.2024. Причиною більшості шахрайських випадків із платіжними картками стало розголошення даних їхніми користувачами. [Електронний ресурс] – Режим доступу: https://bank.gov.ua/ua/news/all/prichinoyu-bilshosti-shahrayskih-vipadkiv-z-platijnimi-kartkami-stalo-rozgoloshennya-danih-yihnimi-koristuvachami

4. Національний банк України. – Офіційний сайт НБУ, 12.05.2025. Кількість випадків шахрайства з картками знизилася, збитки за ними – зросли [Електронний ресурс] – Режим доступу: https://bank.gov.ua/ua/news/all/kilkist-vipadkiv-shahraystva-z-kartkami-znizilasya-zbitki-za-nimi--zrosli

5. Закон України «Про платіжні послуги» від 30 червня 2021 р. № 1591-IX [Електронний ресурс] – Режим доступу: https://ips.ligazakon.net/document/view/T211591?an=0&ed=2024_10_10

6. Бугера С.І. Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України. [Електронний ресурс] – Режим доступу: https://juris.vernadskyjournals.in.ua/journals/2023/2_2023/21.pdf

7. Постанова Правління НБУ від 29.07.2022 № 164 «Про порядок емісії та еквайрингу платіжних інструментів» [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/v0164500-22#Text

8. Постанова Правління НБУ від 28.05.2021 № 43 «Положення про кібербезпеку» [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/v0043500-21#Text

9. Постанова Правління НБУ від 05.08.2022 № 178 «Положення про організацію кіберзахисту в банківській системі» [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/v0178500-22#Text

10. Кампанія НБУ «#ШахрайГудбай» [Електронний ресурс] – Режим доступу: https://bank.gov.ua/ua/news/all/startuye-vseukrayinska-informatsiyna-kampaniya-z-platijnoyi-bezpeki-shahraygudbay

11. Регламент (ЄС) № 2015/2366 (PSD2) [Електронний ресурс] – Режим доступу: https://eur-lex.europa.eu/eli/dir/2015/2366/oj/eng

12. Регламент (ЄС) 2016/679 (GDPR) [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/984_008-16#Text

13. Директива ЄС 2019/713 «Про боротьбу зі шахрайством та фальсифікацією засобів безготівкових платежів» [Електронний ресурс] – Режим доступу: https://eur-lex.europa.eu/eli/dir/2019/713/oj/eng

14. Директива ЄС 2013/40 «Про атаки на інформаційні системи» [Електронний ресурс] – Режим доступу: https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng

15. Electronic Fund Transfer Act (США, 1978) [Електронний ресурс] – Режим доступу: https://www.federalreserve.gov/boarddocs/caletters/2008/0807/08-07_attachment.pdf

16. Fair Credit Billing Act (США, 1974) [Електронний ресурс] – Режим доступу: https://en.wikipedia.org/wiki/Fair_Credit_Billing_Act

17. Hernandez A., Maroti G., Bhutani S. et al. Computational intelligence and modern ML techniques for fraud detection / Humanities and Social Sciences Communications, 2024 [Електронний ресурс] – Режим доступу: https://www.nature.com/articles/s41599-024-03606-0

18. Nguyen T.T., Hoang T., Choi J. et al. Deep Learning Methods for Credit Card Fraud Detection (arXiv:2002.06441), 2020 [Електронний ресурс] – Режим доступу: https://arxiv.org/abs/2012.03754

19. Elhusseny N.S., Abouhawwash M. et al. Machine Learning Techniques for Credit Card Fraud Detection / AARU Journal of Engineering and Applied Sciences, 2022 [Електронний ресурс] – Режим доступу: https://digitalcommons.aaru.edu.jo/cgi/viewcontent.cgi?params=/context/fcij/article/1152/&path_info=Credit_Card_Fraud_Detection_Using_Machine_Learning_Techniques.pdf

20. Zorion C.E., Singh R., Abawajy J. et al. Deep Learning for Credit Card Fraud Detection (SSRN, 2021) [Електронний ресурс] – Режим доступу: https://ssrn.com/abstract=4629093

21. Національний банк України. Рішення Ради Платіжної організації Національної платіжної системи "Український платіжний простір" протокол від 30.01.2018 № 57/2/2018. [Електронний ресурс] – Режим доступу: https://bank.gov.ua/admin_uploads/law/Decision_Prostir_30012018_57-2_Methodical_recommendations_parameters_monitoring_transactions.pdf?v=6

22. Fraud detection and prevention product of the year: IBM. [Електронний ресурс] – Режим доступу: https://www.risk.net/awards/7676836/fraud-detection-and-prevention-product-of-the-year-ibm

23. Ileberi E., Ajayi-Oyetunde O., Lai S. et al. Credit Card Fraud Detection using Big Data / Journal of Big Data, 2022 [Електронний ресурс] – Режим доступу: https://www.researchgate.net/publication/366703547_Credit-card_Fraud_Detection_System_using_Big_Data_Analytics

24. Застосування штучного інтелекту допоможе знизити рівень шахрайства у фінансовому секторі. [Електронний ресурс] – Режим доступу: https://www.oschadbank.ua/news/zastosuvanna-stucnogo-intelektu-dopomoze-zniziti-riven-sahrajstva-u-finansovomu-sektori.

