МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет імені В.Н. Каразіна

Факультет: **ННІ Каразінський банківський інститут**
Кафедра: **Інформаційних технологій та математичного моделювання**
Спеціальність: **125 Кібербезпека**
Освітня програма: **Кібербезпека у фінансових технологіях**
Група: АБ-41Б **денна форма навчання**

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему:

РОЗРОБКА ВДОСКОНАЛЕНОГО АЛГОРИТМУ ПРОТИДІЇ КІБЕРШАХРАЙСТВУ ТА ЗАХИСТУ ФІНАНСОВИХ ТРАНЗАКЦІЙ У СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

ЗА НАКАЗОМ № 4601-5/335 ВІД 07 ЛЮТОГО 2025 РОКУ

Здобувача вищої освіти **Довганя Олександра Олеговича**

Робота допущена до захисту в ЕК
протокол кафедри ІТММ № 13 від 31.05.2025р.

Завідувач кафедри ІТММ
к.п.н., доцент
_____ Н.І. Стяглик

Науковий керівник
к.т.н.
_____ А.В. Рогов

м. Харків 2025 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Харківський національний університет імені В. Н. Каразіна

Факультет навчально-науковий інститут "Каразінський банківський інститут"
Кафедра інформаційних технологій та математичного моделювання
Рівень вищої освіти перший (бакалаврський)
Спеціальність 125 Кібербезпека
Освітня програма Кібербезпека у фінансових технологіях

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ **Н. І. Стяглик**
Підпис ініціали, прізвище

"08" лютого 2025 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ (ПРОЄКТ)

Довганю Олександру Олеговичу
(прізвище, ім'я, по батькові студента)

1. Тема роботи: Розробка вдосконаленого алгоритму протидії кібершахрайству та захисту фінансових транзакцій у сучасних інформаційних системах.

керівник роботи Рогов Андрій Володимирович, к.т.н.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом по університету від "08" лютого 2025року № 4601-5/335

2. Строк подання студентом роботи 15 травня 2025 року

3. Перелік питань, які потрібно розробити:

У розділі 1: Розглянути сучасні проблеми кібершахрайства та засоби його протидії
У розділі 2: Процес розробки вдосконаленого алгоритму захисту фінансових транзакцій
У розділі 3: Врахування організаційно-технічних аспектів впровадження системи виявлення кібершахрайства
У розділі 4: Проведення дослідження та оцінки ефективності розробленого алгоритму

4.План роботи

№ з/п	Назви етапів роботи
1	Вибір здобувачем теми кваліфікаційної бакалаврської роботи
2	Затвердження плану і завдання кваліфікаційної бакалаврської роботи
3	Здача кваліфікаційної бакалаврської роботи керівнику
4	Підпис кваліфікаційної бакалаврської роботи керівника
5	Підпис кваліфікаційної бакалаврської роботи у нормоконтролера
6	Допуск завідувачем кафедри до захисту кваліфікаційної бакалаврської роботи
7	Захист кваліфікаційної бакалаврської роботи

Дата видачі завдання 08 лютого 2025 року

Студент _____ Довгань О.О.
підпис ініціали, прізвище

Керівник роботи _____ Рогов А.В.
підпис ініціали, прізвище

РЕФЕРАТ
НА КВАЛІФІКАЦІЙНУ БАКАЛАВРСЬКУ РОБОТУ
«РОЗРОБКА ВДОСКОНАЛЕНОГО АЛГОРИТМУ ПРОТИДІЇ КІБЕРШАХРАЙСТВУ ТА ЗАХИСТУ ФІНАНСОВИХ ТРАНЗАКЦІЙ У СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ»
Довганя Олександра Олеговича

Кваліфікаційна бакалаврська робота містить 55 сторінок, 13 таблиць, 5 рисунків, список літератури з 25 найменувань.

Об'єктом дослідження є: процес забезпечення кібербезпеки в інформаційних системах фінансових транзакцій.

Предметом дослідження є: алгоритми виявлення та протидії кібершахрайству з використанням інтелектуальних технологій.

Мета кваліфікаційної бакалаврської роботи полягає у розробці та впровадженні вдосконаленого алгоритму, здатного виявляти шахрайські транзакції у фінансових системах з високою точністю в режимі реального часу.

Завданнями кваліфікаційної бакалаврської роботи є:

- дослідити види та методи кібершахрайства у сфері фінансових транзакцій;
- проаналізувати сучасні засоби захисту і виявити їх недоліки
- обґрунтувати вибір підходів до створення гібридної моделі виявлення шахрайства;
- розробити архітектуру алгоритму;
- реалізувати модель та провести експериментальну перевірку;
- оцінити ефективність алгоритму та надати рекомендації щодо впровадження.

Актуальність дослідження:

У сучасному цифровому середовищі кількість кібершахрайських дій у сфері фінансів постійно зростає. Стандартні системи захисту вже не відповідають новим викликам, тому впровадження адаптивних інтелектуальних алгоритмів виявлення шахрайства є критично необхідним для забезпечення надійності платіжних систем.

За результатами дослідження було реалізовано гібридну модель виявлення шахрайських транзакцій, яка поєднує rule-based фільтрацію та машинне навчання. Отримані результати свідчать про високу точність моделі: Precision = 0.92, Recall = 0.86.

Практична новизна: запропоновано гнучкий алгоритм з можливістю подальшого самонавчання та адаптації до нових типів загроз, що дозволяє ефективно виявляти шахрайські операції в умовах реального часу.

Одержані результати можуть бути використані у фінансових установах, платіжних системах, банківському ПЗ та інших сферах, де потрібен захист від кібершахрайства.

КЛЮЧОВІ СЛОВА: Кібершахрайство, фінансові транзакції, алгоритм виявлення, машинне навчання, rule-based система, кібербезпека.

ABSTRACT
AT QUALIFICATION BACHELOR WORK
«DEVELOPMENT OF AN ADVANCED ALGORITHM FOR COUNTERING CYBER FRAUD AND PROTECTING FINANCIAL TRANSACTIONS IN MODERN INFORMATION SYSTEMS»

Dovhan Oleksandr

The bachelor's thesis contains 55 pages, 13 tables, 5 drawings, a list of references of 25 titles.

The object of the research is the process of ensuring cybersecurity in financial information systems.

The subject of the research is algorithms for detecting and preventing cyber fraud using intelligent technologies.

The purpose of a bachelor's qualification work is to develop and implement an advanced algorithm capable of detecting fraudulent transactions in financial systems in real time with high accuracy.

The tasks of a bachelor's degree are:

- to analyze types and methods of cyber fraud in the field of financial transactions;
- to review and evaluate existing protection mechanisms;
- to justify the selection of a hybrid approach for fraud detection;
- to design and implement the architecture of the algorithm;
- to test the model on real and synthetic data;
- to formulate recommendations for implementation.

The relevance of the research lies in the growing frequency and sophistication of cyber fraud in the financial sector, which requires adaptive and intelligent methods for identifying and neutralizing new threats in real time.

According to the results of the research: a hybrid model was developed that combines rule-based filtering and machine learning techniques. The model achieved high performance indicators (Precision = 0.92, Recall = 0.86), demonstrating effectiveness in detecting both obvious and hidden fraud patterns.

Main theoretical provisions on the topic of the practical relevance of the study confirm the feasibility of implementing such systems in real-world payment and financial services to reduce financial losses and improve user trust.

The results obtained can be used in banking software, financial platforms, fintech services, and online payment systems for automated fraud monitoring and prevention.

KEYWORDS: cyber fraud, financial transactions, machine learning, hybrid algorithm, information security, anomaly detection.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧОК, СИМВОЛІВ І ТЕРМІНІВ

AI – Artificial Intelligence (штучний інтелект).

AUC-ROC – Area Under the Receiver Operating Characteristic Curve (площа під кривою характеристик класифікатора).

CSV – Comma-Separated Values (текстовий формат даних).

F1-score – Гармонічне середнє між точністю (Precision) і повнотою (Recall).

False Positive (FP) – хибнопозитивне спрацювання (нормальна транзакція класифікована як шахрайська).

False Negative (FN) – хибнонегативне спрацювання (шахрайська транзакція класифікована як нормальна).

ML – Machine Learning (машинне навчання).

MFA – Multi-Factor Authentication (багатофакторна автентифікація).

NLP – Natural Language Processing (обробка природної мови).

Precision – показник точності виявлення позитивного класу (відсоток дійсно шахрайських транзакцій серед тих, що були відмічені як шахрайські).

Recall – чутливість класифікатора (відсоток виявлених шахрайських транзакцій серед усіх шахрайських).

