ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
(повне найменування вищого навчального закладу)
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ
(повне найменування інституту, назва факультету (відділення))
КАФЕДРА ПРОГРАМНИХ ЗАСОБІВ ТА ТЕХНОЛОГІЙ
(повна назва кафедри (предметної, циклової комісії))

Пояснювальна записка

до кваліфікаційної роботи
бакалавра
(освітній рівень)

на тему: «Розробка програмних засобів виявлення шахрайських схем у фінансових операціях»

Виконав: здобувач освіти 4 року навчання,
групи ЗПРс спеціальності
121 - «Інженерія програмного забезпечення»
(шифр і назва спеціальності)

Кожухар Денис Сергійович
(прізвище та ініціали)
Керівник к.т.н., доц. Зуб М.П.
(прізвище та ініціали)
Рецензент к.т.н. доцент Вишемирська С.В.
(прізвище та ініціали)

Хмельницький - 2025

Херсонський національний технічний університет
(повне найменування вищого навчального закладу)

Факультет, відділення Інформаційних технологій та дизайну
Кафедра Програмних засобів і технологій
Освітній рівень бакалавр
Спеціальність 121 – Інженерія програмного забезпечення
(шифр і назва)

ЗАТВЕРДЖУЮ

Завідувач кафедри
Програмних засобів та технологій
к.т.н. доц. О.Є. Огнєва
"___" _____ 2025 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ

Кожухарю Денису Сергійовичу
(прізвище, ім'я, по батькові)

Тема роботи «Розробка програмних засобів виявлення шахрайських схем у фінансових операціях»
керівник роботи к.т.н. доцент Зуб М.П.,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджена наказом вищого навчального закладу від 20.01.2025 р. №100-С
2. Строк подання здобувачем роботи 15.06.2025 р.
3. Вихідні дані до роботи дослідити методи нейронних мереж для виявлення шахрайства, середовище розробки VS Code 2023, мова програмування Python, бібліотеки: Numpy, Sklearn, PyTorch, Adam, HOA, DGL
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
1) мета роботи, 2) аналіз предметної галузі і постановка задачі,
3) огляд та аналіз літературних джерел,
4) дослідження теоретичне,
5) дослідження практичне;
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
1. Методи виявлення фінансового шахрайства.
2. Аналіз алгоритмів машинного навчання.
3. Представлення архітектури ML-моделі для виявлення шахрайства.
4. Демонстрація роботи процесу з використанням ML-моделі.
5. Результати оцінки ML-моделі: метрики, графіки, порівняння.
6. Візуалізація інтеграції ML-моделі у бізнес-процеси

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів виконання роботи	Термін виконання етапів роботи	Примітки
1.	Отримання завдання	20.01.2025	Виконано
2.	Підбір літератури	21.01.2025-31.01.2025	Виконано
3.	Аналіз предметної області	01.02.2025-15.02.2025	Виконано
4.	Розробка та обґрунтування завдання	16.02.2025-25.02.2025	Виконано
5.	Розробка концептуальної моделі	26.02.2025-12.03.2025	Виконано
6.	Розробка алгоритму	13.03.2025-25.03.2025	Виконано
7.	Проектування програмної системи	26.03.2025-11.04.2025	Виконано
8.	Розробка інтерфейсу програмної системи	12.04.2025-18.03.2025	Виконано
9.	Тестування програмної системи	19.04.2025-25.04.2025	Виконано
10.	Оформлення пояснювальної записки	26.04.2025-09.05.2025	Виконано
11.	Захист кваліфікаційної роботи	15.06.2025	Виконано

Здобувач вищої освіти _____ Кожухар Д.С.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Зуб М.П.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Кваліфікаційна робота бакалавра: 94 сторінки, 29 рисунків, 9 таблиць, 1 додаток, 20 джерел.

Мета роботи – аналіз різних типів нейронних мереж, їх архітектур та методів навчання з метою визначення оптимального підходу до виявлення шахрайства.

