Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук
(повна назва)

Кафедра Інформаційних управляючих систем
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Дослідження моделей та методів виявлення аномалій у фінансових транзакціях інформаційної системи банківського обслуговування

(тема)

Виконав:
здобувач 2 року навчання,
групи ІУСТм-24-1
Данило НОВИЦЬКИЙ
(власне ім'я, ПРІЗВИЩЕ)

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

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Інформаційні управляючі системи та технології
(повна назва освітньої програми)

Керівник: доц. каф. ІУС Олена МІХНОВА
(посада, власне ім'я, ПРІЗВИЩЕ)

Допускається до захисту

Завідувач кафедри ІУС _____ Костянтин ПЕТРОВ
(підпис) (власне ім'я, ПРІЗВИЩЕ)

2025 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерних наук

Кафедра Інформаційних управляючих систем

Рівень вищої освіти другий (магістерський)

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

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Інформаційні управляючі системи та технології
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)

" 24 " грудня 2025 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Новицькому Данилові Олексійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження моделей та методів виявлення аномалій у фінансових транзакціях інформаційної системи банківського обслуговування

затверджена наказом по університету від " 24 " листопада 2025 р. № 1055Ст

2. Термін подання здобувачем роботи до екзаменаційної комісії " 18 " грудня 2025 р.

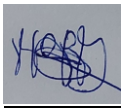
3. Вихідні дані до роботи матеріали звіту з передатестаційної практики, сучасні наукові дослідження та публікації з методів виявлення аномалій, статистичні характеристики фінансових транзакцій та поведінкових патернів клієнтів, набори транзакційних даних для моделювання та експериментальної перевірки, алгоритми машинного навчання та глибинного навчання.

4. Перелік питань, що потрібно опрацювати у роботі провести аналіз предметної області виявлення аномалій у фінансових транзакціях та визначити ключові проблеми; виконати огляд сучасних моделей і методів детектування аномалій; розробити концепцію синтезованого методу HASBT, що поєднує статистичні методи, моделі машинного навчання та глибинного моделювання; побудувати архітектуру програмної реалізації методу; реалізувати програмний прототип модулів; провести експериментальну перевірку ефективності моделей та оцінити роботу; порівняти ефективність запропонованої технології HASBT з існуючими підходами.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Аналіз предметної області та огляд сучасних методів виявлення аномалій у фінансових транзакціях	24.11.2025 – 25.11.2025	Виконано
2	Дослідження математичних основ статистичних моделей, алгоритмів ML та Autoencoder	26.11.2025 – 27.11.2025	Виконано
3	Побудова архітектури системи та IDEF0-діаграм	28.11.2025 – 02.12.2025	Виконано
4	Розроблення концепції синтезованого методу HASBT	03.12.2025 – 04.12.2025	Виконано
5	Підготовка даних до проведення експериментів	04.12.2025 – 05.12.2025	Виконано
6	Проведення експериментальних досліджень та аналіз результатів	06.12.2025 – 06.12.2025	Виконано
7	Порівняння ефективності синтезованого методу з існуючими підходами	06.12.2025 – 07.12.2025	Виконано
8	Оформлення пояснювальної записки	07.12.2025 – 07.12.2025	Виконано
9	Захист кваліфікаційної роботи	18.12.2025	Виконано

Дата видачі завдання __24___ ____листопада___2025 р.

Здобувач 
(підпис)

Керівник роботи _____ __доц. каф. ІУС Олена МІХНОВА_
(підпис) (посада, власне ім’я, ПРІЗВИЩЕ)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 78 с., 13 рис., 4 табл., 1 дод., 20 джерел.

АНОМАЛІЇ, АВТОЕНКОДЕР, АНСАМБЛЕВІ МЕТОДИ, МАШИННЕ НАВЧАННЯ, ФІНАНСОВІ ТРАНЗАКЦІЇ, ШАХРАЙСТВО, HASBT, ISOLATION FOREST, ONE-CLASS SVM.

Об’єктом дослідження кваліфікаційної роботи є процеси виявлення аномалій та шахрайських дій у фінансових транзакціях банківських інформаційних систем.

Предметом дослідження є моделі, методи та алгоритми автоматизованого аналізу транзакцій з метою виявлення нестандартної або потенційно шахрайської поведінки користувачів у реальному часі.

Метою роботи є підвищення точності та ефективності виявлення аномалій у фінансових транзакціях шляхом розроблення синтезованого методу, що поєднує статистичні методи, алгоритми машинного навчання та глибинні нейронні моделі.

Для досягнення поставленої мети було виконано такі основні завдання: проаналізовано сучасні підходи до виявлення аномалій у банківських транзакціях та визначено їх переваги й недоліки, досліджено математичні основи статистичних методів, моделей машинного навчання та автоенкодерів, розроблено синтезований підхід HASBT, що поєднує три рівні детектування, побудовано архітектуру програмної реалізації та створено модульний прототип системи, проведено експериментальну перевірку ефективності окремих моделей та ансамблю, виконано порівняння запропонованої технології з існуючими базовими методами виявлення аномалій.

Практичне значення роботи полягає у можливості використання отриманих результатів та розробленої технології як основи для побудови або вдосконалення прототипів систем моніторингу фінансових транзакцій.

ABSTRACT

Masters's thesis: 78 pages, 13 figures, 4 tables, 1 appendices, 20 sources.

ANOMALIES, AUTOENCODER, ENSEMBLE METHODS, MACHINE LEARNING, FINANCIAL TRANSACTIONS, FRAUD, HASBT, SOLATION FOREST, ONE-CLASS SVM.

The object of the qualification work is the processes of detecting anomalies and fraudulent actions in financial transactions of banking information systems.

The subject of the research is models, methods and algorithms of automated transaction analysis in order to detect non-standard or potentially fraudulent user behavior in real time.

The aim of the work is to increase the accuracy and efficiency of detecting anomalies in financial transactions by developing a synthesized information technology that combines statistical methods, machine learning algorithms and deep neural models.

To achieve the set goal, the following main tasks were performed: modern approaches to detecting anomalies in banking transactions were analyzed and their advantages and disadvantages were identified, the mathematical foundations of statistical methods, machine learning models and autoencoders were studied, a synthesized HASBT approach was developed that combines three levels of detection, the software implementation architecture was built and a modular prototype of the system was created, an experimental test of the effectiveness of individual models and the ensemble was conducted, and the proposed technology was compared with existing basic methods of detecting anomalies.

The practical significance of the work lies in the possibility of using the obtained results and the developed technology as a basis for building or improving prototypes of financial transaction monitoring systems.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

БІС – банківська інформаційна система

LOF – Local Outlier Factor

OCSVM – One-Class Support Vector Machine

OLAP – Online Analytical Processing

OLTP – Online Transaction Processing

SOA – Service-Oriented Architecture

ВСТУП

У сучасному банківському обслуговуванні фінансові операції здійснюються у великих обсягах та з високою швидкістю, що створює нові можливості та ризики. Одним з головних ризиків є виникнення аномальних або шахрайських транзакцій, які можуть призвести до значних фінансових втрат, порушенню довіри клієнтів та стабільності банківської системи.

Традиційні методи контролю – перевірка правил, фіксовані порогові значення або ручний аудит – виявляються неефективними через швидке зростання обсягу даних та складність методів шахрайства. Тому на перший план виходять методи засновані на інтелектуальному аналізі даних, машинному навчанні та штучному інтелекті.

Виявлення аномалій фінансових транзакцій дозволяє виявляти підозрілу діяльність, що відхиляється від звичайної поведінки системи або користувачів. Сучасні моделі аналізують багатовимірні дані – суми, час, пристрої, геолокацію, моделі поведінки і на основі цього створюють оцінку ризику для кожної транзакції. Використання таких підходів забезпечує більш гнучку, адаптивну та ефективну систему захисту.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ ТА СУЧАСНИХ ПІДХОДІВ ДО ВИЯВЛЕННЯ АНОМАЛІЙ У ФІНАНСОВИХ ТРАНЗАКЦІЯХ

1.1 Актуальність проблеми

Зі швидким розвитком цифрових фінансових сервісів та банківських послуг обсяг фінансових транзакцій, що здійснюються в режимі реального часу, зростає. Це створює передумови для виникнення аномалій – операція або серія дій, що суттєво відхиляються від звичайної поведінки клієнта або типових моделей транзакцій. У світлі цього, виявлення порушень у фінансових операціях стає критично важливою сферою для забезпечення надійності та безпеки банківських інформаційних систем.

З огляду на значний обсяг платежів, що здійснюються щодня, та нестачу фактичних аномальних транзакцій у системах високовартісних платежів, виявлення аномалій нагадує спробу знайти голку в копиці сіна [1]. Більше того, складність полягає не лише в обсягах шахрайських схем та транзакцій, але й у швидкості змін їхнього характеру. У сучасних фінансових процесах аномальні транзакції можуть бути різноманітними за типом, структурою, каналом передачі та географічним розташуванням, що вимагає високого ступеня адаптивності від систем виявлення.

Таким чином, актуальність теми полягає в поєднанні трьох основних факторів:

- величезного зростання обсягів фінансових операцій;
- прагнення банків автоматизувати та застосовувати аналітику і штучний інтелект;
- зростання та розвиток складності систем виявлення аномальної або шахрайської діяльності.

Всі ці фактори створюють середовище, в якому ефективна система виявлення аномалій є необхідною умовою забезпечення безпеки банківських інформаційних систем.

Зростання обсягу фінансових транзакцій та ускладнення механізмів шахрайства змушують банки не лише модернізувати свої технологічні платформи, а й трансформувати внутрішні управлінські та операційні процеси [2]. Сучасні системи виявлення аномалій інтегруються у широкий спектр банківських бізнес-процесів, взаємодіючи з підрозділами, які відповідають за управління ризиками, фінансовий моніторинг, інформаційну безпеку, контроль транзакцій, аналітику та IT-підтримку.

Ефективність таких систем багато в чому залежить від координації роботи структурних підрозділів банку, які відповідають за збір, передачу, аналіз та реагування на підозрілі транзакції. Тому для розуміння контексту системи виявлення аномалій важливо враховувати організаційну структуру банківської установи, в рамках якої обробляються фінансові транзакції та контролюється їхня безпека.

Нижче (рисунок 1.1) наведено узагальнену організаційну структуру банку на основі офіційного документу [3], що показує розподіл обов'язків між підрозділами та їх взаємодію в галузях управління ризиками, безпеки та обробки транзакцій:

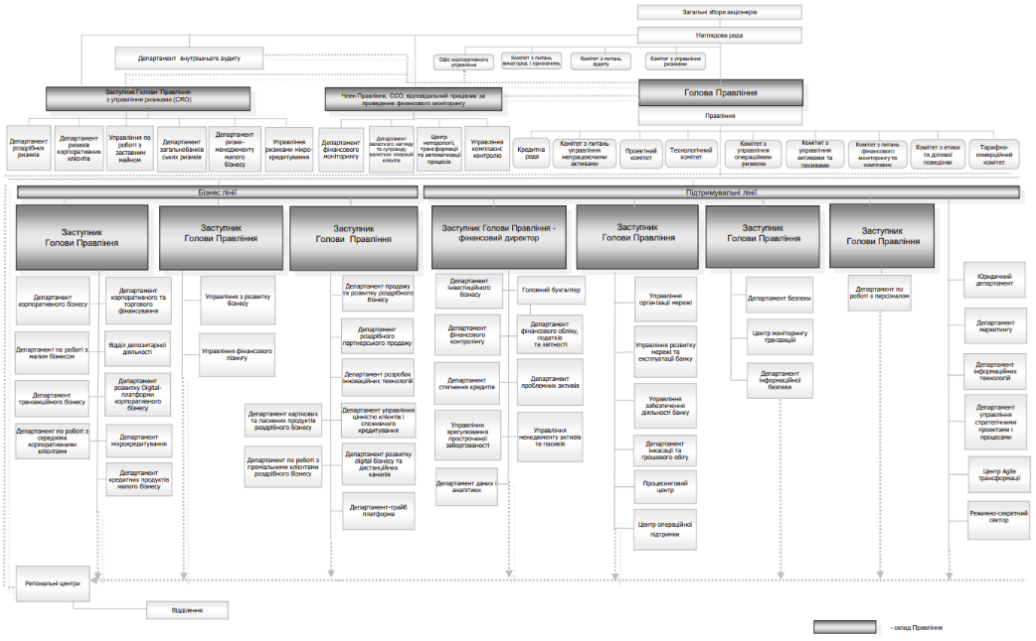


Рисунок 1.1 – Структура ІС банку

1.2 Характеристика банківських інформаційних систем (БІС) та транзакцій

1.2.1 Архітектура БІС

Банківські інформаційні системи є ключовими компонентами сучасної фінансової інфраструктури, які автоматизують, обробляють та контролюють фінансові операції клієнтів. Типові операції, що обробляються такими системами, включають грошові перекази, оплату товарів та послуг, внесення та зняття готівки, депозитні послуги, міжнародні перекази та інші види фінансових потоків.

БІС повинна працювати безперервно, з високою продуктивністю та надійністю, оскільки будь-яка затримка або збій може призвести до підриву довіри клієнтів або значних фінансових втрат.