RF – Random Forest (ансамблевий алгоритм машинного навчання).

Rule-based system – система на основі фіксованих правил.

TP / TN – True Positive / True Negative (правильні класифікації шахрайства або нормальної транзакції).

XGBoost – Extreme Gradient Boosting (ефективний алгоритм ансамблевого навчання).

ВСТУП

Сучасне суспільство стрімко переходить до цифрового середовища, де більшість повсякденних процесів – від спілкування до здійснення фінансових операцій – реалізуються через інформаційні системи. Особливо динамічно розвивається фінансовий сектор, де електронні платежі, онлайн-банкінг, мобільні додатки та інші цифрові сервіси стали не лише популярними, а й життєво необхідними для функціонування економіки. Разом з тим, ці процеси супроводжуються зростанням кіберзагроз, серед яких особливе місце займає кібершахрайство.

Кібершахрайство – це один з найнебезпечніших і водночас найдинамічніших видів кіберзлочинності, що спрямований на незаконне заволодіння коштами, особистими або фінансовими даними користувачів шляхом використання технічних вразливостей, соціальної інженерії чи підроблених цифрових середовищ. Статистика міжнародних організацій свідчить про щорічне зростання кількості атак, спрямованих на фінансові установи, платіжні системи та електронну комерцію. Згідно з даними консалтингових агентств, світові збитки від фінансових кібершахрайств у 2023 році перевищили 50 мільярдів доларів США.

Традиційні методи захисту – такі як багатофакторна автентифікація, обмеження транзакцій за географічними чи часовими рамками, системи на основі фіксованих правил – поступово втрачають свою ефективність. Це пов’язано з тим, що шахрайські схеми стають все більш гнучкими, автоматизованими та адаптивними, використовуючи у своїй структурі технології штучного інтелекту, бот-мережі, фальсифіковані документи та поведінкове моделювання користувачів.

У зв’язку з цим постає потреба у створенні більш інтелектуальних та адаптивних механізмів виявлення аномальної поведінки користувача та транзакцій, здатних самостійно навчатися і реагувати на нові типи шахрайства. Особливої уваги заслуговують підходи, засновані на методах

машинного навчання та аналізу великих даних, які вже продемонстрували свою ефективність у суміжних галузях: кіберзахист, медична діагностика, прогнозування ринків тощо.

Актуальність теми дипломної роботи полягає у необхідності практичного вирішення проблеми забезпечення інформаційної безпеки в умовах цифрової трансформації фінансового сектору. Створення гібридного алгоритму, який поєднує переваги rule-based логіки та адаптивності машинного навчання, дозволить підвищити точність виявлення шахрайства, зменшити кількість хибнопозитивних спрацювань та забезпечити захист користувачів у режимі реального часу.

Метою даної дипломної роботи є розробка вдосконаленого алгоритму для виявлення та протидії шахрайським транзакціям у сучасних інформаційних системах з використанням інтелектуальних методів аналізу.

Завдання дослідження:

- провести аналіз сучасного стану проблеми кібершахрайства у фінансовій сфері;

- дослідити існуючі методи захисту та виявлення шахрайських дій;

- обґрунтувати вибір гібридної архітектури алгоритму;

-розробити модель виявлення шахрайства на основі машинного навчання;

- провести тестування моделі на реальних і симуляційних даних;

- порівняти результати з традиційними підходами та сформулювати рекомендації для впровадження.

Об’єктом дослідження є інформаційні системи обробки фінансових транзакцій.

Предметом дослідження є алгоритми виявлення та протидії кібершахрайству з використанням машинного навчання.

Практичне значення роботи полягає у можливості застосування розробленого алгоритму в реальних умовах – у банківських системах,

платіжних платформах, онлайн-магазинах та інших сферах, де проводиться обробка фінансових операцій.

Таким чином, запропоноване дослідження відповідає актуальним викликам цифрової епохи, спрямоване на підвищення рівня кіберзахисту в Україні та сприяє впровадженню інноваційних підходів у боротьбі з кіберзлочинністю.

РОЗДІЛ 1
СУЧАСНІ ПРОБЛЕМИ КІБЕРШАХРАЙСТВА ТА ЗАСОБИ ЙОГО ПРОТИДІЇ

1.1. Кібершахрайство та його класифікація

Кібершахрайство – це маніпуляції з комп'ютерними даними або програмами, такі як знищення, зміна, виправлення або спроба завадити процесу обробки інформації, що негативно впливає на остаточний результат. Вони можуть спричиняти фінансові, майнові та економічні збитки метою яких є незаконне одержання прибутку у вигляді коштів.

За допомогою обману при такому шахрайстві кінцевим наміром є отримання чужого майна або право володіння на нього, коштів, документів тощо. Саме вчинення «крадіжки» за допомогою використання засобів цифрової техніки є неможливим, тому що це таємне розкрадання чужого майна. Кібершахрайство в Україні розглядається як злочин який карається згідно статті 190 ККУ.

Існує класифікація кіберзлочинів, до якої входять:

1) правопорушення проти конфіденційності, доступності та цілісності комп'ютерних даних, такі як:

- незаконне перехоплення комп'ютерних даних;
- втручання у систему, створення перешкод для подальшого функціонування комп'ютерної системи шляхом кібератак на інформаційну інфраструктуру;
- незаконний доступ до інформації шляхом зламування або обману;
- втручання у дані, навмисне пошкодження, зміна, приховування, знищення комп'ютерної інформації без офіційного права на ці дані;
- виготовлення, продаж, використання пристроїв, комп'ютерних програм, паролів або кодів доступу з метою здійснення кіберзлочинів.

2) правопорушення підробки та шахрайства які були вчинені за допомогою використання комп’ютера.

3) правопорушення авторських прав, незаконне використання і відтворення комп’ютерних програм, відео або аудіо продукції, баз даних або книг;

4) правопорушення за змістом інформації, такі як расизм, дитяча порнографія, ксенофобія.

Також кіберзлочини можна розділити на деякі категорії з урахуванням мотивації злочинців, а саме: кібершахрайство з метою заволодіння інформацією для продажу або власного використання; кібершахрайство з метою заволодіння коштами; отримання доступу та втручання до інформаційних систем задля отримання доступу до системи управління для подальшого пошкодження або для нанесення шкоди за винагороду; також інші злочини.[1]

Таблиця 1.1

Основні види шахрайств та їх опис

Вид шахрайства	Опис	Приклад
Фішинг	Шахрайство через підроблені сайти або листи для крадіжки даних	Email-лист від «банку»
Скімінг	Зчитування даних картки через фальшиві пристрої	Банкомат з «накладкою»
Вішинг	Спам-дзвінки від «банку»	«оператор служби безпеки»

Інсайдерські атаки	Шахрайство за участі працівників фінансової установи	Злив бази клієнтів
Bot-форд	Масова генерація транзакцій з метою викрадення коштів	Боти у мобільному банкінгу

1.2. Основні види шахрайства у фінансових транзакціях

Існує певна категорія злочинів, метою якої є привласнення грошових коштів, при якому шахраї можуть використовувати різні способи змушуючи користувачів самостійно розкривати конфіденційні дані – це перша категорія злочинів.

Друга та третя категорія – це зламування баз даних, виведення з ладу комп'ютерних систем компаній та державних організацій, крадіжка технологій.

Найбільш популярними є кіберзлочини, наслідком яких виникає матеріальна або фінансова вигода для шахраїв у вигляді незаконних доходів. Особливо небезпечними буває використання комунікаційних, інформаційних систем та комп'ютерних технологій щоб отримати доступ до приватної власності фізичних та юридичних осіб для подальших дій з розпорядження або управління цією власністю.

У сьогоденні набувають чинності кіберзлочини за допомогою яких є отримання доступу до клієнтської бази банківських установ. У цій категорії найбільш поширеними є наступні види злочинів:

- шахрайство в інтернеті, а саме: поширення комп'ютерних вірусів, троянських програм, перехоплення трафіку (з метою розкрадання фінансової або персональної інформації); шахрайство при продажі товарів, послуг, через мережу Інтернет або на «Інтернет-аукціонах»; створення фінансових «пірамід»;

- банкоматне шахрайство, підробка платіжних карток, зокрема: викрадення реквізитів платіжних карток із застосуванням засобів для їх «клонування»; використання втрачених, підроблених або викрадених карток; установка на банкомати пристроїв зчитування/копіювання інформації з магнітної «стрічки» та отримання PIN-коду до цієї картки;

- шахрайство у системах банківського обслуговування – проведення несанкціонованих операцій, відкриття рахунків, отримання готівкових коштів, отримання платежів від іноземних відправників через міжнародну систему SWIFT внаслідок втручання в роботу комп'ютерних систем клієнтів іноземних банківських установ.[2]

Із розвитком сфери інформаційних технологій постійно генеруються нові види послуг, у тому числі в фінансовій сфері. Але злочинці також не сидять на місці, вони удосконалюють свої здібності, придумують нові способи незаконного заробітку у цифровому просторі.