Об'єкт дослідження – використання нейронних мереж для виявлення шахрайства в банківській сфері.

Предмет дослідження – математичні моделі та програмне забезпечення оптимізації продуктового кошику.

Методи дослідження базуються на нейронних мережах, а також Python, бібліотеки: Numpy, Sklearn, PyTorch.

Новизна роботи полягає в тому, що розроблено модель для виявлення шахрайських транзакцій, яка здатна правильно ідентифікувати 86% шахрайських операцій (показник Recall) та 90% звичайних (нормальних) транзакцій (показник Specificity), що означає, що більшість шахрайських дій не залишаються непоміченими, а також мінімізується кількість помилок, коли нормальні операції позначаються як підозрілі.

Практична цінність результатів роботи полягає в тому, що їх успішно впроваджено в роботу системи, де процес автоматично обробляє ключові параметри транзакцій, оцінює ризики шахрайства, блокує підозрілі рахунки або передає інформацію до системи моніторингу, що значно підвищує швидкість і якість прийняття рішень..

Ключові слова: банківська галузь, Corezoid, ефективність, нейронні мережі, ризики шахрайства, фінансова безпека.

АНОТАЦІЯ

Кваліфікаційна робота бакалавра складається зі вступу, чотирьох розділів, висновку, списку використаних джерел та додатку.

Роботу присвячено огляду та аналізу методів і технологій, що використовуються для виявлення аномалій у фінансових операціях з метою запобігання шахрайству та підтримки фінансової безпеки клієнтів і банківських установ. Основними завданнями є дослідження та порівняння різних підходів, визначення їх ефективності та розробка рекомендацій щодо використання нейронних мереж у практичному застосуванні для виявлення шахрайства.

У роботі представлено детальний аналіз та дослідження методів виявлення шахрайства, в тому числі з використанням нейронних мереж, у банківській сфері. Дослідження охоплює розвиток цифрових фінансових послуг, аналіз викликів та ризиків шахрайства з банківськими картками, а також розглядає технологічні вразливості та кіберзагрози, які можуть загрожувати фінансовій безпеці.

Дослідження та аналіз показують, що використання нейронних мереж є ефективним засобом виявлення шахрайства в банківській сфері. Глибоке навчання дозволяє моделям адаптуватися до різних шаблонів і виявляти аномалії, що робить їх важливим інструментом у сучасному фінансовому середовищі.

Виконання роботи базується на таких технологіях, як Python, бібліотеки: Numpy, Sklearn, PyTorch.

ABSTRACT

The bachelor's thesis consists of an introduction, four chapters, a conclusion, a list of sources and an appendix.

The work is devoted to a review and analysis of methods and technologies used to detect anomalies in financial transactions in order to prevent fraud and maintain the financial security of customers and banking institutions. The main tasks are to study and compare different approaches, determine their effectiveness and develop recommendations for the use of neural networks in practical applications for fraud detection.

The work presents a detailed analysis and research of fraud detection methods, including those using neural networks, in the banking sector. The research covers the development of digital financial services, analysis of the challenges and risks of bank card fraud and also considers technological vulnerabilities and cyber threats that may threaten financial security.

Research and analysis show that the use of neural networks is an effective means of detecting fraud in the banking sector. Deep learning allows models to adapt to various patterns and detect anomalies, which makes them an important tool in the modern financial environment.

The work is based on technologies such as Python, libraries: Numpy, Sklearn, PyTorch.

ЗМІСТ

ВСТУП

Виявлення шахрайства – це набір процесів та аналізів, які дозволяють компаніям виявляти та запобігати несанкціонованій діяльності. Це стало одним із головних викликів для більшості організацій, особливо в банківській, фінансовій, роздрібній торгівлі та електронній комерції.