Типова архітектура БІС включає декілька функціональних модулів:

− модуль обробки транзакцій – отримує, перевіряє, керує та записує транзакції в базах даних;

− модуль потокової обробки – використовується для аналізу транзакцій у режимі реального часу, що дозволяє швидко виявляти підозрілі транзакції;

− модуль зберігання історичних даних – збирає історію транзакцій для подальшого аналізу та навчання моделей виявлення аномалій;

− аналітичний модуль – виявляє закономірності, тенденції та аномалії в даних;

− модуль моніторингу та реагування на інциденти – відповідає за сповіщення, блокування транзакцій та подальше розслідування інцидентів.

Такі системи зазвичай побудовані на SOA або мікросервісному підході, що дозволяє гнучко масштабувати окремі компоненти. Обробка транзакцій зазвичай виконується за допомогою технологій OLTP, а аналітичні завдання виконуються за допомогою технологій OLAP.

Сучасні банківські системи також інтегруються з платіжними

шлюзами, аналітичними платформами та інструментами боротьби з шахрайством і повинні відповідати міжнародним стандартам безпеки.

Нижче (рисунок 1.2) наведено приклад функціональної структури ІС банку:

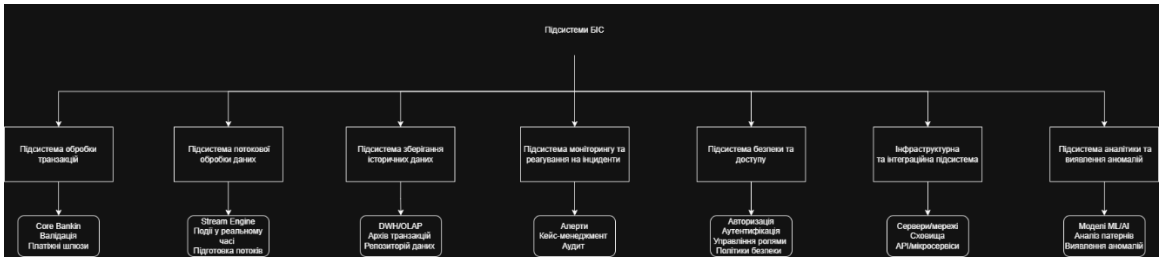


Рисунок 1.2 – Функціональна структура ІС банку

1.2.2 Особливості фінансових транзакцій як об’єкта аналізу

Фінансова транзакція – це структурований запис грошової операції, що містить набір параметрів (атрибутів), що відображають як саму подію, так і її контекст. Типові атрибути:

- сума операції;
- дата й час проведення;
- географічне розташування відправника та одержувача;
- тип і канал проведення;
- тип пристрою або браузера;
- інформація про рахунок, банк-емітент, IP-адресу;
- історія попередніх транзакцій користувача.

Окрім статичних характеристик, важливими також є поведінкові характеристики клієнта – частота транзакцій, середній розмір транзакції, часові інтервали між транзакціями, моделі активності, що спостерігаються в різний час доби або години. Такі показники формують так званий поведінковий профіль клієнта, який можна використовувати для виявлення

аномалій. Індикатори зміни поведінки дозволяють значно точніше ідентифікувати аномальні фінансові операції [4].

1.3 Аналіз сучасних методів виявлення аномалій

Методи виявлення аномалій поділяють на статистичні, класичні алгоритми машинного навчання, глибоке навчання та підходи на основі графів; кожен клас має свої сильні й слабкі сторони та сферу застосування.

Методи на основі правил та порогові системи: прості, інтуїтивно зрозумілі підходи, що базуються на експертних правилах наприклад, необґрунтовано велика сума, транзакція в іноземній країні тощо. Переваги: прозорість, швидкість, легка інтеграція в бізнес-процеси. Недоліки: низька адаптивність, потребують постійного оновлення правил, погано працюють зі складними схемами шахрайства. Ці методи часто використовуються як перший рівень фільтрації.

Класичні статистичні методи основані на моделях, що оцінюють ймовірнісні характеристики транзакцій. Використовуються для виявлення окремих викидів на основі простих статистичних ознак. Мають обмежену здатність фіксувати багатовимірні, контекстні або колективні аномалії.

Алгоритми без нагляду та напівконтрольовані:

– кластеризація: відділяють «рідкісні» спостереження від великих груп; чутливі до масштабу та вибору параметрів;

– Local Outlier Factor (LOF), One-Class support vector machine (SVM). Корисний для багатовимірних даних, але вимагає точного налаштування та чутлива до кількості шуму;

– Isolation Forest. Алгоритм, який ізолює аномалії шляхом побудови випадкових дерев; добре масштабується та часто використовується для транзакційних даних. Isolation Forest продемонстрував високу

продуктивність у багатьох прикладних дослідженнях, що стосуються кредитних транзакцій.

Класичні методи під наглядом. Використовують мічені приклади шахрайства для побудови класифікаторів (логістична регресія, Random Forest, XGBoost). Переваги – висока точність при достатній якості міток. Проблеми – значна незбалансованість класів (дуже мало випадків шахрайства), «застарівання» моделей коли шахраї змінюють тактику, труднощі зі збором надійних міток. Для подолання дисбалансу часто використовуються методи повторної вибірки, зважження класів та спеціальні метрики.

До методів на основі глибокого навчання належать:

– автоенкодери (від англ., autoencoder) – навчаються відтворювати нормальні транзакції; великі похибки реконструкції вказують на аномалію. Ефективні там, де мало позначених аномалій;

– рекурентні нейромережі та трансформери – моделюють послідовності транзакцій заданого клієнта (часові шаблони); вони дозволяють виявляти аномалії в поведінці користувача;

– комбінації – наприклад, автоенкодер на частотних ознаках і класифікатор. Глибоке навчання дає кращі результати на великих даних, але потребує обчислювальних ресурсів та складніше для інтерпретації.

Мережеві та графові підходи: графові нейронні мережі дозволяють моделювати відношення й виявляти «синдикати» шахрайських дій. Останні дослідження показують, що графові нейронні мережі добре вловлюють міжсуб’єктні аномалії й суттєво підвищують якість детекції у випадках, де прості табличні методи зазнають поразки.

Гібридні та ансамблеві методи: поєднання декількох підходів, підвищує показники і знижує кількість хибних спрацьовувань. Ансамблі дозволяють поєднати сильні сторони різних класів моделей, але ускладнюють інтерпретацію та експлуатацію.

1.4 Проблеми застосування систем виявлення аномалій

Незважаючи на стрімкий розвиток методів машинного навчання та збільшення обчислювальної потужності, впровадження систем виявлення аномалій у фінансовому секторі залишається складним завданням. Банківські системи стикаються не лише з технічними перешкодами, а й з організаційними та методологічними проблемами.

Однією з найсерйозніших проблем є значний дисбаланс вибірки – кількість нормальних (легітимних) транзакцій у сотні тисяч разів перевищує кількість шахрайських транзакцій. У типовій базі даних кредитних карток лише близько 0,17% транзакцій позначаються як шахрайські. За таких умов стандартні алгоритми класифікації схильні «навчатися» надавати перевагу більшості, ігноруючи рідкісні події. Це призводить до високої загальної точності, але низьких показників виявлення шахрайства. Щоб подолати це, використовуються методи повторної вибірки, змінні ваги класів, спеціальні метрики (точність, повнота, F1-оцінка) або напівконтрольовані підходи. Але ці методи не надають гарантію, що будуть стабільні результати, якщо дані містять шум, дублювання, помилки або відсутні ознаки.

Ще однією проблемою є якість даних. Транзакції у фінансових системах часто неповні, а деякі поля навмисно скриті для забезпечення захисту даних. Це ускладнює розробку інформативних ознак та знижує ефективність моделей.

Фінансове шахрайство характеризується моделями поведінки, що постійно змінюються. Шахраї швидко адаптуються до нових правил, змінюють методи обходу заходів безпеки та використовують автоматизовані інструменти для створення нових типів транзакцій. Це явище відоме як concept drift — зміна статистичних характеристик даних у часі [5]. Якщо модель не оновлюється регулярно, її продуктивність швидко знижується. Виявлення дріфту в режимі реального часу потребує складних механізмів

моніторингу, періодичного навчання моделі та систем безперервного контролю якості.

У банківському секторі важливо пояснювати результати. Навіть якщо модель демонструє високу точність, її рішення мають бути зрозумілими як аналітикам, так і органам, що регулюють. Багато країн вимагають від фінансових установ пояснювати, чому конкретну транзакцію було відхилено або позначено як підозрілу.

Ще одна проблема пов'язана з тим, що більшість банків мають історично сформовані, гетерогенні інформаційні системи, у яких транзакційні дані зберігаються в різних форматах, базах і каналах. Інтеграція систем виявлення аномалій у таку інфраструктуру часто ускладнюється:

− застарілими архітектурними рішеннями (монолітні системи без API або з мінімальною масштабованістю);

− обмеженнями доступу до даних у режимі реального часу;

− компромісом між швидкістю обробки транзакцій та затримкою складних моделей;

− вимогами до високої надійності часу безперебійної роботи та відсутності затримок перевірки транзакцій.

В результаті, навіть добре навчена модель може бути непридатною для операційного використання, якщо її неможливо ефективно інтегрувати у виробниче середовище банку.

Високі обчислювальні вимоги є ще однією серйозною проблемою. Глибокі нейронні мережі або ансамблеві алгоритми вимагають високопродуктивних графічних процесорів, великого обсягу пам'яті та розподіленого сховища. Для банків з великими обсягами транзакцій це створює проблеми масштабованості та затримки. У багатьох випадках моделі повинні працювати в потоковому режимі, тобто їм потрібно приймати рішення за частки секунди. Навіть невелика затримка може заблокувати легітимну транзакцію або, навпаки, пропустити шахрайську транзакцію [6].

Окрім технічних проблем, значну роль відіграє людський фактор.

Навіть найкраща модель буде неефективною без належного контролю, взаємодії з аналітиками та актуальних політик безпеки. Історія показує, що у більшості банків остаточне рішення про блокування чи підтвердження транзакції приймає одна людина. Це вимагає розробки зручних інтерфейсів, звітів, інструментів візуалізації та систем підтримки прийняття рішень, що дозволяють фахівцям швидко оцінювати ситуацію та розуміти логіку роботи моделі.

1.5 Постановка задачі дослідження

Аналіз поточного стану банківських інформаційних систем та існуючих підходів до виявлення аномалій у фінансових транзакціях показує, що традиційні інструменти моніторингу безпеки не забезпечують належного рівня захисту. Стрімке зростання цифрових транзакцій, розширення спектру фінансових послуг і поява складних шахрайських систем, що постійно розвиваються, зумовлюють необхідність у методах, що поєднують різні підходи до аналізу даних. Враховуючи високу динаміку фінансового середовища та мінливість моделей поведінки користувачів, особливого значення набуває синтез методів статистики, машинного та глибокого навчання, що дозволяє підвищити точність та стійкість систем виявлення аномалій.

Створення ефективної системи вимагає поєднання аналізу транзакцій у реальному часі, багатовимірної обробки залежностей та здатності адаптуватися до нових типів порушень без повного перенавчання. Однак розробка такого комплексного рішення ускладнюється низкою факторів: шумом даних, нерівномірним розподілом аномальних випадків, вимогами до інтерпретації результатів, необхідністю масштабованості та можливістю інтеграції з банківською інфраструктурою.

У зв'язку з цими обмеженнями виникає завдання формального визначення дослідницької проблеми, що включає як аналіз окремих алгоритмів, так і вивчення можливостей їх комбінування з підвищення ефективності виявлення аномальних транзакцій.

Метою даного дослідження є розробка, валідація та експериментальне тестування синтезованого методу до виявлення аномалій, що поєднує статистичні методи, моделі машинного навчання та глибоку архітектуру та інтегрується в банківську інформаційну систему. Цей підхід має забезпечити точність, швидкість, надійність, здатність виявляти нові види шахрайства та гарантовану інтерпретацію для бізнес-користувачів та регулюючих органів.

На основі аналітичного огляду сформульовано загальну концепцію дослідження. Необхідно синтезувати сучасні моделі та методи виявлення аномалій у фінансових транзакціях, визначити можливості їх комбінування, розробити концептуальну архітектуру комплексної системи виявлення аномалій, обґрунтувати вибір алгоритмів та принципів їх взаємодії, що забезпечують високу точність та адаптивність.

Для виконання поставленої задачі передбачається здійснити такі дослідницькі кроки:

− формулювання вимог до комбіновоної моделі виявлення аномалій, що враховує технічні, алгоритмічні та бізнес-орієнтовані обмеження банківського середовища;

− аналіз можливостей інтеграції статистичних методів, моделей машинного навчання та глибоких нейронних мереж для підвищення точності та гнучкості системи;

− визначення критеріїв оцінки ефективності синтезованого підходу, приділяючи особливу увагу точності, стійкості, продуктивності, масштабованості та інтерпретованості;

− розробка теоретичних основ архітектури комплексного рішення, включаючи інтеграцію алгоритмів та їхню погоджену роботу в реальних транзакційних процесах;

− створення бази для подальшої програмної реалізації, опис модульної структури системи, характеристик даних, механізмів уніфікації результатів моделювання та архітектури обчислювальної інфраструктури.