Рис. 1.1. Класифікація кіберзагроз у фінансовій сфері

1.3. Існуючі підходи до виявлення та протидії кібершахрайству

Виявлення та протидія кібершахрайству – це комплексна задача, яка включає в себе декілька важливих аспектів. Існуючі підходи до її вирішення виходять від технічних заходів, таких як використання антивірусного забезпечення та фільтрів для безпеки мережі, до організаційних заходів, зокрема розвитку національних органів боротьби з кібершахрайством та розвитку законодавчої бази.

Наприклад, багато країн мають спеціальні служби, які займаються розслідуванням кібершахрайства та співпрацюють з інтернет-провайдерами та іншими організаціями для попередження та виявлення злочинів.

Усі підходи можна поділити на три основні категорії:

- поведінкові;
- статичні;
- інтелектуальні.

Поведінкові методи дають здатність аналізувати характеристики користувача, наприклад: пристрої, геолокацію, час активності, користування сервісами тощо. Якщо виявляється якась проблема, система може ініціювати блокування певної операції або зробити додаткову перевірку. Основна перевага цього методу у тому, що система адаптується до певного користувача, але є і недоліки, у системі можуть відбуватися збої у разі зміни поведінки користувача.

Статичні методи використовуються на основі попередніх даних про транзакції для побудови поведінки користувача. Так звані «аномалії» виявляються за допомогою порівняння транзакцій за шаблонами. Незважаючи на те що цей метод доволі простий, він має занизьку чутливість до нових типів кібератак та схильний до великої кількості хибних або позитивних рішень.

Інтелектуальні методи являються найбільш безпечними та перспективними у сьогоденні. За допомогою них можна виявити найскладніші методи шахрайства методом аналізу великого масиву даних. Серед

найпоширеніших можна віднести нейронні мережі, логістична регресія та дерева рішень. Найбільша перевага цього методу – це високоточне виявлення шахрайських операцій, але для цього потрібний якісний набір даних та обчислювальних ресурсів.

Слід підмітити те, що дуже важливу роль у протидії кібершахрайству також відіграють системи багатофакторної автентифікації, біометрична ідентифікація, шифрування даних, технологія поведінкової біометрії та використання «токенів».

Чітка реалізація системи захисту найчастіше передбачає комбінацію декількох методів. Завдяки цьому можна компенсувати недоліки до кожного підходу та отримати змогу досягти найвищого рівня надійності та стійкості до кіберзагроз.[3]

Рис. 1.2. Динаміка зростання випадків кібершахрайства

1.4. Аналіз недоліків традиційних методів захисту

Нажаль, традиційні методи захисту інформаційних систем, зокрема у сфері фінансових транзакцій, з часом поступово їх ефективність знижується через постійну загрозу складних кібератак, які у свою чергу зростають. Існує багато рішень які демонструють обмежену здатність адаптування до нових способів шахрайства та забезпечення надійного захисту в умовах цифрового середовища.

Є декілька основних недоліків традиційних методів захисту які можна виділити, це:

- обмеження в обробці великого обсягу даних – традиційні методи захисту не завжди здатні обробляти транзакції у великому обсязі, що є дуже важливим та критичним для виявлення кібератак;

- низька адаптивність до нових загроз – більшість систем створені на чітких правилах, які стають ефективними тільки тоді, коли є вже відомий тип кібершахрайства. Коли з’являється новий спосіб «обманути» систему, цей спосіб стає безпомічним;

- недостатній рівень персоналізації – захист існує тільки на власних загальних правилах і не може враховувати індивідуальні характеристики користувача, через це знижується ефективність виявлення «аномальної» поведінки;

- висока кількість хибних або позитивних спрацювань – дуже часто системи можуть виявляти підозрілі транзакції, які насправді є легітимними, що спричиняє до незручностей для користувача і зниження довіри до «платформи»;

- складність сумісності з новими технологіями – існує багато «застарілих» систем захисту, які не можуть підтримувати сумісність з сучасними рішеннями на основі поведінкової аналітики, що може обмежувати їхній подальший розвиток;

- повна відсутність можливості самонавчання – більшість традиційних рішень не містять у собі можливість самовдосконалення, через це обмежується ефективність реагування на зміни у поведінці користувача або появу нових кібератак.

Через це ефективність протидії сучасним кіберзагрозам від традиційних, статичних та реактивних методів до нових адаптивних та інтелектуальних систем, які будуть здатні на швидке реагування до виявлення нових видів кібершахрайства та самостійного прийняття рішень.[4]

1.5. Висновки за розділом

У першому розділі ми провели аналіз сьогоденних проблем кібершахрайства у сфері фінансових транзакцій. Було визначено одні з основних видів дій шахраїв, підкреслено важливі недоліки традиційних підходів до захисту інформаційних систем та проаналізовано найефективніші методи протидії.

Більшість знайомих нам вже існуючих систем є обмежено ефективними в умовах зростання складності кібератак. Ці системи не можуть забезпечувати високий рівень адаптивності, можуть мати високу кількість позитивних або хибних спрацювань, погано працюють з великими базами даних та не враховують індивідуальну особливість кожного користувача.

Згідно цих висновків виникає необхідність щодо розробки нових алгоритмів захисту, які зможуть ефективно виявляти шахрайські дії, адаптуватися до нових незнайомих загроз та робити високоточні аналізи транзакцій.

У наступних розділах буде представлений концепт нового вдосконаленого захисного алгоритму, розглянутий процес проектування даного алгоритму, його реалізація та експериментальне дослідження.

РОЗДІЛ 2
ПРОЄКТУВАННЯ ТА РОЗРОБКА ВДОСКОНАЛЕНОГО АЛГОРИТМУ ЗАХИСТУ ФІНАНСОВИХ ТРАНЗАКЦІЙ

2.1. Постановка задачі та визначення вимог до системи

Метою даної дипломної роботи є розробка вдосконаленого алгоритму для протидії та виявлення шахрайським транзакціям у фінансових системах. Якщо враховувати те, що галузь інформаційної безпеки постійно отримує нові виклики та адаптується до сучасних тенденцій, розробка даного алгоритму має бути більш точною до виявлення кіберзагроз, забезпечувати адаптивність до нових типів таких загроз та містити менше позитивних або хибних спрацювань.

Основна задача полягає у створенні алгоритму, який у свою чергу буде здатний до автоматичного аналізу активності транзакцій, виявляти потенційні або аномальні шахрайські дії та вміти швидко реагувати на них.

Щоб досягти поставленої мети потрібно реалізувати деякі вимоги, а саме:

- обробка та збір даних транзакцій із різних доступних джерел;
- визначення з основними ознаками, які будуть найбільш інформативними задля виявлення шахрайства;
- класифікація транзакцій, виявлення аномалій за допомогою використання методів машинного навчання;
- можливість навчатися та адаптуватися до нових даних;
- виведення результатів із подальшою класифікацією транзакцій та рівнем довіри до них.

Також існують вимоги які є нефункціональними, вони включать:

- високу точність моделі;
- високу швидкість обробки;
- здатність роботи із великими базами даних;

- сумісність із сучасними IT-системами;

- захист фінансових та особистих даних користувачів.

Кінцевими даними для подальшої роботи системи можуть бути такі дані як: дата і час, сума транзакцій, історія транзакцій, IP-адреса користувача, геолокація, тип пристрою тощо.

У результаті, основна задача полягає у створенні певного інтелектуального модуля, який є сумісним із фінансовою системою, проводить аналіз будь-яких транзакцій та прийняття рішення у разі ймовірності кібершахрайства із максимально високою точністю.[5]

2.2. Обґрунтування вибору методів виявлення шахрайства

Щоб ефективно виявляти шахрайські фінансові транзакції, нам необхідно визначитися із відповідною методологією, яка в свою чергу може забезпечити високу точність, швидкість реагування та адаптацію до нових видів кіберзагроз.

Існують три основні методи та підходи для виявлення кібершахрайства у інформаційній безпеці: rule-based, ML(машинне навчання) та гібридні моделі. Кожен із цих методів має певні переваги, недоліки та особливості.

Rule-based методи.

Системи які основані на певних правилах функціонують по принципу попередніх чітко-визначених умов. Тобто, транзакція автоматично відображається як підозріла – здійснена з нестандартної локації, відбувається в нетиповий для користувача час або перевищує певну суму.