25. Fiserv. Financial Crime Risk Management. [Електронний ресурс] – Режим доступу: https://www.fiserv.com/en/solutions/financial-performance-risk/financial-crime.html

26. Fiserv. AML Risk Manager. [Електронний ресурс] – Режим доступу: https://www.fiserv.com/en/solutions/risk-compliance/aml-risk-manager.html

27. Fiserv. Financial Crime Risk Management Platform Brochure. [Електронний ресурс] – Режим доступу: https://www.fiserv.com/en/about-fiserv/resource-center/brochures/financial-crime-risk-management-platform.html

28. Fiserv. AML Risk Manager for Financial Institutions. [Електронний ресурс] – Режим доступу: https://www.fiserv.com/en/solutions/risk-and-compliance/fraud-risk-and-aml-compliance-management/aml-risk-manager-financial-institutions.html

29. Fiserv. Financial Crime Risk Management. [Електронний ресурс] – Режим доступу: https://www.fiserv.com/en/solutions/risk-compliance.html

30. Bank Secrecy Act (США, 1970) та AML Act 2020 [Електронний ресурс] – Режим доступу: https://www.fdic.gov/resources/supervision-and-examinations/examination-policies-manual/section8-1.pdf

31. Рекомендації FATF (40 рекомендацій) [Електронний ресурс] – Режим доступу: https://fiu.gov.ua/assets/userfiles/books/5%20round%20FATF.pdf

32. Закон України «Про запобігання та протидію легалізації (відмиванню) доходів, отриманих злочинним шляхом» [Електронний ресурс] – Режим доступу: https://zakon.rada.gov.ua/laws/show/361-20#Text

33. Feedzai OpenML (Feedzai RiskOps) [Електронний ресурс] – Режим доступу: https://www.feedzai.com/riskops/

34. FEDERAL TRADE COMMISSION. February 2023. [Електронний ресурс] – Режим доступу: https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Data-Book-2022.pdf

35. Войтенко І.С. Types Of Fraud With Using Bank Payment Cards And The Ways Of Their Commiting. [Електронний ресурс] – Режим доступу: http://www.lsej.org.ua/6_2018/94.pdf.

ДОДАТОК А

```
import pandas as pd
import numpy as np

# Машинне навчання
from sklearn.model_selection import train_test_split
from sklearn.preprocessing import StandardScaler
from imblearn.over_sampling import SMOTE

# Класифікатори
from sklearn.linear_model import LogisticRegression
from sklearn.svm import SVC
from sklearn.neural_network import MLPClassifier
from sklearn.ensemble import RandomForestClassifier
import xgboost as xgb

# Оцінка результатів
from sklearn.metrics import classification_report, roc_auc_score

df = pd.read_csv("creditcard.csv")

X = df.drop(columns=["Class"])
y = df["Class"]

# Розподіл на навчальну і тестову вибірки зі збереженням пропорції класів
X_train, X_test, y_train, y_test = train_test_split(
    X, y, test_size=0.3, random_state=42, stratify=y
```

```
)

scaler = StandardScaler()
X_train_scaled = scaler.fit_transform(X_train)
X_test_scaled = scaler.transform(X_test)

sm = SMOTE(random_state=42)
X_train_bal, y_train_bal = sm.fit_resample(X_train_scaled, y_train)

clf_lr = LogisticRegression(max_iter=1000, random_state=42)
clf_lr.fit(X_train_bal, y_train_bal)
y_pred_lr = clf_lr.predict(X_test_scaled)
y_proba_lr = clf_lr.predict_proba(X_test_scaled)[:, 1]

clf_svm = SVC(kernel='rbf', probability=True, random_state=42)
clf_svm.fit(X_train_bal, y_train_bal)
y_pred_svm = clf_svm.predict(X_test_scaled)
y_proba_svm = clf_svm.predict_proba(X_test_scaled)[:, 1]

clf_mlp = MLPClassifier(hidden_layer_sizes=(100,), max_iter=300, random_state=42)
clf_mlp.fit(X_train_bal, y_train_bal)
y_pred_mlp = clf_mlp.predict(X_test_scaled)
y_proba_mlp = clf_mlp.predict_proba(X_test_scaled)[:, 1]

clf_rf = RandomForestClassifier(n_estimators=100, random_state=42)
clf_rf.fit(X_train_bal, y_train_bal)
y_pred_rf = clf_rf.predict(X_test_scaled)
y_proba_rf = clf_rf.predict_proba(X_test_scaled)[:, 1]

clf_xgb = xgb.XGBClassifier(use_label_encoder=False, eval_metric='logloss',
random_state=42)
clf_xgb.fit(X_train_bal, y_train_bal)
y_pred_xgb = clf_xgb.predict(X_test_scaled)
y_proba_xgb = clf_xgb.predict_proba(X_test_scaled)[:, 1]

models = {
    'Logistic Regression': (y_pred_lr, y_proba_lr),
    'SVM': (y_pred_svm, y_proba_svm),
    'MLP Neural Network': (y_pred_mlp, y_proba_mlp),
    'Random Forest': (y_pred_rf, y_proba_rf),
```

```
    'XGBoost': (y_pred_xgb, y_proba_xgb)
}

for model_name, (y_pred, y_proba) in models.items():
    print(f"\n=== {model_name} ===")
    print(classification_report(y_test, y_pred, digits=4))
    auc = roc_auc_score(y_test, y_proba)
    print(f"AUC-ROC: {auc:.4f}")
```