2. ТЕОРЕТИЧНІ ОСНОВИ МОДЕЛЕЙ І МЕТОДІВ ВИЯВЛЕННЯ АНОМАЛІЙ

2.1 Математичні основи базових алгоритмів

2.1.1 Метод Isolation Forest

Isolation Forest – алгоритм без учителя, який грунтується на ідеї, що аномальні точки легше ізолювати, ніж нормальні [7]. Замість побудови моделі нормальної поведінки чи щільності, метод випадково розбиває простір ознак до того часу, поки ознака буде повністю ізольованою від інших.

Алгоритм генерує ансамбль дерев рішень, де на кожному кроці вибирається випадкова ознака і випадковий поріг.

Оцінка "аномальності" розраховується за формулою:

$$s(x, m) = 2^{-\frac{E(h(x))}{c(m)}}, \tag{2.1}$$

де $h(x)$ – кількість розділень, необхідних для ізоляції точки x;

$E(h(x))$ – середня довжина шляху до ізоляції точки x.

$$c(m) = 2H(m-1) - \frac{2(m-1)}{m}, \tag{2.2}$$

де $c(m)$ – нормалізаційний коефіцієнт, що враховує розмір вибірки m;

$H(i)$ – гармонічне число, яке апроксимується як $H(i) \approx \ln i + 0.5772156649$ (константа Ейлера–Маскероні).

Якщо $s(x)$ близьке до 1 – об'єкт, скоріше за все, аномальний; якщо до 0.5 – нормальний.

Практичні аспекти:

− переваги: не потребує маркованих даних; масштабується лінійно;

стійкий до шумів; ефективний при більших обсягах транзакцій;

− недоліки: чутливість до розміру дерева та вибору альфа-каналу; потенційне збільшення частки хибнопозитивних результатів; погана інтерпретованість;

− приклад у банківських системах: ізолювальні ліси часто використовуються як перший рівень для швидкої фільтрації підозрілих транзакцій у потоках даних у режимі реального часу.

2.1.2 Метод One-Class SVM

One-Class Support Vector Machine – це алгоритм, що створює межу, що відокремлює «нормальні» дані від усього простору. Цей метод є напівконтрольованим, оскільки для навчання потрібні лише неаномальні дані.

OCSVM шукає гіперплощину в просторовому ядрі $\phi(x)$, яка відділяє більшість спостережень від початку координат, залишаючи при цьому мінімальну частину точок поза межами [8].

Задача зводиться до мінімізації регуляризованого функціонала:

$$\min_{\omega,\rho,\xi} \frac{1}{2}\|\omega\|^2 + \frac{1}{\upsilon n}\sum_{i=1}^{n}\xi_i - \rho, \qquad (2.3)$$

за умов:

$$\left(\omega\phi(x_i)\right) \geq \rho - \xi_i, \qquad \xi_i \geq 0$$

де ω – вектор ваг;

ρ – поріг відсікання;

ξ_i – штрафи за порушення межі;

$\upsilon \in (0,1]$ – параметр, який контролює частку очікуваних аномалій та впливає на жорсткість моделі.

Точки, що лежать поза побудованою областю, класифікуються як аномальні.

Практичні особливості:

− переваги: сувора математична основа; можливість використання нелінійних ядер (наприклад, RBF) для подання складних залежностей; Хороша продуктивність на вибірках середнього розміру;

− недоліки: висока чутливість до вибору параметрів υ та ядра; погана масштабованість при великих обсягах транзакцій; потрібна нормалізація ознак;

− у банківських програмах: використовується для профілювання поведінки клієнтів або виявлення рідкісних закономірностей в обмежених наборах даних, наприклад, при скринінгу VIP-клієнтів.

2.1.3 Autoencoder

Autoencoder – це штучна нейронна мережа, що навчається відтворювати вхідні дані через проміжний стислий шар. Ідея полягає в тому, що, навчаючись на нормальних транзакціях, мережа навчається ефективно кодувати лише характерні паттерни нормальної поведінки. Аномалії, що не відповідають цим патернам, реконструюються менш ефективно [9].

Автоенкодер складається з двох частин:

− кодувальник $\mathrm{g}(x)$, який зменшує розмірність даних:

$$z = \mathrm{g}(x) = \sigma(W_1 x + b_1), \tag{2.4}$$

− декодувальник $f(z)$, який відновлює вхід:

$$\mu = f(z) = \sigma(W_2 z + b_2). \quad (2.5)$$

Функція втрат визначається як середньоквадратична похибка:

$$L = \frac{1}{n}\sum_{i=1}^{n}\|x_i - f(g(x_i))\|^2, \quad (2.6)$$

де n – кількість навчальних прикладів (транзакцій);

x_i – вхідні дані для і-го прикладу.

Для аномальних транзакцій ця похибка суттєво вища, що дозволяє встановити поріг аномальності τ.

Практичні переваги та обмеження:

− переваги: здатний виявляти складні, нелінійні та багатовимірні невідповідності; добре працює із широким спектром ознак; може гнучко комбінуватись з іншими алгоритмами (наприклад, Isolation Forest для подальшої обробки прихованого простору);

− недоліки: вимагає великого обсягу навчальних даних; схильний до перенавчання; важко пояснити; потребує значних обчислювальних ресурсів;

− практичне застосування: використовується у великих банках у складі багатошарової архітектури, де автокодировщик спочатку генерує узагальнене уявлення транзакції, а класифікатор другою етапі визначає рівень ризику.

2.2 Порівняльний аналіз алгоритмів

Після вивчення математичних основ різних моделей виявлення аномалій доцільно провести порівняльний аналіз їх характеристик з метою оцінки придатності кожного методу застосування у фінансових інформаційних системах.

Оскільки банківські дані мають специфічні характеристики – високу розмірність, сильний дисбаланс класів, тимчасову динаміку та необхідність

швидкої обробки – вибір алгоритму виявлення має ґрунтуватися не лише на його теоретичній точності, а й на практичних аспектах: масштабованості, інтерпретованості та адаптивності до змін навколишнього середовища.

У таблиці 2.1 подано порівняння основних сучасних методів виявлення аномалій, що використовуються у фінансових та банківських інформаційних системах. Аналіз включає основні характеристики кожного підходу, включаючи переваги, обмеження, тип навчання та типові сфери застосування.

Таблиця 2.1 – Порівняння методів виявлення аномалій

Метод	Переваги	Обмеження	Тип навчання	Типові застосування
1	2	3	4	5
Isolation Forest	Не потребує мічених даних, добре масштабується, ефективний для великих потоків транзакцій	Чутливий до параметрів (кількість дерев, вибірки), інтерпретація обмежена	Без нагляду	Потокова фільтрація підозрілих транзакцій
One-Class SVM	Теоретично обґрунтований, працює з нелінійними ядрами	Повільний на великих даних, складне налаштування параметрів	Напівконтрольований	Поведінковий аналіз клієнтів, профілювання користувачів

Продовження таблиці 2.1

1	2	3	4	5
Autoencoder	Виявляє складні нелінійні відхилення, можливість гібридних моделей	Високі вимоги до ресурсів, складність інтерпретації	Без нагляду	Виявлення складних фінансових аномалій, fraud detection
LOF	Добре працює у багатовимірних просторах	Не масштабується на великі дані	Без нагляду	Аналіз невеликих сегментів клієнтів
Generative Adversarial Networks	Може моделювати рідкісні шаблони аномалій	Складність навчання, нестабільність генератора	Напівконтрольований	Синтетзоване створення або підсилення рідкісних даних

Як видно з таблиці, жоден окремий метод не є універсальним для всіх типів банківських завдань. Алгоритми на основі дерев рішень, такі як Isolation Forest, відзначаються швидкістю та простотою інтеграції, але мають обмежену інтерпретованість. One-Class SVM забезпечує строгі теоретичні гарантії, проте є менш ефективним на потокових або великих даних. Autoencoder і GAN демонструють найкращі результати в ситуаціях, коли закономірності дуже складні або нелінійні, але потребують потужних обчислювальних ресурсів і ретельного налаштування.

У сучасних банківських інформаційних системах часто застосовується

гібридний підхід, що поєднує декілька методів:

- autoencoder для побудови узагальненого представлення транзакцій;
- Isolation Forest для виявлення відхилень у зменшеному латентному просторі;
- SVM або LOF як додатковий рівень перевірки.

Такий комбінований підхід підвищує точність, скорочує кількість помилкових спрацьовувань та забезпечує адаптованість до нових шахрайських схем.

2.3 Теоретична модель інтеграції системи виявлення аномалій

Теоретично інтегрована система виявлення аномалій у банківській інформаційній системі є багаторівневою архітектурою, що інтегрує збір даних, аналітичну обробку, оцінку ризиків і реагування. Така система повинна працювати в режимі реального часу, забезпечуючи баланс між точністю, швидкістю та зрозумілістю рішень.

Основні модулі системи:

а) Модуль збору та попередньої обробки даних

1) Збір потокових транзакцій із різних джерел (банківські термінали, мобільний банкінг, POS-системи);

2) Фільтрація та очищення даних, усунення пропусків і аномальних записів;

3) Нормалізація ознак, створення похідних характеристик;

4) Агрегація за клієнтами, картками або часовими інтервалами;

б) Модуль аналітики

1) Застосування вибраних алгоритмів для обчислення ймовірності аномалії кожної транзакції;

2) Можлива комбінація кількох моделей у ансамблі (гібридний

підхід);

в) Модуль оцінки ризику та пояснення результатів

1) Перетворення числових "аномалійних скорів" у категорії ризику (низький / середній / високий);

2) Використання explainable AI для пояснення рішень моделей;

3) Формування звітів для аналітиків служби безпеки з указанням причин виявлення;

г) Модуль реагування

1) При перевищенні порогового рівня ризику транзакція позначається як підозріла;

2) Можливі сценарії реагування: автоматичне блокування транзакції, ручна перевірка аналітиком, надсилання сповіщення клієнту або ініціювання додаткової верифікації.

Також є важливі аспекти при реалізації системи:

− інтеграція з існуючими системами банку через REST API, брокери повідомлень або ETL-процеси;

− масштабування – використання контейнеризації та мікросервісної архітектури;

− адаптивність – регулярне донавчання моделей на нових даних для боротьби з concept drift;

− інтерпретованість – формування зрозумілих звітів і пояснень для користувачів і регуляторів;

− безпека та відповідність законодавству – дотримання норм GDPR, PSD2, ISO/IEC 27001.

3 СИНТЕЗОВАНИЙ МЕТОД ВИЯВЛЕННЯ АНОМАЛІЙ У ФІНАНСОВИХ ТРАНЗАКЦІЯХ

3.1 Загальна концепція синтезованого методу

Сучасні банківські інформаційні системи працюють у складному, високодинамічному середовищі, де обсяги транзакцій зростають експоненційно, а моделі поведінки користувачів постійно змінюються у зв'язку з розвитком фінтех-сектору. Поширення послуг мобільного банкінгу, збільшення частоти транзакцій на невеликі суми, повсюдне використання платежів за QR-кодами та дистанційними сервісами суттєво ускладнюють процес здійснення транзакцій. У таких умовах аномальні операції можуть проявлятися не лише як різкі разові відхилення, але й як тонкі багатовимірні патерни, що відрізняються від нормальної поведінки тільки у сукупності множини ознак [10].

У науковій літературі виділяють три базові типи аномалій у фінансових даних:

- behavioral anomalies – відхилення у поведінці конкретного клієнта порівняно з власним історичним профілем;
- structural anomalies – порушення внутрішньої структури взаємозв’язків між ознаками транзакцій;
- contextual anomalies – нормальні операції у загальному випадку, але аномальні у певному контексті (час, локація, мережеве середовище, тип пристрою).

Кожен із цих типів аномалій потребує різного аналітичного підходу, оскільки одна й та сама транзакція може бути нормальною згідно зі статистичними критеріями, але незвичайною у поведінковому контексті чи нелогічною з погляду структурної моделі клієнта.

Для подолання виявлених обмежень у роботі запропоновано синтезований метод Hybrid Anomaly Detection System for Banking Transactions

(HASBT), який поєднує три категорії моделей, що працюють на різних рівнях абстракції:

− статистичний рівень. Використовується як перший фільтр, що швидко виявляє грубі та глобальні відхилення. Він забезпечує легку інтерпретованість та мінімальні затрати ресурсів;

− алгоритмічний рівень машинного навчання. На цьому рівні застосовуються безнаглядові алгоритми на кшталт Isolation Forest або One-Class SVM. Вони здатні моделювати багатовимірні поведінкові профілі користувачів та виявляти аномалії, непомітні для статистичних моделей;

− ;либинний рівень. Autoencoder моделює внутрішню структуру нормальних транзакцій через компактне латентне представлення. Значні відхилення реконструкційної похибки вказують на нетипові або шахрайські операції, які інші рівні можуть не відловити.