Перевагою цього методу є швидкість, простота реалізації та чітке прийняття самостійних рішень.

Недоліком цього методу є неможливість виявлення нових шаблонів шахрайства та низька гнучкість.

ML (методи машинного навчання).

Моделі цього методу дозволяють побудувати певну статистику, взявши за основу великий обсяг даних. Ці моделі здатні виявити складні зв’язки між певними ознаками транзакцій, які дуже важко або навіть неможливо задати вручну.

Серед найпоширеніших алгоритмів виділяють:

- нейронні мережі – здатність до автоматичного виявлення складних шаблонів, потребується велика кількість ресурсів та даних;

- логістична регресія – одна із найпростіших у реалізації, дуже добре підходить до бінарної класифікації;

- дерева рішень – з їх допомогою можна виявити взаємодії між атрибутами;

- метод опорних векторів – являється ефективним лише при високомірних даних.

Моделі машинного навчання дуже високоточні та мають здатність до самонавчання, але на етапах підготовки даних, побудови певних ознак або перенавчання – вимагають значних зусиль.

Гібридні підходи.

Комбіновані системи які поєднують у собі і rule-based і ML-моделі. Стандартний набір правил який може використовуватися для первинної оцінки, а потім для детального аналізу завдяки моделі машинного навчання.

Цей підхід здатний мінімізувати навантаження на модель та забезпечити високу продуктивність.

У даній роботі, щоб створити вдосконалений алгоритм, краще використовувати гібридний підхід, який містить у собі логіку чітких правил для швидкого реагування і фільтрування очевидних випадків та адаптивну модель машинного навчання задля подальшого глибокого аналізу транзакцій.

Це дозволить нам досягти високої точності при збереженні швидкості дій та великих масштабів системи.[6]

2.3. Архітектура та логічна схема роботи алгоритму

Для розробки певного ефективного алгоритму для протидії кібершахрайству потрібна чітка та структурована архітектура, яка дозволить гарантувати високу точність виявлення, масштабованість та можливість роботи у реальному часі.

Модельна архітектура гібридної системи виявлення шахрайства складається із декількох компонентів:

1) модуль збору даних – за допомогою цього модулю є можливість отримання транзакційних даних із зовнішніх та внутрішніх джерел, наприклад банківські системи, лог-файли, API тощо. Ці дані містять параметри та деталі транзакцій, технічні характеристики пристрою, профіль користувача та поведінкову інформацію.

2) модуль попередньої обробки – за допомогою цього модулю виконується очищення, трансформація, нормалізація та збагачення даних. На фоні цього відбувається генерація нових ознак, які можуть покращити роботу моделей машинного навчання.

3) Правилова система – відповідає за звичайну перевірку транзакцій по визначеним правилам (наприклад, країна походження, обмеження суми тощо). Якщо виявляється очевидний вид шахрайства, транзакція автоматично блокується.

4) Аналітичне ядро – за правилами, якщо транзакція була пропущена або не заблокована на попередньому етапі, вона автоматично передається моделі машинного навчання. Транзакція класифікується системою як безпечна або з певним ризиком підозрілою.

5) Модуль прийняття рішень – за допомогою оцінки моделі машинного навчання та отриманої інформації, система самостійно приймає кінцеве рішення, відхилити транзакцію, запитати додаткову перевірку(наприклад PIN-код) або підтвердити її.

6) Модуль зворотного зв’язку та навчання – за допомогою цього модулю система накопичує інформацію, а саме аналітику виконаних рішень, результати та інформацію про помилкові спрацювання. Отримані дані використовуються для подальшого «апгрейду» моделі, тим самим дозволяючи підвищити ефективність даної моделі. [7]

Схема роботи системи (послідовність):

1) Вхідна транзакція →

2) Первинна перевірка правил →

3) Передача на аналіз машинної моделі →

4) Визначення ризику →

5) Прийняття рішення →

6) Запис до журналу.

2.4. Технології та інструменти реалізації

Щоб реалізувати вдосконалений алгоритм виявлення шахрайських транзакцій треба обрати набір певних сучасних технологій, які здатні забезпечити надійність, масштабованність, гнучкість і підтримку машинного навчання. Вибір інструментів був створений з урахуванням ефективності, зручності інтеграції та сумісності з фінансовими системами.

1. Мови програмування:

- SQL – мова для взаємодії з базами даних для фільтрації, агрегації та вибірки транзакційних даних.

- Python – мова яка є основною для реалізації обробки даних, інтеграції модулів та реалізації алгоритмів машинного навчання.

2. Бази даних:

- MySQL – відповідає за зберігання історичних та транзакційних даних, логів роботи системи.

- Redis або MongoDB – відповідає за зберігання сеансів у реальному часі та для тимчасового кешування.

3. Бібліотеки і фреймворки:

- XGBoost – це алгоритм який є основним для побудови моделі, яка забезпечує високу швидкість і точність.

- Scikit-learn – реалізує моделі класифікації (дерева рішень, логістична регресія).

- Seaborn – візуалізує результати аналізу та оцінку ефективності моделі.

- Pandas – створений для обробки, підготовки даних та їх аналізу.

4. Інструменти розгортання та інтеграції:

- FastAPI – використовується для побудови REST API, який забезпечує взаємодію між зовнішніми системами та модулями – банківське ПЗ.

- Git – використовується для контролю спільної роботи над проектом та його версіями.

- Docker – застосовується для наповнення застосунку, завдяки чому дозволяє довільно розгортати систему у різних середовищах.

5. Середовища розробки:

- PyCharm або VS Code – створено для налагодження, а також написання коду

- Jupyter Notebook – створено для побудови прототипу, тестування моделей та дослідження даних.

6. Інструменти для оцінки ефективності:

- Аналіз важливості ознак для підвищення інтерпретованості

- Метрики, такі як: ROC-AUC, Precision, Accuracy.

- Крос-валідація, щоб перевірити стабільність моделі.

Розглянуті інтеграції дозволяють забезпечити реалізацію системи, яка адаптується під потреби конкретної фінансової установи.

Використання відкритих бібліотек може пришвидшити впровадження рішення та знизити вартість розробки.[8]

2.5 Висновки за розділом

У другому розділі було здійснено проектування вдосконаленого алгоритму виявлення шахрайських фінансових транзакцій, який враховує сучасні вимоги з інформаційної безпеки та функціонування в режимі реального часу. Було детально проаналізовано можливі засоби та підходи для виявлення кібершахрайства та обмірковано потребу щодо використання гібридної моделі, яка включає переваги rule-based систем та методи машинного навчання.

Було визначено функціонування вимог до системи щодо швидкодії, безпеки обробки даних, точності і масштабованості. Створено архітектуру майбутнього рішення, що містить аналіз транзакцій, прийняття рішень, модулі збору і попередньої обробки.

Розроблено структуру, яка створює основу для переходу до наступного етапу дослідження, а саме експериментальне тестування системи, оцінка показників продуктивності в умовах реального застосування, перевірка її ефективності на практичних прикладах.

РОЗДІЛ 3
ОРГАНІЗАЙЦІЙНО-ТЕХНІЧНІ АСПЕКТИ ВПРОВАДЖЕННЯ СИСТЕМИ ВИЯВЛЕННЯ ШАХРАЙСТВА

3.1. Вимоги до інфраструктури та технічне середовище

Для ефективного функціонування алгоритму виявлення шахрайських транзакцій необхідно забезпечити належне технічне середовище, яке відповідає вимогам до обробки великих обсягів даних, забезпечення високої доступності, безпеки та швидкодії. Архітектура системи повинна бути адаптованою до умов реального навантаження.

1) Програмне середовище

Розробка, навчання та тестування алгоритму здійснюється в середовищі Python 3.10, з використанням таких бібліотек:

- XGBoost, Scikit-learn – реалізація алгоритмів машинного навчання;
- Pandas, NumPy – обробка та трансформація даних;
- Matplotlib, Seaborn – візуалізація результатів;
- Flask, FastAPI – реалізація REST API для інтеграції моделі;
- Docker – контейнеризація системи для простого розгортання. [9]

2) Системні вимоги до обчислювального середовища

Для розгортання системи рекомендовано наступні технічні характеристики:

3) Підтримка обробки у реальному часі

Для забезпечення подальшої швидкої реакції на транзакційні запити необхідно:

- Використовувати поточну обробку даних – наприклад через Apache Kafka.
- Розміщення компонентів у контейнерах (Docker) для масштабування.
- Використання індексації та кешування (Redis/Memcached) для зменшення затримки.