Шахрайська діяльність включає відмивання грошей, кібератаки, шахрайські банківські претензії, підроблені банківські чеки, крадіжка особистих даних і багато подібних незаконних дій.

У результаті організації впроваджують сучасні технології виявлення та запобігання шахрайству та стратегії управління ризиками для боротьби зі зростаючими шахрайськими транзакціями на різних платформах.

Ці методи застосовують адаптивну та прогнозну аналітику (тобто машинне навчання) для створення оцінки ризику шахрайства разом із моніторингом шахрайських подій у реальному часі, що дозволяє постійно контролювати транзакції та злочини в режимі реального часу.

Це також допомагає розшифрувати нові та складні профілактичні заходи за допомогою автоматизації [1].

Будь-який вид шахрайства негативно впливає на фінансові результати та ринкову репутацію організації, а також відлякує як майбутніх потенційних, так і нинішніх клієнтів. Враховуючи масштаб і охоплення цих вразливих організацій, для них стало критично важливим запобігати шахрайству і навіть передбачати підозрілі дії в режимі реального часу [2].

Є кілька ключових речей, які слід мати на увазі щодо можливостей виявлення. По-перше, важливо мати систему, яка може ідентифікувати потенційні загрози. Ця система повинна мати можливість відстежувати дані та активність на всіх каналах, включаючи онлайн, особисто та по телефону [3].

За останні кілька років спостерігається тенденція до зростання попиту на застосування моделей виявлення аномалій у різних галузях. Але найбільший

попит має банківська галузь. В наш час ця тенденція зумовлена зростанням кількості транзакцій та підвищенням попиту фінансових послуг через Інтернет.

У банківському секторі боротьба з картковим шахрайством має особливе значення, оскільки шахраї можуть використовувати різні хитрощі та технологічні інновації, щоб обійти традиційні методи безпеки банків. Шахрайство з банківськими картками може нанести велику шкоду для людей. Це може принести втрату зарплатні або велику суму яку людина відкладала на якусь цінну покупку.

Існує кілька способів запобігання шахрайству, наприклад використання аналітики для ідентифікації ризик факторів, налаштування систем, виявлення або навчання працівників пошуку ознак шахрайства. Вживаючи превентивних заходів, бізнес може захистити себе від фінансових втрат і шкоди своїй репутації.

Виявлення шахрайства має на меті виявити шахраїв і шахрайську діяльність, одночасно запобігаючи втраті грошей та майна. Існують різноманітні системи та інструменти виявлення шахрайства, які використовуються, щоб не відставати від цифрових загроз, що постійно розвиваються, особливо у фінансовій, медичній, державній, страховій та роздрібній галузях. Машинне навчання є життєво важливими компонентами виявлення шахрайства, які використовують методи аналізу даних для виявлення шахрайства [4].

Виявлення шахрайства є складною проблемою. Справа в тому, що шахрайські операції трапляються рідко; вони представляють дуже невелику частину діяльності всередині організації. Проблема полягає в тому, що невеликий відсоток активності може швидко перетворитися на великі втрати, без відповідних інструментів і систем. Оскільки традиційні схеми шахрайства не окупаються, шахраї навчилися змінювати свою тактику. Хороша новина полягає в тому, що завдяки прогресу в аналітиці шахрайства системи можуть вивчати, адаптувати та виявляти нові моделі запобігання шахрайству [5].

Об'єктом дослідження є використання нейронних мереж для виявлення шахрайства в банківській сфері.

Робота присвячена огляду та аналізу методів і технологій, що використовуються для виявлення аномалій у фінансових операціях з метою запобігання шахрайству та підтримки фінансової безпеки клієнтів і банківських установ. Основними завданнями є дослідження та порівняння різних підходів, визначення їх ефективності та розробка рекомендацій щодо використання нейронних мереж у практичному застосуванні для виявлення шахрайства.

Методи розробки базуються на таких технологіях, Python, бібліотеки: Numpy, Sklearn, PyTorch.