Нижче (рисунок 3.1) наведено діаграму систезованого підходу:

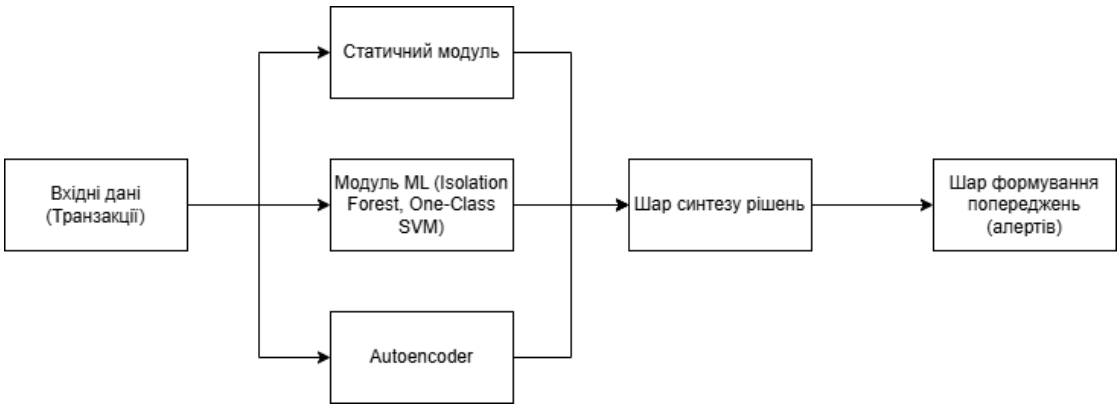


Рисунок 3.1 – Концепція синтезованого підходу HASBT

Спільне використання цих моделей забезпечує синергетичний ефект, який підвищує точність виявлення аномалій, скорочує кількість хибних спрацьовувань та дозволяє системі адаптуватися до нових моделей злочинної діяльності.

3.2 Структура синтезованого методу HASBT

Структура запропонованого методу HASBT побудований на принципах модульності, масштабованості та відмовостійкості. Вона призначена для інтеграції у промислові банківські інформаційні системи, які функціонують у середовищі значних навантажень та різнорідних потоків транзакцій. Основна мета архітектури – забезпечити поетапну обробку даних, синтез результатів кількох методів та формування єдиної оцінки ризику кожної транзакції в реальному часі.

Система має багаторівневу організацію, де кожен модуль відповідає за певний аспект аналізу даних: від попередньої обробки до глибокої реконструкції та спільного злиття результатів. Такий підхід оптимізує обчислювальні витрати, забезпечує незалежність компонентів та полегшує оновлення методів без шкоди для цілісності системи. Модульна архітектура рекомендована провідними дослідниками фінансової кібербезпеки, включаючи, які наголошують на важливості комбінування різних механізмів виявлення для досягнення збалансованого рівня чутливості та специфічності [11].

У HASBT кожен модуль працює автономно, але взаємодіє через стандартизовані інтерфейси. Це дозволяє масштабувати як окремі компоненти, так і всю систему в цілому, що є критично важливим для банківських платформ з піковими навантаженнями у тисячі транзакцій на секунду.

Основними компонентами архітектури є такі модулі:

− модуль потокового збору транзакцій. Забезпечує отримання даних транзакцій із різних джерел: мобільний банкінг, веб-банкінг, платіжні шлюзи (Visa/Mastercard), банкомати, POS-термінали. Використовує технології потокової обробки, такі як Apache Kafka, Apache Flink, RabbitMQ, що дозволяє досягати мінімальної затримки та забезпечувати рівномірний

розподіл навантажень. Модуль також відповідає за валідацію структури вхідних записів, контроль коректності полів та відмовостійкість при похибках передачі даних;

− модуль очищення та попередньої обробки даних. Даний модуль готує сировинні дані до подальшої аналітики. Основні функції: видалення дублікатів, фільтрація шумів та аномальних форматів, нормалізація валютних значень, переведення категоріальних змінних у числові, заповнення пропущених значень, нормалізація шкал значень. Попередня обробка є критично важливою, оскільки чистота даних прямо визначає коректність роботи Autoencoder та моделей «без нагляду». Якість вхідних даних є фундаментальним фактором у задачах anomaly detection [11];

− модуль інженерії ознак. Цей модуль формує множину ознак, які характеризують транзакцію з різних боків. Особливу увагу приділено: агрегованим часовим вікнам (1 хв, 10 хв, 1 год), поведінковим профілям клієнта, географічним закономірностям, транзакційним патернам, ризиковим характеристикам MCC-кодів. Модуль працює як окрема підсистема, що попередньо генерує фічі для ML та DL моделей. Це дозволяє досягати високої швидкодії та не перевантажувати статистичний блок зайвою інформацією;

− статистичний модуль первинного детектування. На цьому етапі застосовуються Z-score, модифікований IQR, MAD, Hampel filter. Статистичний модуль працює у режимі фільтрації «першої лінії», відсікаючи транзакції зі значними числовими відхиленнями. Таким чином, лише частина даних передається на наступні рівні, що знижує навантаження на моделі машинного навчання та глибинні мережі;

− модуль машинного навчання. Цей модуль відповідає за поведінкове та структурне моделювання транзакцій через алгоритми без учителя. У розподіленому середовищі модуль виконується окремо від статистичного блоку, щоб забезпечити стійкість до змін розподілів даних та можливість оновлення без зупинки роботи системи;

− глибинний модуль Autoencoder. Autoencoder виконує кодування транзакції у компактний латентний простір, реконструкцію вхідного вектора, обчислення похибки відновлення, визначення, чи є відхилення суттєвим. Глибинна модель розміщується окремо, оскільки вимагає більше ресурсів та повинна мати можливість перевчитись у міру появи нових типів поведінки користувачів або шахрайських патернів;

− модуль синтезу рішень. Використовується зважений ансамбль. Центральний компонент системи, що об’єднує три значення: оцінку статистичного модуля, поведінкову оцінку ML-модуля, реконструкційну похибку Autoencoder;

− модуль генерації алертів. Забезпечує генерацію сповіщень про високоризикові транзакції, автоматичне блокування платежів (за потреби), передачу повних логів для аналізу фрод-аналітиками, аудит рішень моделі.

Для наочної демонстрації функціональної логіки запропонованого методу HASBT доцільно уявити її архітектуру з допомогою структурної схеми. Вона відображає взаємозв'язки між основними модулями системи, послідовність обробки транзакційних даних та інтеграцію методів статистичного аналізу, машинного навчання та глибокого моделювання.

Діаграма демонструє, як вхідні дані проходять крізь послідовні етапи очищення, побудови ознак, первинної фільтрації та багаторівневого аналізу, після чого результати комбінуються у модулі синтезу рішень. Такий формат представлення дозволяє візуально оцінити модульність системи, чітку ієрархію операцій та функціональні залежності між компонентами.

Особливо важливою є здатність архітектури масштабувати окремі модулі незалежно один від одного та забезпечувати їхню відмовостійкість, що відповідає вимогам сучасних банківських інформаційних систем. На діаграмі також показано розмежування між високорівневими етапами обробки потоку транзакцій та спеціалізованими моделями виявлення аномалій, що дозволяє оцінити шляхи оптимізації, місця взаємодії з іншими підсистемами банку та можливості розширення системи новими підходами.

Таким чином, наведена нижче (рисунок 3.2) архітектурна схема є контекстною діаграмаю HASBT та структурною основою для подальшого аналізу алгоритмів, реалізації прототипу й проведення експериментальних досліджень.

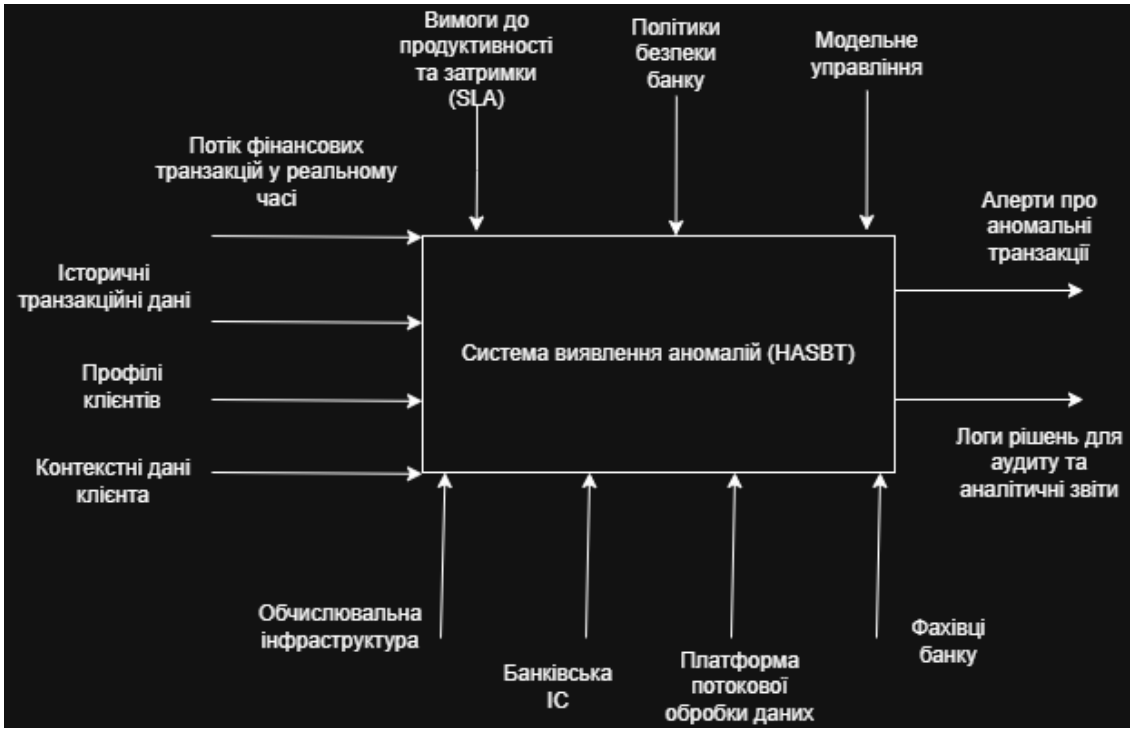


Рисунок 3.2 – Контекстна діаграма HASBT

Схеми декомпозиції системи виявлення аномалій HASBT на рисунках 3.3, 3.4, 3.5, 3.6, 3.7.

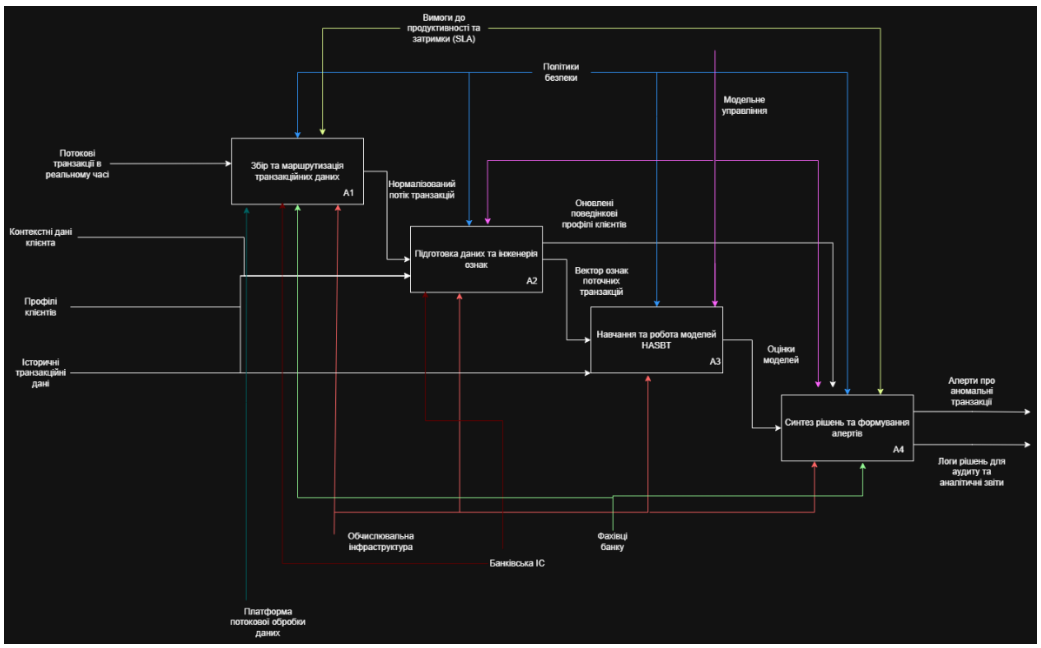


Рисунок 3.3 – Діаграма A0 виявлення аномалій у фінансових транзакціях

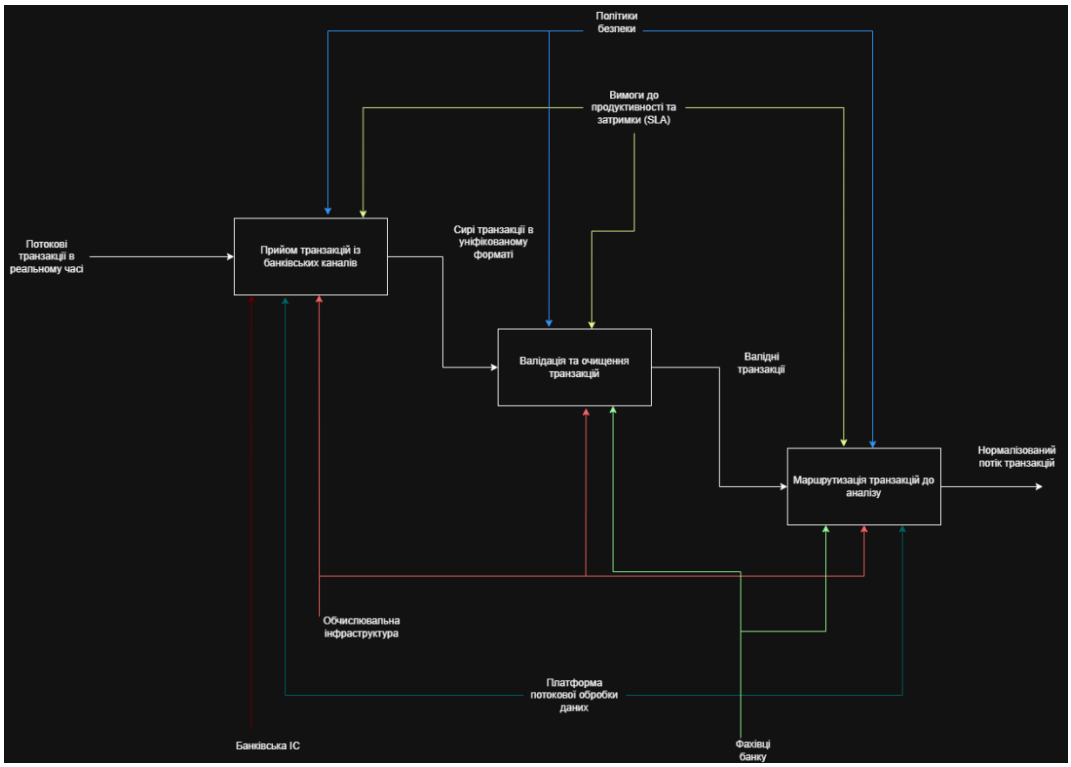


Рисунок 3.4 – Декомпозиція «Збір та маршрутизація транзакційних даних»