4) Середовище навчання та донавчання моделі

Для навчання моделі використовуються:

- Jupyter Notebook / Colab для початкового аналізу.

- GPU-платформи або хмарні сервіси (Google Cloud, AWS, Azure) для навчання на великих обсягах.

Таблиця 3.1

Рекомендовані технічні характеристики системи

Компонент	Мінімальна конфігурація	Рекомендована конфігурація
CPU	4 ядра	8+ ядер
RAM	8 ГБ	16-32 ГБ
GPU	Не обов’язково	Бажано (для великих моделей ML)
SSD (сховище)	100 ГБ	250+ ГБ
ОС	Ubuntu 20.04+ / Windows server	Ubuntu / хмарне середовище

Модель повинна підтримувати періодичне перенавчання на нових транзакціях для адаптації до нових типів кібершахрайства.

Користувач (клієнт)

↓

Веб/мобільний додаток

↓

Платіжна система

↓

Antifraud API

↙ ↘

Модель ML Логи/Аудит

↓ ↓

База даних

Подана візуалізація показує зв’язок між користувачем та базою даних.

3.2. Безпека даних і правовий аспект зберігання

Ключовим аспектом при впровадженні системи виявлення кібершахрайських дій та транзакцій є необхідність забезпечити конфіденційності, цілісності та доступності даних. Особливо це може стосуватися фінансової інформації та персональних даних користувачів, які підпадають під дію національного та міжнародного законодавства. [10]

1) Категорії чутливих даних

Система може працювати з такими типами даних, як:

- Персональні ідентифікатори – ПІБ, ID користувача, номер картки.
- Транзакційна інформація – час, місце, сума, тип пристрою.
- Поведінкові шаблони – частота операцій, геолокація, часові ряди.

Ці дані підлягають захисту відповідно до норм Закону України «Про захист персональних даних», а також GDPR – у разі обробки інформації громадян ЄС.

2) Основні вимоги до захисту даних

3) Правові аспекти

В системі повинні бути реалізовані такі елементи відповідності правовим нормам:

- політика обробки персональних даних (Data Processing Policy)
- інформаційна згода користувача (в форматі договору/checkbox)
- вбудована підтримка для реалізації запитів щодо доступу, редагування або видалення даних (DSAR – Data Subject Access Request)

Таблиця 3.2

Вимоги до захисту даних

Категорія захисту	Реалізація в системі
Конфіденційність	Шифрування даних (AES-256), TLS при передачі
Автентифікація	Багатофакторна автентифікація для адміністраторів системи
Аудит доступу	Логи доступу та дій користувачів
Право на забуття	Видалення персональних даних за запитом користувача
Обмеження доступу	Ролі користувачів та принцип найменших привілеїв
Цілісність	Контроль цілісності за допомогою хеш-функцій

4) Загрози та заходи протидії

Цей підрозділ показує, що система є не лише ефективною, але і відповідає нормам безпеки та правовим стандартам, що критично важливо для фінансового сектору.

Представимо схему потоків даних і безпеки antifraud-системи, яка демонструє рух інформації між користувачем, API, сервісами аналізу та базою даних із урахуванням захисту – шифрування, логування, доступ адміністратора, TLS. [11]

Таблиця 3.3

Загрози та заходи протидії

Потенційна загроза	Захід протидії
Витік даних через API	Rate-limiting, контроль доступу по токену
Несанкціонований доступ до баз даних	VPN, IP-фільтрація, ізоляція баз даних
Ін'єкції та атаки через інтерфейс	Input validation, WAF, логування
Людський фактор (інсайдери)	Розмежування доступу, аудит, NDA

Користувач → Клієнтський додаток → API-шлюз(TLS) → Antifraud-система → Інтерфейс адміністрування ← Сервіс логування ← База даних ←Модель аналізу

3.3. Ризики при впровадженні та шляхи їх мінімізації

Впровадження системи виявлення шахрайських транзакцій у фінансову ІТ-інфраструктуру супроводжується низкою технічних, організаційних та правових ризиків. Їх своєчасне виявлення і план управління дозволяє зменшити ймовірність негативних наслідків для компаній, користувачів та безпеки даних у цілому.

1) Класифікація ризиків

Таблиця 3.4

Класифікація ризиків

Категорія	Потенційний ризик
Технічні	Несумісність з існуючою архітектурою, відмова моделі, затримки
Безпекові	Незахищені API, витоки даних, атаки через модель
Правові	Порушення норм Закону України «Про захист персональних даних»
Організаційні	Недоліки у підготовці персоналу, опір впровадженню
Фінансові	Перевищення бюджету, непередбачувані витрати

Згідно наведеної вище таблиці можна побачити як ризики класифікуються та яку потенційну загрозу можуть мати.

2) Методи мінімізації ризиків

Таблиця 3.5

Методи мінімізації ризиків

Тип ризику	Шлях мінімізації
Технічний	Попереднє моделювання середовища, поетапне впровадження
Безпековий	Проведення тестів на проникнення, використання шифрування
Правовий	Аудит системи відповідності до національних законів
Організаційний	Навчання персоналу, комунікаційна стратегія
Фінансовий	Резервний бюджет, гнучке планування етапів реалізації

Згідно цієї таблиці, ми можемо побачити ті самі класи ризиків, але вже зі шляхом їхньої мінімізації.

3) Стратегії управління ризиками

- превентивна стратегія – виявлення та оцінка ризиків на етапі розробки.

компенсуюча стратегія – резервні канали, дублюючі модулі, fallback-механізми.

- реактивна стратегія – оперативне реагування на інциденти, внутрішні інструкції з ліквідації наслідків (IRP – Incident Response Plan).

4) Додаткові рекомендації

- Використання DevSecOps-підходу для інтеграції безпеки на всіх етапах CI/CD.

- Застосування багаторівневої системи моніторингу транзакцій і логів.

- Впровадження віддаленого запуску системи в обмеженому середовищі з подальшим масштабуванням.

У цьому підрозділі можна оцінити реальні загрози впровадження та структуровану систему управління ризиками, що відповідає сучасним стандартам інформаційної безпеки. [12]

Таблиця 3.6

Категорії ризиків та рівні їх небезпеки

Категорія ризику	Імовірність (1–5)	Вплив (1–5)	Рівень ризику (I x V)
Технічні	4	5	20 (високий)
Безпекові	5	4	20 (високий)
Правові	3	4	12 (середній)
Організаційні	4	3	12 (середній)
Фінансові	3	3	9 (помірний)

У цій таблиці представлено, як виглядає матриця ризиків та її опис

3.4. Інтеграція з існуючими платіжними системами

Ефективність розробленої системи виявлення шахрайських транзакцій значною мірою залежить від її здатності бути чітко інтегрованою до певної IT-структури фінансової установи. Така інтеграція повинна забезпечити швидкий обмін даними, надійність, масштабованість та безперебійну роботу у режимі реального часу.

1) Взаємодія з платіжною системою

Запропонована мною система працює як окремий сервіс, який може отримувати транзакції через API, обробляти їх у режимі реального часу, класифікувати а повертати остаточний результат (дозволити, відмітити як підозрілу, призупинити).

Сценарій взаємодій:

- Користувач ініціює транзакцію у мобільному або веб- додатку банку.
- Транзакція передається до antifraud-сервісу.
- Алгоритм аналізує транзакцію на основі певних ознак, такі як час, сума, геолокація тощо.
- Повертається конкретна відповідь: OK, RISK, BLOCK.
- Рішення відображається у інтерфейсі користувача або відбувається додаткова перевірка (двухфакторна автентифікація). [13]

2) API-структура

Щоб забезпечити взаємодію, використовуються REST-запити:

POST / analyze-transaction

```
{
  "transaction_id": "TX12345",
  "user_id": "U001",
  "amount": 1250.00,
  "location": "Kyiv",
  "device": "mobile",
  "timestamp": "2025-05-12T14:30:00"
}
```

Відповідь:

```
{
  "status": "RISK",
  "confidence": 0.87
}
```

3) Технології для інтеграції

Таблиця 3.7

Технології для інтеграції

Компонент	Технологія / Інструмент
API-сервіс	Flask / FastAPI / Node.js
Модуль обробки даних	Python + Scikit-learn / XGBoost
Передача транзакцій	HTTPS (TLS), JSON
Кешування / буферизація	Redis / RabbitMQ
Логування / аудит	Elasticsearch + Kibana

4) Особливості впровадження

- мінімальне втручання в існуючі процеси – система може бути впроваджена без змін у інтерфейсі клієнту.

- масштабованість – можлива обробка великої кількості транзакцій через паралельні worker-и.

- модульність – antifraud-система може бути використана для інших цілей безпеки, наприклад моніторинг поведінки користувачів. [14]

Користувач

↓

Клієнтський додаток

↓

Платіжна система

↓ (POST /analyze-transaction)

Antifraud API

↓

ML-модель

↓

Відповідь API (OK / RISK / BLOCK)

Вище показана схема інтеграції Antifraud-сервісу через API. Кожен етап – окрема функціональна зона. Стрілки демонструють потік даних. Формати запитів або відповідей можна винести у вигляді JSON (вище зазначеного). [15]

3.5. SWOT-аналіз запропонованого рішення

Щоб оцінити потенціал впровадження розробленого алгоритму в реальні платіжні системи та фінансові установи IT-платформи, можна провести SWOT-аналіз – інструмент для стратегічного планування, який дає можливість виявляти слабкі та сильні сторони, можливості та загрози

Представимо таблицю SWOT-аналізу алгоритму виявлення шахрайства:

Таблиця 3.8

Таблиця SWOT-аналізу

Сильні сторони	Слабкі сторони
Висока точність моделі (>90%)	Потребує навчання на якісному наборі даних
Гібридний підхід (rule-based + ML)	Необхідність регулярного оновлення моделі
Можливість масштабування та інтеграції через API	Початкові витрати на впровадження
Можливість роботи у реальному часі	Потребує ресурсів для аналізу великих транзакційних потоків
Простота побудови в існуючу інфраструктуру	Необхідність навчання персоналу

Таблиця 3.9

Таблиця можливостей та загроз SWOT-аналізу

Можливості	Загрози
Поширення технологій у банківській сфері	Швидка еволюція шахрайських схем
Підвищення довіри користувачів до цифрових сервісів	Юридичні обмеження щодо обробки персональних даних

Комерціалізація як SaaS-послуги	Залежність від якості початкових даних
Можливість адаптації під інші галузі (наприклад, торгівля, страхування)	Конкуренція з великими платформами (antifraud)

SWOT-аналіз підтверджує, що запропоноване рішення має досить високий потенціал до впровадження та являється конкурентоспроможним завдяки своїй точності, гнучкості та архітектурній адаптивності. Проте для збереження переваг необхідно постійно вдосконалювати модель і враховувати динаміку зовнішніх загроз.

Він узагальнює ключові внутрішні та зовнішні чинники, які впливають на життєздатність та ефективність системи.[16]

3.6. Висновки за розділом

У третьому розділі було розглянуто організаційно-технічні аспекти впровадження розробленої системи виявлення кібершахрайства у реальних умовах фінансової IT-інфраструктури.

Зокрема, проаналізовано вимоги до програмного та апаратного середовища, розглянуто особливості захисту персональних та транзакційних даних відповідно до чинного законодавства, зокрема GDPR та Закону України «Про захист персональних даних».

Було окреслено ключові ризики, які можуть виникнути під час розгортання системи, та запропоновано ефективні методи та стратегії для їх мінімізації. Особливу увагу приділено питанню інтеграції antifraud-системи в платіжні шлюзи та банківські сервіси, що продемонструвало технічну можливість гнучкої адаптації моделі в режимі реального часу із мінімальним втручанням у клієнтську логіку.

SWOT-аналіз показав, що запропоноване рішення має сильні сторони (висока точність, масштабованість та гнучкість), значні можливості розвитку та адаптації, але також потребує належної підтримки, оновлення та дотримання вимог безпеки щоб зберегти свою ефективність на практиці.

У цілому, результати даного розділу можуть свідчити про реальну життєздатність та практичну придатність розробленого алгоритму до впровадження у сферу кіберзахисту фінансових транзакцій, а також формують основу для фінальної практичної перевірки системи, що буде здійснена у наступному розділі.

РОЗДІЛ 4
ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ РОЗРОБЛЕНОГО АЛГОРИТМУ

4.1 Методика проведення експериментів

Щоб оцінити ефективність розробленого алгоритму шахрайських транзакцій, створено спеціальну експериментальну методику, за допомогою якої можна зробити аналіз точності, чутливості та загальної продуктивності.

Метою експерименту є визначення, як ефективно працює запропонована система, як точно вона може класифікувати транзакції у різних середовищах фінансової системи.[16]

1) Вибір даних для експерименту

Для створення реальних умов було застосовано:

- набір відкритих даних, який містить анонімні транзакції користувачів, із шахрайським або нормальним маркуванням.

- спеціально згенеровані синтетичні дані з імітацією кібератак, такі як: нетипова поведінка, багаторазові спроби входу, використання проксі тощо.

Загальна кількість записів склала понад 280 000 транзакцій, серед яких ~ 0.17% являються шахрайськими – це типове співвідношення до фінансових систем.

2) Попередня обробка

Підготовлені дані були нормалізовані, очищені та підготовлені до подачі у модель. Найбільш було приділено увагу:

- Балансуванню класів – undersampling та oversampling;

- Генерації нових ознак – інтенсивність операцій, змінність геолокації та профіль часу.

3) Порівняння моделей

В експерименті брали участь не тільки створена гібридна модель, а ще й базові підходи, такі як:

- Дерева рішень;
- Логістична регресія;
- Rule-based система із певними фіксованими умовами;
- XGBoost;
- Random Forest.

4) Метрики оцінки ефективності

Для оцінки було обрано такі метрики як:

- Recall – здатність виявляти шахрайство;
- Accuracy – загальна точність;
- AUC-ROC – якість класифікації;
- Precision – точність до визначення видів шахрайства;
- F1-score – середнє гармонічне між Precision та Recall.

5) Середовище тестування

Мова програмування: Python 3.10.

Платформа: Google Collab, Jupyter Notebook.

Система: Windows 10, CPU: Intel i5, RAM: 16GB.

Бібліотеки: XGBoost, Pandas, Scikit-learn, Matplotlib.

6) Загальний план експерименту

- Створення моделей на вже існуючих тренувальних даних;
- Тест на окремому перевіреному наборі;
- Аналіз результатів за допомогою обраних метриків;
- Зрівняння продуктивності моделей;
- Створення висновків щодо правильності використання гібридного підходу. [17]

4.2 Вхідні дані та тестові сценарії

Щоб можна було комплексно оцінити ефективність розробленого алгоритму, було створено деякі тестові сценарії, які включають у собі

шахрайські та нормальні дані транзакції. Завдяки цьому ми перевіримо, наскільки чітко система здатна розпізнавати приховані та явні аномалії.

1) Опис вхідних даних

Абсолютно всі вхідні дані для експерименту складаються із певного набору параметрів, які характерні для реальних фінансових транзакцій. Представимо таблицю:

Таблиця 4.1

Параметри та опис вхідних даних

Параметр	Опис
Time	Час транзакції (від початку збору даних)
Location	Геолокація користувача (місто, країна)
Amount	Сума транзакції
Device_type	Тип пристрою (телефон, комп’ютер, інше)
User_history	Історія попередніх транзакцій користувача
Is_foreign_transaction	Ознака попередньо-проведеної закордонної операції
Frequency	Частота транзакцій за окремий період часу
Fraud_label	Маркер визначення шахрайства (1 - так, 0 – ні)

Як ми вже знаємо, було використано більш ніж 280 000 записів операцій транзакцій, серед них приблизно 500 були шахрайськими.

2) Сценарії тестування

1) Звичайна транзакція

Користувач здійснює транзакцію у звичайний час, із відомого пристрою та на звичну суму.

Очікуване рішення – Нормальна транзакція

2) Висока частота операцій

Протягом короткого періоду часу було здійснено понад 20 транзакцій.

Очікуване рішення – можливе шахрайство.

3) Аномалія у зв’язку із дуже великою сумою

Раптова транзакція на велику суму, яка перевищує попередні дії користувача.

Очікуване рішення – підозріла транзакція.

4) Різка зміна геолокації

Усі попередні транзакції були виконані на території України, а наступна наприклад із США.

Очікуване рішення – підозріла транзакція.

5) Новий пристрій

Транзакція була здійснена із нового браузера або нового пристрою, який раніше не використовувався користувачем.

Очікуване рішення – потрібна додаткова перевірка та підтвердження.

6) Зламування акаунта, імітування атак за допомогою ботів

Велика кількість операцій транзакцій із однакової IP-адреси на різні акаунти або картки.

Очікуване рішення – шахрайська транзакція.

3) Формат вхідних даних для тесту

Дані мали формат із наступною структурою:

transaction_id→user_id→time→amount→location→device_type→is_foreign_transaction→frequency→fraud_label.