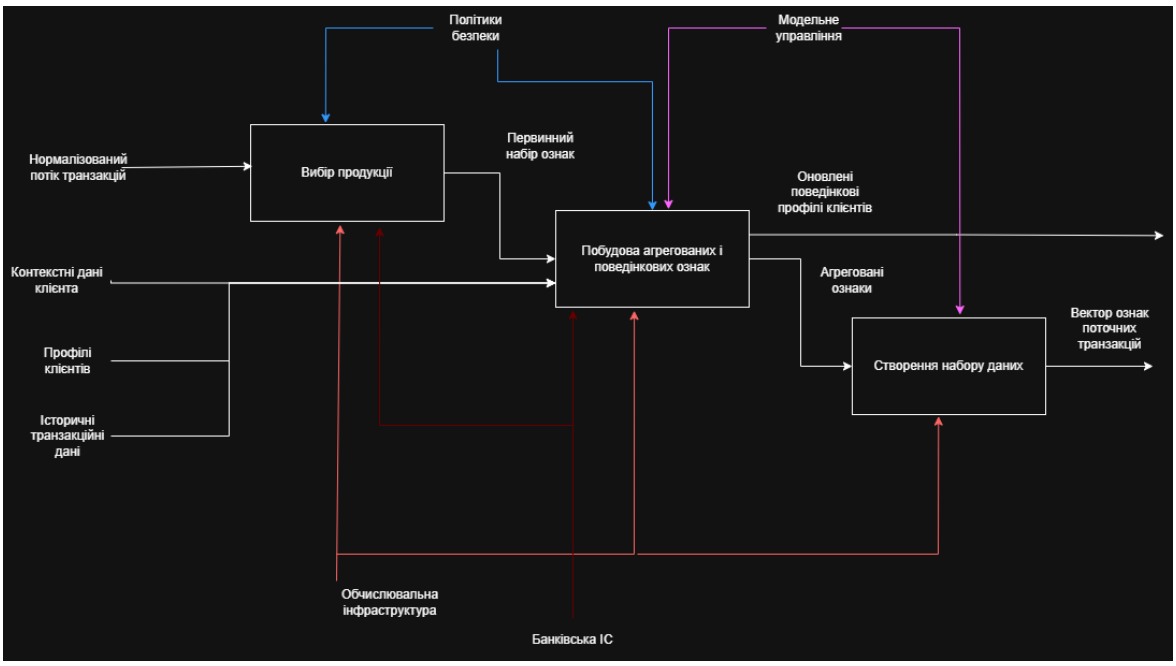


Рисунок 3.5 – Декомпозиція «Підготовка даних та інженерії ознак»

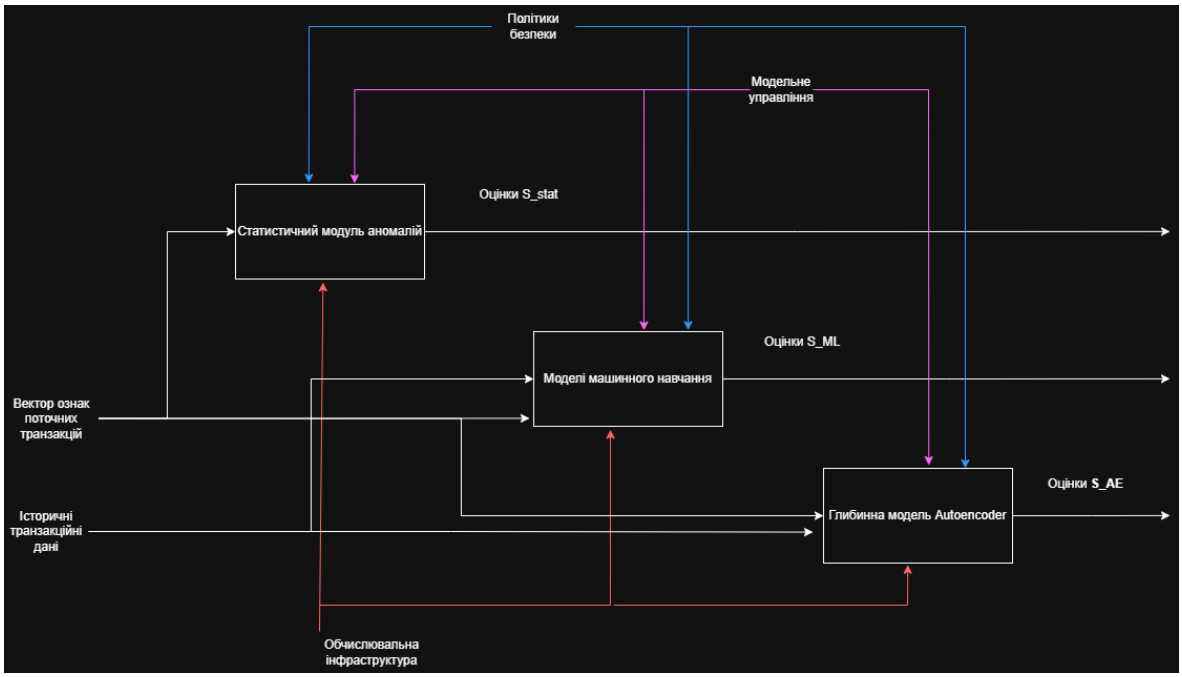


Рисунок 3.6 – Декомпозиція «Навчання та робота моделей HASBT»

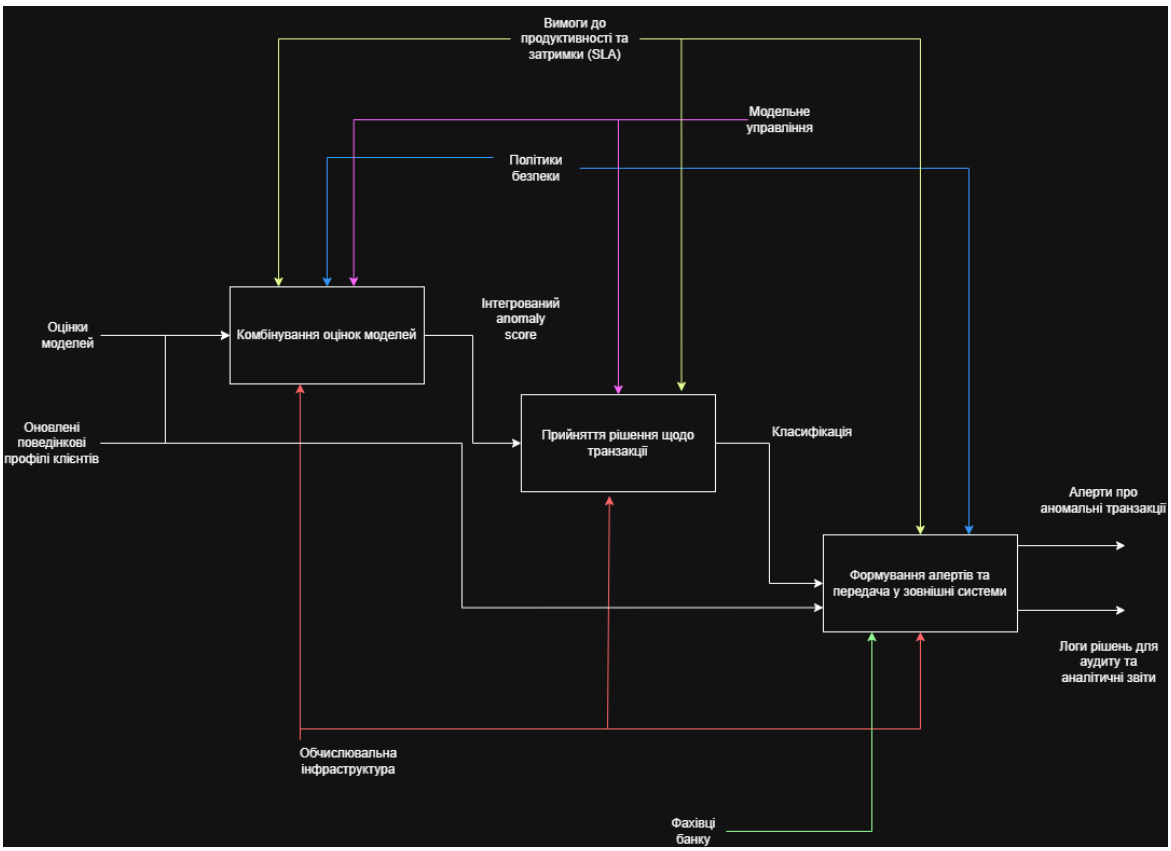


Рисунок 3.7 – Декомпозиція «Синтез рішень та формування алертів»

3.3 Інженерія ознак у синтезованому методі HASBT

3.3.1 Загальні принципи формування ознак

Ефективність будь-якої системи виявлення аномалій суттєво залежить від інформативності ознак, що описують транзакції. У наукових дослідженнях неодноразово зазначалося, що «якість фічей впливає на точність моделі більше, ніж вибір алгоритму» [11]. Це особливо актуально у банківському секторі, де транзакції короткі, лаконічні та часто не містять прямої інформації про шахрайство. У таких умовах інженерія ознак дозволяє створювати структуровані профілі поведінки клієнтів та виявляти приховані закономірності, не видимі у вихідних даних.

У рамках методу HASBT розроблено багаторівневий механізм розробки ознак, що поєднує базові транзакційні характеристики, поведінкові

патерни, географічні та контекстуальні фактори, а також часові та ризикові індикатори. Модуль розробки ознак працює незалежно та надає єдиний набір ознак для статистичного модуля, механізмів машинного навчання та автоенкодера. Такий підхід забезпечує узгодженість вхідних даних на всіх етапах обчислень, підвищуючи стабільність системи та знижуючи ризик хибних спрацьовувань.

Під час створення фічей для фінансових транзакцій враховуються такі принципи:

− інформативність. Кожна ознака повинна містити інформацію, яка розрізняє нормальні та аномальні транзакції;

− стабільність у часі. Ознаки повинні зберігати коректність при зміні поведінки клієнтів;

− мінімум кореляційних дублювань. Надмірно корельовані фічі можуть погіршити роботу Autoencoder та призвести до переобучення моделей;

− робота у реальному часі. Обчислення повинні виконуватися з малою затримкою (<5 мс на транзакцію), щоб підтримувати роботу потокових систем;

− адаптивність до нових патернів. Фічі повинні мати здатність оновлюватися (online-updating), особливо поведінкові та агреговані ознаки.

3.3.2 Класи та характеристики ознак у HASBT

Базові ознаки – це первинна інформація, яка надходить безпосередньо з транзакції і використовується для статистичного аналізу, нормалізації та подальшої роботи ML і DL моделей. До них належать:

− сума транзакції;

− тип операції (переказ, оплата, зняття готівки, депозит);

- канал виконання (POS, ATM, online, mobile);
- валюта операції;
- час доби та день тижня;
- дані щодо отримувача, включаючи MCC-код і категорію сервісу.

Ці ознаки формують «скелет» транзакційного запису та дозволяють виявляти первинні, найбільш очевидні порушення, пов’язані з аномальними сумами, нетиповими операційними каналами або незвичайними категоріями витрат.