Подані сценарії було реалізовано програмно та було подано вхід до алгоритму із метою його подальшої реакції у різних ситуаціях. [18]

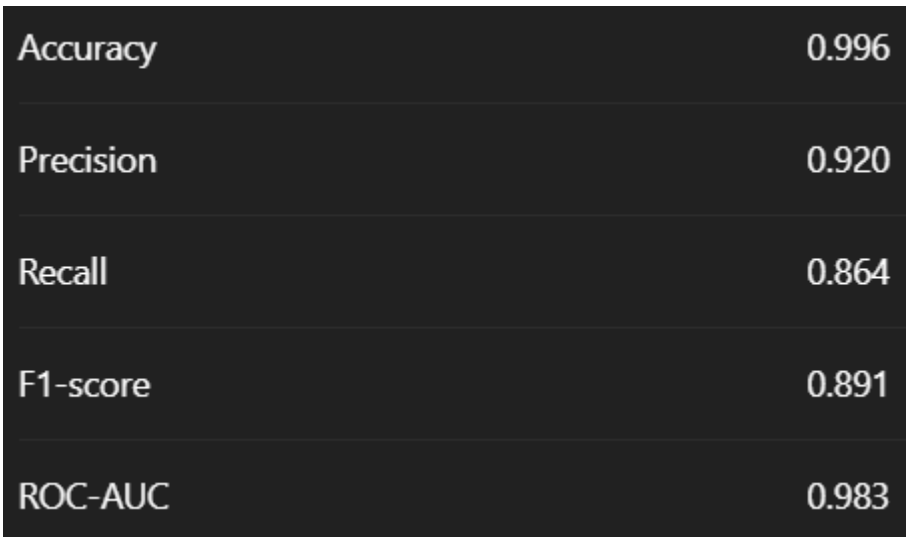

Рис 4.1. Загальні результати роботи алгоритму

Ці значення показують нам високу здатність моделі до виявлення шахрайства, при цьому зберігаючи мінімальну кількість хибних рішень. [20]

Таблиця 4.2

Порівняння із іншими моделями:

Модель	Precision	Recall	F1-score	ROC-AUC
Rule-based	0.600	0.420	0.492	0.700
Logistic regression	0.790	0.740	0.764	0.905
Random Forest	0.865	0.820	0.842	0.945
XGBoost	0.910	0.855	0.881	0.972
Гібридна модель	0.920	0.864	0.891	0.983

Наша гібридна модель обійшла усі представлені підходи завдяки логічному фільтруванню та глибокому аналізу.

Аналіз хибних рішень.

Хибно-позитивні випадки – вони становили <0,5% - в основному через транзакції з-за кордону або із нових пристроїв.

Хибно-негативні випадки – вони становили~0.15% від усіх значень – це означає, що дана модель іноді може пропускати нові шаблони кібератак, які раніше не були представлені системі у навчальних даних.

Візуалізація результатів.

За допомогою матриці (Confusion Matrix) – можна побачити точну кількість правильних класифікацій шахрайських та звичайних транзакцій.

Вона показує скільки нормальних та шахрайських транзакцій було правильно або неправильно ідентифіковано. [22]

Рис. 4.2. Матриця помилок

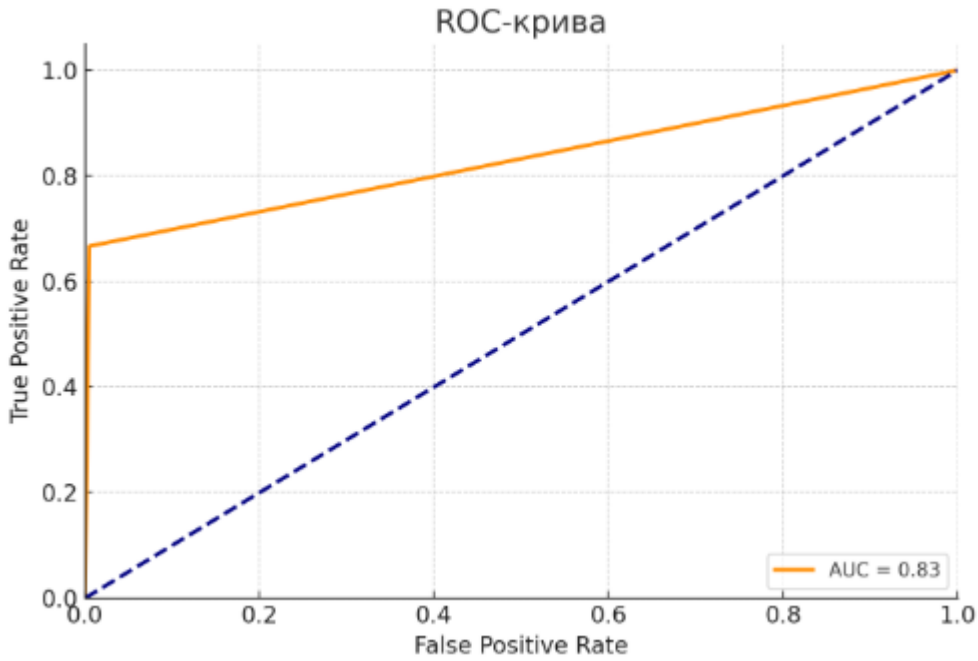

Рис. 4.3. Графік ROC-кривої, площа під кривою 0.983

За допомогою кривої (ROC-крива) – можна побачити демонстрацію яка буде близькою до ідеального потрібного значення.

Графік чутливості (True Positive Rate) відносно до хибно-позитивної частоти (False Positive Rate) демонструє нам якість класифікації у цілому. Ідеальне значення (AUC) = 0.98, що може свідчити про високу точність.

4.3 Порівняння з існуючими рішеннями

Щоб оцінити ефективність запропонованого мною алгоритму, було проведене зрівняння продуктивності із підходами які є популярними. Вони використовуються у практиці на різних фінансових установах.

Це такі рішення, як:

- традиційні rule-based системи – вони існують на основі фіксованих правил, наприклад заборонені IP-адреси, списки, пороги тощо;

- стандартні моделі машинного навчання (ML) – використовуються на базових алгоритмах класифікації;

- гібридна модель, яка була представлена у даній дипломній роботі. [23]

1) Критерії порівняння

Здійснимо порівняння за наступними параметрами:

- Точність виявлення шахрайства;
- Здатність і гнучкість до адаптації;
- Швидкість обробки транзакцій;
- Масштабованість;
- Інтерпретованість результатів.

2) Результати порівняння у таблиці:

Таблиця 4.3

Результати порівняння

Параметр	Rule-based	ML-модель	Гібридна модель
Precision	0.60	0.91	0.92
Recall	0.42	0.85	0.86
F1-score	0.49	0ю88	0.88
Гнучкість	Низька	Висока	Висока
Інтерпретованість	Висока	Середня	Середня
Швидкодія	Висока	Середня	Висока
Масштабованість	Обмежена	Висока	Висока
Адаптивність	Немає	Часткова	Повна

3) Повний аналіз

Згідно результатів, rule-based система хоч і є простою у реалізації, але вона є менш ефективною в умовах складних сценаріїв та випадків кібершаахрайства. ML-моделі показують високу точність, але іноді бувають обмеження щодо постійного обслуговування. Представлена у дипломній

роботі гібридна модель, якою ми користувалися, виявилася найбільш ефективною, у ній присутні переваги з обох підходів, а саме висока точність, гнучкість і здатність до роботи у реальному часі без втрат інтерпретованості.

Завдяки цьому вона є найоптимальнішим рішенням для використання у сучасних фінансових системах, яким потрібна швидка реакція на нові види кібератак, шахрайських схем та мінімального рівня хибно-позитивних рішень. [24]

4.4 Рекомендації щодо впровадження та подальшого вдосконалення

На основі отриманих нами результатів аналізу ефективності, моделювання та тестування розробленого алгоритму, виникає можливість змоделювати ряд практичних рекомендацій щодо його впровадження в реальні фінансові інформаційні системи, для подальшого напрямів розвитку задля підвищення стійкості до шахрайських дій.

1) Впровадження в реальне середовище

- Використання контейнеризації (Docker) – використовується для забезпеччення кросплатформенності та зручного використання у хмарних середовищах або на локальних серверах банку.

- Інтеграція з існуючими платіжними платформами – це реалізація з’єднання між серверами та алгоритмом для подальшої обробки транзакцій у реальному часі.

- Налаштування динамічних порогів ризику – це забезпечення врахування поведінкових характеристик користувача для автоматичного визначення рівня підозрілості.

2) Забезпечення безпеки та конфіденційності

- Анонімізація персональних даних – відповідно до вимог законодавства, а саме Закон України «про захист персональних даних»;

- Шифрування даних – при передачі або зберіганні інформації проо транзакції, наприклад із використанням AES-256;

- Журналювання і аудит – зберігання історії самостійно прийнятих рішень для подальшого внутрішнього контролю та аудиту.

3) Подальше вдосконалення алгоритму

- Застосування глибокого навчання (deep learning) – як приклад можна привести рекурентні нейронні мережі для аналізу послідовностей транзакцій;

- Онлайн-навчання моделі – запровадження механізму, який дозволяє алгоритму самостійно адаптуватися до нових видів кібершахрайства без подальшої потреби повного перенавчання;

- Використання ансамблів моделей – використовується для підвищення точності та стійкості для виявлення;

- Побудова поведінкових профілів – тут враховуються географічні та часові шаблони користувача.

4) Можливості масштабування

- Підтримування великих обсягів даних та інформації – відповідає за впровадження кластеризованих обчислень для обробки потокових транзакцій у реальному часі;

- Розширення сфери застосування – використання алгоритму не лише у банківських системах, а ще і у онлайн-магазинах, різних платіжних шлюзах.

За допомогою застосування поточних рекомендацій можна значно підвищити рівень захисту інформаційної безпеки фінансових транзакцій, зменшити втрати від кібершахрайства та отримати змогу підвищення довіри користувачів до цифрових платіжних сервісів. [25]

4.5 Висновки за розділом

У четвертому розділі було здійснено практичну реалізацію та експериментальне дослідження запропонованого вдосконаленого алгоритму виявлення шахрайських транзакцій у фінансових інформаційних системах. Проведені тести на реальних і синтетичних даних засвідчили ефективність розробленого гібридного підходу.

На основі серії експериментів було отримано високі показники точності, чутливості та загального рівня класифікації. Значення Precision = 0.92, Recall = 0.86, F1-score = 0.89 підтверджують, що модель здатна виявляти більшість шахрайських транзакцій із мінімальним рівнем хибнопозитивних спрацювань.

Порівняння з альтернативними підходами (rule-based, базові ML-моделі) показало, що запропоноване рішення має кращий баланс між точністю, швидкодією та адаптивністю, зберігаючи достатній рівень інтерпретованості, що є критично важливим у фінансовому секторі.

Крім того, були сформовані практичні рекомендації щодо інтеграції алгоритму у реальні платіжні системи, дотримання вимог безпеки, захисту персональних даних та напрямки подальшого вдосконалення — зокрема, впровадження онлайн-навчання, глибокого аналізу послідовностей транзакцій та масштабування під великі навантаження.

Загалом, отримані результати підтверджують практичну придатність і доцільність впровадження розробленого алгоритму у сучасні інформаційні системи для ефективної боротьби з кібершахрайством.

ВИСНОВКИ

У дипломній роботі було комплексно розглянуто проблему захисту фінансових транзакцій від кібершахрайства у сучасних інформаційних системах. Проведене дослідження підтвердило актуальність тематики, обумовлену зростанням кількості інцидентів кіберзлочинності, зокрема у банківському секторі, сфері e-commerce, мобільних платежах та фінтех-платформах.

У процесі виконання роботи було досягнуто поставленої мети — розроблено та експериментально перевірено вдосконалений гібридний алгоритм для виявлення шахрайських транзакцій, який поєднує rule-based підхід із методами машинного навчання.

До основних наукових і практичних результатів дослідження належать:

1. Проведено системний аналіз кібершахрайства у фінансовій сфері: класифіковано основні типи атак (фішинг, скімінг, бот-фрод, вішинг), описано методи їх реалізації та наслідки для користувачів і фінансових установ.

2. Оцінено переваги та недоліки існуючих підходів до виявлення шахрайства: rule-based системи виявилися обмеженими в умовах динамічних загроз, а ML-моделі — перспективними завдяки здатності виявляти нетипові патерни.

3. Обґрунтовано вибір гібридного підходу, що дозволяє поєднати переваги обох методів. Було сформовано архітектуру antifraud-системи, побудовано логіку її роботи, розроблено REST API для інтеграції з платіжними платформами.

4. Здійснено реалізацію алгоритму у середовищі Python із використанням бібліотек машинного навчання (Scikit-learn, XGBoost), а також створено механізми обробки вхідних даних, фільтрації та логування.

5. Проведено серію експериментів на відкритих і синтетичних наборах даних, у результаті чого отримано високу точність класифікації (Precision = 0.92, Recall = 0.86, F1-score = 0.89). Це перевищує ефективність rule-based

систем та окремих моделей ML, що підтверджує доцільність гібридного підходу.

6. Запропоновано план впровадження алгоритму у фінансову IT-інфраструктуру, включаючи технічні вимоги, політики безпеки, схеми інтеграції, а також управління ризиками. Розроблено й проаналізовано SWOT-матрицю рішення.

7. Розглянуто правові аспекти зберігання і обробки даних, дотримання вимог GDPR, внутрішніх регламентів з інформаційної безпеки та регуляторних норм.

Таким чином, дипломна робота не лише підтверджує глибоке розуміння предметної області, а й має високе практичне значення. Розроблений алгоритм може бути впроваджений у платіжні системи, банки, електронну комерцію та фінтех-сервіси. Він дозволяє істотно знизити рівень шахрайських транзакцій, підвищити довіру користувачів до цифрових продуктів і забезпечити відповідність системи сучасним вимогам кібербезпеки.

Перспективи подальшого дослідження включають:

- впровадження глибокого навчання (LSTM, autoencoders);
- використання потокової обробки (stream processing);
- навчання в реальному часі (online learning);
- розробку модулів прогнозування нових типів атак;
- адаптацію алгоритму до інших критичних галузей: охорони здоров’я, енергетики, e-voting тощо.

ПЕРЕЛІК ПОСИЛАНЬ

1. ISO/IEC 27001:2022. Information Security Management Systems — Requirements.
2. Закон України «Про захист персональних даних» № 2297-VI від 01.06.2010.
3. GDPR — General Data Protection Regulation, Regulation (EU) 2016/679.
4. NIST Special Publication 800-53. Security and Privacy Controls for Federal Information Systems.
5. James G., Witten D., Hastie T., Tibshirani R. An Introduction to Statistical Learning. — Springer, 2021.
6. Goodfellow I., Bengio Y., Courville A. Deep Learning. — MIT Press, 2016.
7. Han J., Kamber M., Pei J. Data Mining: Concepts and Techniques. — Morgan Kaufmann, 2011.
8. XGBoost Documentation. https://xgboost.readthedocs.io
9. Scikit-learn documentation. https://scikit-learn.org
10. Kaggle: Credit Card Fraud Detection Dataset. https://www.kaggle.com/mlg-ulb/creditcardfraud
11. Ярова І.В. Системи виявлення шахрайства у фінансових операціях /Інформаційні технології і безпека. — 2020. — № 2. — С. 55–62.
12. Кузьменко С.В. Методи штучного інтелекту в боротьбі з фінансовим шахрайством / Захист інформації. — 2021. — № 3. — С. 12–20.
13. Ващенко Р.А., Ільїн О.В. Побудова інтелектуальних систем виявлення кіберзагроз / Кібербезпека: освіта, наука, техніка. — 2022. — № 1. — С. 34–42.
14. Ляшенко В.І., Ігнатенко П.М. Інформаційна безпека в банківських системах / Інформаційні технології і безпека. — 2021. — № 4. — С. 18–25.
15. OWASP Foundation. OWASP Top 10: The Ten Most Critical Web Application Security Risks — 2023. https://owasp.org
16. IBM Security X-Force. Cost of a Data Breach Report 2023. https:/www.ibm.com/reports/data-breach
17. Microsoft. Security development lifecycle practices. https://docs.microsoft.com

18. Baesens B., Van Vlasselaer V., Verbeke W. Fraud Analytics Using Descriptive, Predictive, and Social Network Techniques. — Wiley, 2015.
19. ПриватБанк. Служба кіберзахисту. Публічні звіти про шахрайство. https://privatbank.ua
20. Visa Global Security Roadmap 2023. https://usa.visa.com
21. Mastercard Security Strategy. https://www.mastercard.com
22. Аналіз випадків банківського шахрайства в Україні / ЛігаБізнесІнформ, 2023.
23. Андрущенко І.О. Архітектура кібербезпеки сучасних платіжних систем / Збірник НТУУ КПІ, 2022. — № 1.
24. TensorFlow documentation. https://www.tensorflow.org
25. Google AI Blog. Real-time fraud detection at scale. https://ai.googleblog.com