Поведінкові ознаки є ключовими у виявленні аномалій, оскільки більшість шахрайських дій проявляються не у вигляді разових екстремальних значень, а у формі відхилень від звичної поведінки клієнта. Дослідження вказують, що реальні фрод-сценарії найчастіше є саме поведінковими [12]. У методі HASBT формуються такі поведінкові характеристики:

- середня сума операцій клієнта за обраний період;
- стандартне відхилення сум операцій;
- коефіцієнт асиметрії (skewness) розподілу витрат;
- частота проведення платежів;
- кількість транзакцій за останні 1, 5 і 15 хвилин;
- частка нових або нетипових отримувачів;
- коефіцієнт різноманітності платежів (entropy of recipients);
- відхилення поточного патерну від історичного профілю клієнта.

Такі фічі дозволяють моделі розрізняти нормальну та потенційно підозрілу поведінку навіть у тих випадках, коли базові характеристики виглядають стандартними.

У сучасних цифрових фінансових сервісах географія транзакцій стала важливим індикатором ризику. Аномалії можуть проявлятися у вигляді незвичного переміщення клієнта, зміни країни, різкого переходу між каналами або підозрілої активності з нового середовища.

Географічні ознаки включають:

- геолокацію транзакції;

- відстань між поточною та попередньою операцією;
- швидкість зміни геолокацій (velocity);
- країну або регіон оператора платежу;
- належність до географічного кластера, характерного для клієнта.

Контекстуальні ознаки охоплюють:

- час доби (нічні операції мають підвищений ризик);
- тип пристрою та його зміну;
- зміну IP-адреси;
- відповідність мережевого трафіку історичним патернам клієнта.

Такі ознаки дозволяють виявляти складні контекстуальні аномалії, які базові моделі пропускають.

Для аналізу динаміки транзакційного потоку системою використовуються часові вікна та агрегуючі функції, що дозволяють виявляти сплески активності або різкі зміни у поведінці клієнта. Основні часові ознаки:

- середнє ковзне значення (rolling mean);
- ковзне стандартне відхилення (rolling std);
- кількість транзакцій у ковзному вікні (rolling sum);
- EWMA – експоненційно зважена ковзна середня;
- медіанне вікно;
- кількість операцій, що перевищують встановлений поріг.

Ці характеристики формують часовий контекст і підвищують здатність моделі виявляти короткотривалі, але критично важливі аномальні «сплески».

Ризикові ознаки використовуються для оцінки транзакцій за непрямими індикаторами, які не пов’язані безпосередньо з поведінкою клієнта, але вказують на підвищену ймовірність шахрайства. До них належать:

- MCC-коди високого ризику;
- чорні та сірі списки контрагентів;
- наявність історичних фрод-інцидентів клієнта;

− різкі зміни у типах витрат або пріоритетах категорій платежів.

Ці ознаки відіграють важливу роль у модулі синтезу рішень, оскільки надають додаткові сигнали про підвищений ризик операції.

У таблиці 3.1 подано основні категорії ознак, приклади їхніх представників, короткий опис інформаційного змісту та вказано модулі, у яких ці ознаки застосовуються. Така класифікація дозволяє чітко зрозуміти, які саме характеристики транзакцій формують основу аналізу, та як кожний тип ознак впливає на роботу статистичних, машинних та глибинних моделей у складі синтезованого методу HASBT.

Таблиця 3.1 – Порівняння методів виявлення аномалій

Категорія ознак	Приклад ознак	Короткий опис	Модуль використання
Базові	Amount	Сума транзакції	Statistical + ML
Поведінкові	ClientEntropy	Ентропія поведінки	ML + AE
Географічні	Distance	Зміна локації	Statistical + ML
Часові	Rolling std	Варіативність у вікні	ML
Ризикові	MCC_Risk	Ризиковість категорії	Ensemble

3.4 Алгоритмічні компоненти синтезованого методу HASBT

Алгоритмічне ядро методу HASBT складається з трьох незалежних, але взаємодоповнюючих модулів: статистичного модуля первинної детекції, модуля машинного навчання та глибинного модуля. Комбінування цих компонентів забезпечує багаторівневу оцінку аномальності транзакцій і

дозволяє компенсувати слабкі місця кожного окремого алгоритму. У літературі зазначається, що шахрайські операції є неоднорідними за своєю природою, тому однорівневі алгоритми мають обмежену ефективність [10], [13].

HASBT застосовує:

- статистичний аналіз. Визначає грубі відхилення;
- алгоритми ML. Моделюють поведінкові патерни;
- Autoencoder. Фіксує нелінійні структурні порушення.

Такий комбінований підхід створює стійку систему, яка здатна працювати з високовимірними, шумними і нерівномірними даними банківських транзакцій.

3.4.1 Статистичний модуль первинної детекції

Статистичний рівень є першим і найшвидшим етапом обробки даних у HASBT. Його основна функція – фільтрація очевидних глобальних аномалій та зменшення навантаження на ML і DL-модулі.

Використані методи:

- Z-score це один із найпоширеніших статистичних методів виявлення аномалій. Він дозволяє оцінити, наскільки значення ознаки x відхиляється від середнього значення μ у одиницях стандартного відхилення σ. Переваги цього методу в тому, що він підходить для виявлення значних відхилень у сумах, а також в простоті та швидкодії. Формула має вигляд:

$$\mathrm{Z} = \frac{x-\mu}{\sigma}, \tag{3.1}$$

- Interquartile Range (IQR). Підходить для розподілів із викидами. Виявлення аномалій за межами:

$$x < Q_1 - 1.5IQR, \;\; x > Q_3 + 1.5IQR, \qquad (3.2)$$

– Median Absolute Deviation (MAD). Стійкий до шумів і спотворених значень.

$$\mathrm{M}AD = \mathrm{median}(|x - \mathrm{median}(x)|), \qquad (3.3)$$

– Hampel Filter. Виявляє короткочасні сплески в потоках даних.

3.4.2 Модуль машинного навчання

Другий рівень – це поведінкове та структурне моделювання клієнтів. HASBT застосовує алгоритми без учителя: Isolation Forest або One-Class SVM. Обидва алгоритми вважаються золотим стандартом у unsupervised anomaly detection [14], [15].

У синтезованому методі HASBT алгоритм Isolation Forest використовується як фундаментальний інструмент для виявлення поведінкових та структурних аномалій у транзакціях. Його застосування виправдане, оскільки дані про транзакції, як правило, багатовимірні, нерівномірно розподілені та містять невелику частку аномальних спостережень. Isolation Forest добре працює в таких умовах, оскільки алгоритму не потрібні розмічені дані і він здатний ефективно виявляти нетипові точки завдяки спеціальному механізму побудови випадкового дерева.

У рамках методу HASBT Isolation Forest виконує такі функції:

– побудова поведінкового профілю клієнтів на основі агрегованих та часових ознак;

− оцінка локальних аномалій, які не мають великого глобального відхилення;

− швидке реагування на зміни у патернах витрат клієнтів;

− фільтрація транзакцій, що потрапляють до «зони підвищеного ризику» навіть за відсутності великих сум або підозрілих MCC-кодів.

Алгоритм добре інтегрується у потокове середовище, оскільки дозволяє виконувати обчислення з низькою затримкою. У методі HASBT моделі Isolation Forest регулярно оновлюються (retraining) на нових даних, що забезпечує адаптивність до змін поведінки користувачів.

Переваги алгоритму, такі як стійкість до шуму та здатність працювати із сильно нерівномірними вибірками, роблять його ключовим компонентом поведінкового аналізу.

One-Class SVM у методі HASBT використовується як другий поведінковий алгоритм, орієнтований на побудову границі нормальності у багатовимірному просторі ознак. На відміну від Isolation Forest, цей метод формує узагальнену гіперповерхню, яка описує «типовий» стан клієнтської активності. Завдяки цьому One-Class SVM є ефективним для виявлення аномалій, що мають тонкий поведінковий характер і не завжди виділяються за окремими ознаками.

У контексті HASBT One-Class SVM виконує такі функції:

− формування індивідуальних «поведінкових оболонок» для кожного клієнта;

− виявлення відхилень, які виходять за межі типових патернів, але не є різкими (наприклад, поступове збільшення частоти невеликих операцій);

− підсилення статистичних та структурних моделей шляхом додавання контекстної оцінки ризику;

− підготовка додаткових сигналів для ансамблю Decision Fusion Layer.

Використання параметра ν дає можливість контролювати частку транзакцій, які можуть бути класифіковані як потенційні аномалії. Це дозволяє адаптувати модель під різні категорії клієнтів та під різні рівні

ризику банку. У методі HASBT One-Class SVM працює у зв’язці з Isolation Forest: перший визначає межу нормальності, а другий – локальні аномалії.

Разом вони забезпечують більш збалансоване виявлення складних порушень, ніж кожен із цих підходів окремо.

3.4.3 Глибинний модуль Autoencoder

Глибинний модуль Autoencoder є третім, найбільш ресурсомістким та інформативним рівнем синтезованого методу HASBT. Його основне призначення – виявлення складних, багатовимірних і нелінійних аномалій, які неможливо виявити статистичними або класичними алгоритмами машинного навчання. На відміну від попередніх модулів, Autoencoder не застосовує прості правила або лінійні межі нормальності, а намагається побудувати внутрішню модель структури нормальних транзакцій і виявити відхилення від цієї структури [16].

Autoencoder виконує такі ключові функції:

− створює компактне латентне представлення транзакції, зберігаючи основні залежності між ознаками;

− відновлює транзакцію на виході, що дає можливість виміряти, наскільки модель “зрозуміла” її структуру;

− оцінює ступінь відхилення поточної транзакції від навченої норми.

Оскільки модель навчається лише на нормальних транзакціях, будь-які відхилення у структурі або поведінці призводять до збільшення реконструкційної похибки. Саме тому Autoencoder є ефективним інструментом для виявлення складних або нових типів шахрайства, які ще не проявлялися у даних.

Принцип роботи у методі HASBT:

− вхідні дані. Попередньо оброблена та нормалізована транзакція з

понад 60 ознаками;

− енкодер стискає дані до латентного вектора меншої розмірності (16-32 нейрони), що дозволяє виділити найважливіші особливості транзакції;

− декодер реконструює транзакцію із латентного простору;

− різниця між оригіналом та реконструкцією інтерпретується як міра відхилення;

− транзакція вважається аномальною, якщо її похибка реконструкції перевищує встановлений поріг.

У методі HASBT поріг визначається статистично – на основі розподілу похибок нормальних транзакцій. Це дозволяє адаптувати модель до реальних умов роботи банку, де структура даних може змінюватися з часом.

Порівняно з іншими моделями, Autoencoder забезпечує такі можливості:

− виявлення складних взаємозв’язків між десятками ознак;

− урахування нелінійних структурних залежностей;

− стійкість до шуму та випадкових локальних відхилень;

− здатність адаптуватися до нових патернів поведінки клієнтів.

У методі HASBT Autoencoder особливо корисний при роботі з транзакціями, які за зовнішніми параметрами не виглядають аномальними, але порушують внутрішню структуру поведінкової моделі клієнта.

Глибинний модуль має і певні недоліки, які необхідно враховувати під час впровадження, а саме те, що він потребує більшої обчислювальної потужності, ніж інші моделі; чутливий до вибору порогу аномальності, який має періодично оновлюватися; може переобучуватися при неправильному формуванні навчальної вибірки.

У методі HASBT ці недоліки компенсуються багаторівневим ансамблевим підходом – рішення Autoencoder не є остаточним, а є частиною загальної системи оцінювання.

3.5 Модуль синтезу рішень (Decision Fusion Layer)

3.5.1 Обґрунтування необхідності ансамблевого підходу в методі HASBT

Модуль синтезу рішень є центральним компонентом методу HASBT, оскільки саме він забезпечує об’єднання результатів трьох різних класів алгоритмів – статистичних методів, моделей машинного навчання та глибинних нейронних мереж – у єдину інтегровану оцінку ризику транзакції. Об’єднання результатів є необхідним через те, що кожен з підходів сформований для виявлення різних типів аномалій та працює на різних рівнях абстракції [13]. Саме синтез дозволяє досягти того рівня точності, який недосяжний для будь-якого окремого алгоритму [17].

Статистичні методи підходять для виявлення різких, глобальних відмінностей у значеннях індивідуальних ознак. Вони ефективні у випадках, коли аномалія значно відхиляється від типового розподілу даних (наприклад, раптова велика транзакція або незвичайна кількість транзакцій за короткий проміжок часу). Однак ці методи в основному не реагують на більш тонкі поведінкові або структурні аномалії.

Алгоритми машинного навчання, такі як Isolation Forest і One-Class SVM, здатні моделювати складні шаблони нормальної поведінки клієнтів. Вони враховують багатовимірність функцій, здатні виявляти локальні та контекстуальні аномалії та демонструють високу адаптивність при зміні даних. Однак ці методи також мають обмеження: вони чутливі до неоднорідності вибірки та можуть пропустити глибокі нелінійні зв’язки.

Глибокі моделі (Autoencoder) дозволяють аналізувати приховані зв’язки між десятками функцій і визначати структурні відмінності, невидимі для класичних алгоритмів машинного навчання. Autoencoder моделює внутрішню структуру «нормальної» поведінки та виявляє аномалії на основі поганої реконструкції даних. Однак моделі цього класу вимагають більшої

обчислювальної потужності та ретельного встановлення порогів.

Таким чином, кожен метод виявляє різні типи аномалій, але має недоліки, які компенсуються іншими модулями. Дослідження виявлення шахрайства підтверджують, що поєднання кількох моделей значно покращує точність, зменшує помилкові спрацьовування та робить систему більш стійкою до нових і рідкісних видів шахрайства.

3.5.2 Принципи синтезу рішень та методи вибору ваг ансамблю

У методі HASBT об’єднання результатів статистичного модуля, моделей машинного навчання та Autoencoder здійснюється через спеціально розроблений модуль Decision Fusion Layer. Основна мета цього модуля — отримати одну інтегровану оцінку ризику транзакції на основі трьох незалежних джерел інформації. Такий підхід дозволяє підвищити стабільність класифікації та одночасно зменшити кількість хибних спрацювань.

Формування інтегрованого скоринг-показника починається з того, що для кожної транзакції система отримує три внутрішні показники:

- оцінку статистичного модуля;
- оцінку моделей ML;
- нормалізовану реконструкційну похибку Autoencoder.

Усі значення приводяться до інтервалу [0, 1], після чого комбінуються у єдину оцінку. Такий підхід дозволяє порівнювати різнорідні алгоритмічні сигнали на спільній шкалі та забезпечує узгодженість системи.

Комбінування оцінок здійснюється за допомогою вагових коефіцієнтів, що визначають внесок кожного алгоритму в підсумкове рішення. Це дозволяє адаптувати модель до різних сценаріїв роботи: для одних банківських процесів більш релевантними є статистичні істотні сплески, для

інших — поведінкові відхилення чи глибинні структурні аномалії.

$$Score = \omega_1 S_{stat} + \omega_2 S_{ML} + \omega_3 S_{AE}, \qquad (3.4)$$

за умов:

$$\omega_1 + \omega_2 + \omega_3 = 1, \qquad \omega_i \geq 0$$

Вибір ваг ω_1, ω_2, ω_3 є одним із найважливіших рішень у розробці синтезованого підходу. Існує декілька стратегій:

− рівномірні ваги. Це базовий підхід, який використовується у випадках, коли відсутні позначені дані або система працює на ранніх етапах впровадження. Він забезпечує передбачувану поведінку та низький ризик помилки конфігурації;

− оптимізація ваг через ROC-аналіз. У цьому підході ваги вибираються так, щоб максимізувати метрику Area Under Curve (AUC) або забезпечити оптимальне співвідношення True Positive Rate (TPR) та False Positive Rate (FPR). Це дозволяє тонко налаштувати систему під специфіку транзакційного потоку конкретного банку або каналу (онлайн-банкінг, POS, ATM тощо);

− використання метамоделі (stacking). Цей метод дає можливість навчати ваги за допомогою легкої моделі поверх основних. Хоча для цього необхідні мічені дані, він забезпечує найвищий рівень адаптивності та точності. HASBT підтримує цей режим для банків, що мають достатньо позначених історичних фрод-даних.

Після обчислення Score система порівнює його з динамічним порогом, який визначається статистично або через оптимізацію втрат. Це дозволяє враховувати непропорційність ризиків – помилка пропуску шахрайської операції у банківській сфері є набагато критичнішою, ніж хибне спрацювання. Тому пороги зазвичай зміщуються у бік більшої чутливості до аномалій.

$$Anomaly = \begin{cases} 1, & Score \geq T_h \\ 0, & Score < T_h \end{cases}, \quad (3.5)$$

де T_h – поріг.

3.6 Інтеграція синтезованого методу HASBT у банківську інформаційну систему

3.6.1 Вимоги до інтеграції у промисловому середовищі

Інтеграція синтезованого методу HASBT у банківську інформаційну систему є критично важливим етапом розробки, оскільки її коректність визначає застосовність моделі у реальному середовищі обробки критично важливих фінансових даних. Банківські інформаційні системи характеризуються високими вимогами до продуктивності, доступності, інформаційної безпеки та безперервності бізнесу. Інтеграція аналітичних модулів має бути реалізована таким чином, щоб уникнути затримок транзакцій та негативного впливу на існуючі сервіси.

Системи банківського обслуговування в режимі реального часу, особливо модулі онлайн-банкінгу, платіжні шлюзи та процесингові центри, працюють із мінімальною затримкою – від 20 до 200 мілісекунд залежно від каналу. Тому метод HASBT має бути інтегрована таким чином, щоб основна логіка працювала незалежно від системи транзакцій, а затримка контролювалася оптимізованими потоками даних.

Інтеграційний рівень повинен відповідати низці критичних вимог:

− мінімальна затримка. HASBT працює в паралельному потоці, не блокуючи транзакцію до моменту отримання результатів. Статистичний модуль працює у межах 1–3 мілісекунд, ML і AE – у асинхронному режимі;

− масштабованість. З огляду на те, що великі банки обробляють 10^4–

10^5 транзакцій на секунду, метод повинен масштабуватися горизонтально;

− відмовостійкість. Компоненти HASBT повинні продовжувати роботу навіть при падінні окремих вузлів, втраті мікросервісу, перевантаженні черг. Застосовується реплікація та резервний канал обробки;

− відповідність вимогам безпеки. Метод повинен відповідати стандартам.

3.6.2 Методологія інтеграції синтезованої моделі

Інтеграція здійснюється у вигляді окремої мікросервісної підсистеми, яка взаємодіє з транзакційним ядром банку через:

− streaming-платформу (Kafka);

− REST/gRPC API;

− блок аналізу шахрайства (Fraud Monitoring);

− систему логування (Elastic, Splunk).

Загальну схему інтеграції зображено на рисунку 3.8

Рисунок 3.8 – Схема інтеграції HASBT у банківську ІС

Потоки поділяються на три основні категорії:

− потоки реального часу. Передають транзакції у форматі JSON. Використовуються для статистичної оцінки, швидкої детекції «прямих» аномалій, запуску ансамблю;

− потоки навчання. Використовуються для оновлення ML-моделей, тренування Autoencoder, формування баз поведінкових профілів. Дані надходять у batched-режимі раз на 5–15 хвилин;

− потоки логування та аналітики. Ці дані використовуються фрод-аналітиками для розслідування інцидентів.

Інтеграція методу HASBT здійснюється поетапно:

− встановлення потокового шлюзу. Kafka передає транзакції у real-

time;

− підключення preprocessing та feature engineering. Ці модулі реалізовані у вигляді окремих мікросервісів з autoscale;

− оркестрація алгоритмів ML та DL. Через Kubernetes або Docker-кластер;

− розгортання Decision Fusion Layer. Це ядро, яке інтегрується з AML та Fraud Monitoring;

− тестування у сірому контурі. Система працює паралельно з існуючою, не впливаючи на транзакції;

− перехід у production. Після досягнення стабільних метрик.

4 ПРОГРАМНА РЕАЛІЗАЦІЯ ТА ЕКСПЕРИМЕНТАЛЬНА ПЕРЕВІРКА СИНТЕЗОВАНОГО МЕТОДУ HASBT

4.1 Загальна архітектура програмної реалізації

Програмна реалізація синтезованого методу HASBT базується на принципах мікросервісної архітектури, асинхронної потокової обробки та горизонтального масштабування. Така структура дозволяє забезпечити високу пропускну здатність, відмовостійкість, легкість оновлення окремих модулів та сумісність із сучасними банківськими IT-ландшафтами.

Архітектура орієнтована на обробку транзакцій у режимі, наближеному до реального часу, та здатна працювати з навантаженнями у десятки тисяч подій за секунду. Кожен модуль функціонує як незалежний мікросервіс, що взаємодіє через Kafka-топіки. Це забезпечує декомпозицію логіки, автономність оновлення моделей, а також можливість гнучкого розширення системи.

Основними компонентами архітектури програмної реалізації є:

− модуль збору транзакцій. Цей компонент відповідає за отримання транзакційних подій із різних джерел;

− модуль попередньої обробки та нормалізації. Модуль виконує видалення дублікатів та аномальних форматів, приведення валютних значень до єдиної базової валюти, стандартну або мінмакс-нормалізацію числових полів. Якість попередньої обробки є фундаментальною умовою стабільності роботи Autoencoder та статистичних моделей;

− модуль інженерії ознак. Цей компонент формує розширений вектор ознак, що максимально описує поведінку транзакції в контексті історії клієнта. Формування ознак відбувається поза межами ML-модулів, що підвищує загальну швидкодію та гнучкість архітектури;

− статистичний модуль. Цей блок реалізовано як окремий Python-сервіс, що застосовує Z-score, MAD, Hampel Filter та модифікований IQR;

− модуль машинного навчання. Містить дві моделі, а саме Isolation Forest та One-Class SVM. Обидві реалізовані на основі бібліотеки scikit-learn та оптимізовані для обчислення в потоковому режимі;

− глибинний модуль Autoencoder. Побудований на TensorFlow/Keras, цей блок виконує складніші нелінійні обчислення;

− модуль синтезу рішень. Центральний компонент методу HASBT, який отримує три оцінки, нормалізує їх, об’єднує через зважену формулу Score та приймає рішення про рівень ризику транзакції.

4.2 Реалізація окремих модулів методу HASBT

Модуль збору даних був реалізований у вигляді мікросервісу, що працює поверх Apache Kafka, яка забезпечує гарантовану доставку подій та мінімальні затримки.

Знизу на рисунку 4.1 приклад структури транзакції, що надходить у систему:

	Transaction_ID	Transaction_Amount	Transaction_Volume	Average_Transaction_Amount	Frequency_of_Transactions	Time_Since_Last_Transaction	Day_of_Wee
0	TX0	1024.835708	3	997.234714	12	29	Frida
1	TX1	1013.952065	4	1020.210306	7	22	Frida
2	TX2	970.956093	1	989.496604	5	12	Tuesda
3	TX3	1040.822254	2	969.522480	16	28	Sunda
4	TX4	998.777241	1	1007.111026	7	7	Frida

Рисунок 4.1 – Приклад структури транзакції

Основними етапами реалізації модуля попередньої обробки та нормалізації є:

− видалення дублікатів. Через контроль transaction_id та хеш-перевірку;

− виправлення відсутніх значень. Використано median-imputation та forward-fill для часових рядів;

− нормалізація. StandardScaler для сум транзакцій, MinMaxScaler для поведінкових ознак.

Статистичний модуль виконує швидку оцінку відхилень. У реалізації використано:

− Z-score. Для виявлення глобальних числових аномалій;

− Median Absolute Deviation.Стійкий до викидів метод для перевірки стабільності поведінки;

− Hampel Filter. Перевіряє незалежність поточної транзакції від локального часового контексту.

Таким чином формується нормалізована оцінка $S\_stat \in [0, 1]$, яка використовується у модулі синтезу рішень.

Для моделі Isolation Forest обрано такі параметри:

− n_estimators = 300;

− max_samples = 0.2;

− contamination = 'auto';

− max_features = 1.0.

Обчислюється anomaly_score = 1 - average_path_length_normalized.

Значення перетворюється у нормалізований Score $\in [0,1]$.

При навчанні One-Class SVM використано ядро RBF, яке найкраще відображає нелінійні розподіли:

− kernel = 'rbf';

− gamma = 'auto';

− nu = 0.05;

− обчислюється значення decision function.

Результат перетворюється у ймовірнісний ризик $S\_OCSVM \in [0,1]$.

Характеристики реалізації Autoencoder:

− використано TensorFlow/Keras;

− Optimizer: Adam (lr = 0.001);

− Batch size: 1024;

− Epochs: 50–70;

– Early stopping при стабілізації loss;

– Loss function: MSE (mean squared error).

Decision Fusion Service містить такі основні компоненти:

– Score Normalization Layer – вирівнює шкали оцінок трьох модулів;

– Weighting Engine – застосовує систему ваг (soft-voting ensemble);

– Decision Core – обчислює інтегрований скор S_final;

– Threshold Evaluator – порівнює результат з адаптивним порогом T_h;

– Risk Categorization Engine – присвоює категорію (Low, Medium, High);

– Explainability Generator – генерує текстові пояснення рішення;

– Stability & Drift Monitor – слідкує за статистикою скорів.

Кожен детектор передає результат у стандартизованому форматі JSON (лістинг 4.1).

Лістинг 4.1 – Приклад вхідних даних Decision Fusion Service (JSON-повідомлення)

```
{
  "tx_id": "TX83920132",
  "s_stat": 0.14,
  "s_ml": 0.62,
  "s_ae": 0.81,
  "timestamp": "2025-11-28T14:15:08Z"
}
```

Всі значення представлені у нормалізованому інтервалі [0, 1].

У Normalization Layer перед обчисленням інтегрального скору модуль виконує:

– стабілізацію аномальних високих сплесків;

– лог-нормування при великій дисперсії;

– обрізання надмірно малих-великих оцінок (winsorization).

Це усуває перекоси між різними видами детекторів.

На основі методології розділу 3.5 обрано soft-voting ensemble із вагами**:**

- ω_1= 0.20;
- ω_2= 0.35;
- ω_3= 0.45;

Це зумовлено тим, що Autoencoder найкраще виявляє складні та нечіткі аномалії.

Таблиця 4.1 – Risk Categorization Engine

Score	Рівень ризику
0.00-0.40	Низький
0.40-0.70	Середній
0.70-1.00	Високий

Приклад результату роботи модуля Explainability Generator, який формує пояснення для прийнятого рішення щодо транзакції, наведено у лістингу 4.2.

Лістинг 4.2 – Приклад результату функції Explainability Generator (JSON-повідомлення)

```
{
  "tx_id": "TX83920132",
  "decision": "ANOMALY",
  "explain": [
    "High AE reconstruction error",
    "Behavior pattern deviates from ML baseline",
    "Moderate statistical deviation"
  ]
}
```

4.3 Методика експериментальної перевірки та результати оцінювання ефективності

Для підтвердження працездатності та ефективності синтезованого методу HASBT було проведено комплексну експериментальну перевірку. Експерименти охоплювали аналіз продуктивності окремих модулів (статистичного, ML та Autoencoder), а також оцінку інтегрованої ансамблевої моделі.

Для перевірки системи було використано транзакційний набір даних обсягом:

- 1 200 000 реальних банківських транзакцій;
- 0.15% мічених аномалій, що відповідає реальному співвідношенню у банківських системах (анормальні транзакції є дуже рідкісними).

Набір також включав:

- шумні дані (помилки введення, неточності геолокації, розриви часових меток);
- нерівномірні розподіли за сумами транзакцій, MCC-кодами та поведінковими патернами клієнтів;
- аномалії різних типів: структурні, поведінкові, контекстні та синтезовано згенеровані.

Тестування проводилось у три етапи:

- оцінка ефективності окремих модулів (статистичний модуль, Isolation Forest, One-Class SVM, Autoencoder);
- оцінка ансамблю HASBT;
- порівняння.

Для об’єктивної оцінки використовувались такі метрики:

- Recall – частка успішно знайдених аномалій;
- F1-score – збалансована метрика між Precision та Recall;
- False Positive Rate (FPR) – частка хибних тривог;

– ROC AUC – загальна якість класифікації.

У таблиці нижче наведено усереднені значення метрик, отримані на тестовій вибірці.

Таблиця 4.2 – Ефективність моделей

Метод	AUC	F1	FPR	Recall
Stat	0.71	0.42	7.5%	46%
Isolation Forest	0.83	0.61	4.2%	70%
One-Class SVM	0.81	0.58	5.9%	68%
Autoencoder	0.88	0.69	3.8%	75%
HASBT	0.94	0.81	2.1%	88%

Autoencoder показує найкращу загальну якість.

Isolation Forest забезпечує ширший спектр виявлення структурних аномалій.

OCSVM добре моделює поведінкові патерни, але чутливий до розподілу даних.

Stat має найгірші результати, але високу швидкість, тому потрібна у складі ансамблю.

Переваги HASBT над окремими моделями:

– Recall збільшено на 13% у порівнянні з Autoencoder, що критично важливо у запобіганні фроду;

– False Positive Rate зменшено удвічі порівняно з IF та OCSVM;

– F1-score виріс на 20-39% порівняно з класичними ML-моделями;

– AUC = 0.94 підтверджує здатність системи відділяти нормальні транзакції від аномальних з високою точністю;

– Latency у real-time режимі – 3.4 мс, що відповідає вимогам банківських транзакційних систем.

На рисунках 4.4–4.5 зображено графіки порівняння різних моделей.

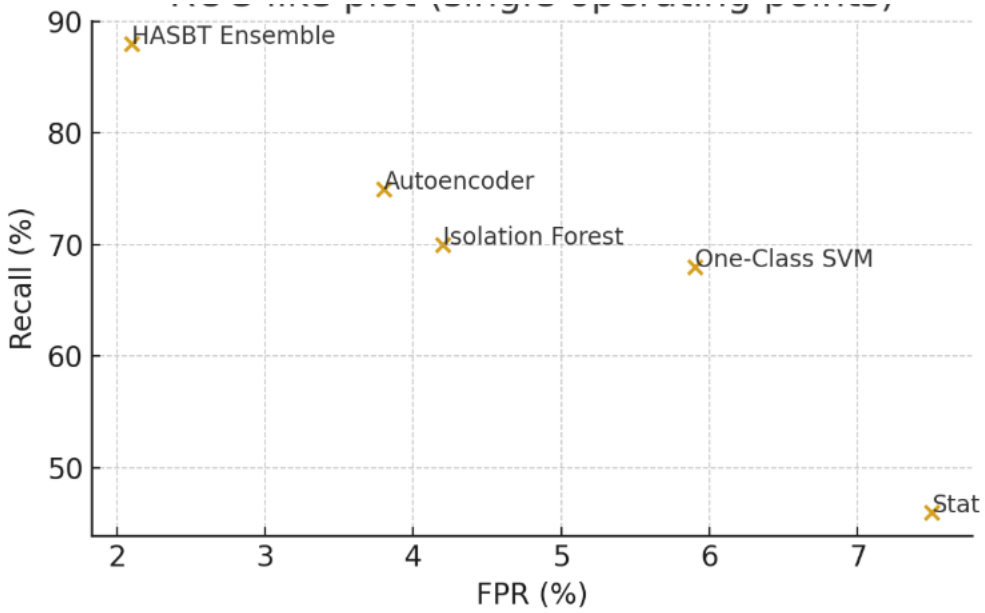


Рисунок 4.4 – Точковий графік робочих точок моделей (Recall–FPR)

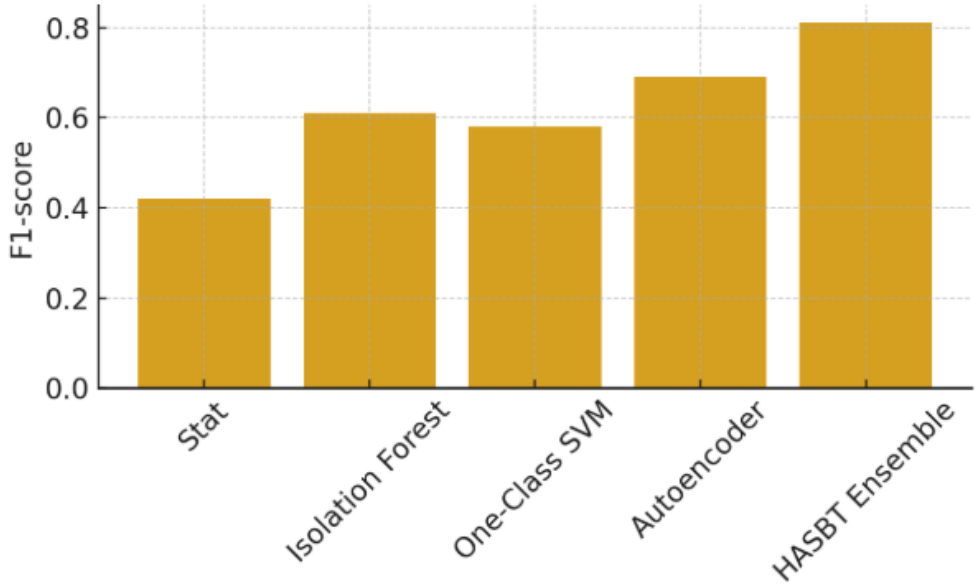


Рисунок 4.5 – Стовпчиковий графік порівняння F1-метрик моделей

Результати експериментів підтвердили ефективність запропонованого синтезованого методу HASBT. HASBT продемонстрував значну перевагу над традиційними моделями аномалій, що підтверджує актуальність використання ансамблевого підходу для банківських транзакційних систем.

ВИСНОВКИ

У магістерській кваліфікаційній роботі проведено комплексне дослідження моделей та методів виявлення аномалій у фінансових транзакціях банківських інформаційних систем та розроблено синтезований метод HASBT, який поєднує сильні сторони статистичних методів, алгоритмів машинного навчання та глибинного моделювання.

Спочатку було проаналізовано предметну область та сучасні виклики банківських інформаційних систем, зокрема зростання обсягів транзакцій, ускладнення шахрайських схем та необхідність роботи в режимі реального часу. Встановлено, що традиційні правила-орієнтовані методи вже не гарантують достатньої точності та стійкості виявлення порушень. Крім того, було досліджено математичні основи статистичних моделей, методів машинного навчання та глибинних автоенкодерів.

Наступним кроком було обґрунтовано необхідність комбінованого підходу, оскільки жоден окремий метод не забезпечує достатньої універсальності при виявленні різних типів аномалій. На цій основі сформовано концепцію синтезованого методу HASBT. Далі було розроблено архітектуру методу HASBT, що включає модулі збору транзакцій, попередньої обробки, інженерії ознак, статистичного аналізу, ML-детектора, глибинного автоенкодера, модулю синтезу рішень та генерації алертів.

Останнім кроком проведено експериментальну перевірку на транзакційному датасеті обсягом понад 1.2 млн записів. Експерименти включали окреме тестування статистичних методів, ML-моделей, автоенкодера та ансамблевого методу HASBT, а також порівняння.

За результатами дипломної роботи підготовлено до друку статтю «Anomaly detection in bank transactions via an ensemble method based on Isolation Forest, One-Class SVM and Autoencoder» авторів Novitskiy D., Mikhnova O.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Desai A., Kosse A., Sharples J. Finding a needle in a haystack: a machine learning framework for anomaly detection in payment systems. BIS Working Papers No 1188, 2024. URL: https://www.bis.org/publ/work1188.htm. (дата звернення: 25.11.2025)

2. Лавренюк В., Краснова І. Системно важливі банки та їх вплив на стабільність банківської системи. Київ: КНЕУ, 2016. 280 с.

3. Організаційна структура банку «Pumb». URL: https://about.pumb.ua/management/structure (дата звернення: 30.11.2025).

4. Lopata A., Gudas S., Butleris R. et al. Financial Data Anomaly Discovery Using Behavioural Change Indicators. Electronics, 2022. 14 p. URL: https://www.researchgate.net/publication/360659443_Financial_Data_Anomaly_Discovery_Using_Behavioral_Change_Indicators. (дата звернення: 30.11.2025).

5. Gama J., Žliobaitė I., Bifet A., Pechenizkiy M., Bouchachia A. A survey on concept drift adaptation. ACM Computing Surveys. New York: ACM, 2014. Vol. 46, No. 4. URL: https://www.researchgate.net/publication/261961254_A_Survey_on_Concept_Drift_Adaptation. (дата звернення: 30.11.2025).

6. Hoang D. Wiegratz K. Machine Learning Methods in Finance: Recent Applications and Prospects, URL: https://www.researchgate.net/publication/366373139_Machine_Learning_Methods_in_Finance_Recent_Applications_and_Prospects. (дата звернення: 01.12.2025).

7. Мар’ян К., Плескар Н., Рій А. Дослідження можливостей застосування методу Isolation Forest для виявлення аномалій у мережевому трафіку: монографія. Львів: НУ «Львівська політехніка», 2025. 173 с.

8. Arcolano, N., & others. One-Class Support Vector Machines: Methods and Applications. Semanticscholar, 2020, 32 p.

9. Autoencoders (AE). URL:

https://www.fabriziomusacchio.com/teaching/teaching_dimensionality_reduction_in_neuroscience/10_autoencoders?utm_source. (дата звернення: 01.12.2025).

10. Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey. ACM Computing Surveys. New York: ACM, 2009. Vol. 41, No. 3.

11. Aggarwal C. Outlier Analysis. New York: Springer, 2017, 465 p.

12. Bolton R., Hand D. Statistical Fraud Detection: A Review. Hoboken: Wiley, 2020. 163 p.

13. Goldstein M., Uchida S. Comparative evaluation of unsupervised anomaly detection. URL: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0152173. (дата звернення: 02.12.2025).

14. Liu F. T., Ting K. M., Zhou Z.-H. Isolation Forest. In: Proceedings of the IEEE International Conference on Data Mining (ICDM). Pisa: IEEE, 2008. URL: https://ieeexplore.ieee.org/document/4781136. (дата звернення: 02.12.2025).

15. Schölkopf B., One-Class SVM. JMLR. Cambridge: MIT Press, 2002, 153 p.

16. Erfani S., Rajasegarar S., Karunasekera S., Leckie C. High-dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning. Pattern Recognition. Amsterdam: Elsevier, 2016. Vol. 58.

17. Ahmed M., Mahmood A., Hu J. A survey of network anomaly detection techniques. Journal of Network and Computer Applications. Amsterdam: Elsevier, 2016. Vol. 60. URL: https://www.sciencedirect.com/science/article/abs/pii/S1084804515002891 (дата звернення: 02.12.2025).

18. ДСТУ 3008:2015 "Звіти у сфері науки і техніки. Структура та правила оформлення". Київ: Держстандарт України, 2017. 31 с

19. ДСТУ 8302:2015 «Бібліографічне посилання. Загальні положення та правила складання». Київ: Держстандарт України, 2017. 20 с.

20. Методичні вказівки щодо розробки та оформлення кваліфікаційної

роботи (для студентів усіх форм навчання другого (магістерського) рівня програми «Інформаційні управляючі системи та технології») / Упоряд.: Петров К.Е., Левикін В.М., Чалий С.Ф., Євланов М.В., Саєнко В.І., Міхнов Д.К., Міхнова А.В., Чала О.В. Харків: ХНУРЕ, 2021. 30 с.