**Міністерство освіти і науки України**
**Київський національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

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

# ПОЯСНЮВАЛЬНА ЗАПИСКА

## кваліфікаційної роботи

**галузь знань** 12 Інформаційні технології
(шифр і назва галузі знань)

**спеціальність** 125 Кібербезпека
(код і назва спеціальності)

**освітній ступень** бакалавр

**освітня програма** Кібербезпека
(назва освітньо-професійної програми)

**на тему:** «Програмний модуль для оцінки ризиків транзакцій при монетизації мобільних ігор»

**Виконавець:** студентка IV курсу, групи КБ-43

_____ **Юлія ПАСЬКО**
(підпис) (ім'я, прізвище)

| | **Підпис** | **Ім'я, прізвище** |
|---|---|---|
| **Керівник** | | Інна МИХАЛЬЧУК |
| **Нормоконтроль** | | Юрій ЩЕБЛАНІН |

**Київ 2025**

**Міністерство освіти і науки України**
**Київський національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

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

# ЗАВДАННЯ
## на виконання кваліфікаційної роботи

**спеціальності** 125 Кібербезпека
(код і назва спеціальності)

**освітньої програми** Кібербезпека
(назва освітньо-професійної програми)

**Студентці** **КБ-43** **Пасько Юлії Романівні**
(група) (прізвище ім'я по батькові)

**Тема кваліфікаційної роботи** Програмний модуль для оцінки ризиків транзакцій при монетизації мобільних ігор

### 1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

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

### 2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Сучасні методи захисту транзакцій у мобільних іграх

### 3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Ознайомлення із сучасними методами монетизації, реалізацією методів захисту транзакцій, вразливостями з боку безпеки даних та їх типовими технологіями захисту, розроблення програмного модуля для оцінки ризиків при платежах у мобільних іграх

### 4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

**Практична цінність** Розроблений програмний модуль дозволяє

автоматизовано оцінювати ризики транзакцій у мобільних іграх, що сприяє зниженню фінансових втрат і підвищенню безпеки.

**5. ДАТА ВИДАЧІ ЗАВДАННЯ**

Дата видачі завдання: 29 листопада 2024 року

Завдання видала _____ (підпис) Інна МИХАЛЬЧУК (ім'я, прізвище)

Завдання прийняла до виконання _____ (підпис) Юлія ПАСЬКО (ім'я, прізвище)

**КАЛЕНДАРНИЙ ПЛАН**

| № п/п | Найменування етапів робіт | Строки виконання робіт (початок-кінець) | Відмітка про виконання |
|---|---|---|---|
| 1 | Уточнення постановки задачі | 29.11.2024-06.12.2024 | *виконано* |
| 2 | Аналіз літератури | 09.12.2024-27.12.2024 | *виконано* |
| 3 | Обґрунтування вибору методів дослідження | 30.12.2024-10.01.2025 | *виконано* |
| 4 | Дослідження методів монетизації мобільних ігор | 13.01.2025 – 31.01.2025 | *виконано* |
| 5 | Аналіз вразливостей та технологій захисту транзакцій | 03.02.2025 – 03.03.2025 | *виконано* |
| 6 | Розробка програмного модуля для оцінки ризиків транзакцій у мобільних іграх | 05.03.2025-28.04.2025 | *виконано* |
| 7 | Тестування модуля на змодельованих даних | 29.04.2025-16.05.2025 | *виконано* |
| 8 | Оформлення пояснювальної записки | 19.05.2025-23.05.2025 | *виконано* |
| 9 | Підготовка до захисту кваліфікаційної роботи | 26.05.2025-03.06.2025 | *виконано* |

Завдання видала _____ (підпис) Інна МИХАЛЬЧУК (ім'я, прізвище)

Завдання прийняла до виконання _____ (підпис) Юлія ПАСЬКО (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 13 червня 2025 року

# РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків, має 65 сторінки основного тексту та 3 таблиці, 4 рисунків. Список використаних джерел містить 60 найменувань і займає 5 сторінки.

*Метою роботи* є розробка програмного модуля для автоматизації оцінки ризиків транзакцій у процесі монетизації мобільних ігор з метою зменшення фінансових втрат і підвищення безпеки.

*Об'єктом дослідження* є процес формування віртуального ігрового активу з використанням транзакцій в системах монетизації мобільних ігор.

*Предметом дослідження* є методи аналізу та моделювання ризиків транзакцій у мобільних іграх, а також алгоритми їх автоматизованої оцінки.

*Методи дослідження* кваліфікаційної роботи:

- аналіз транзакційних даних та поведінкових моделей користувачів;
- статистичний аналіз та методи машинного навчання для виявлення аномалій;
- тестування ефективності програмного модуля на змодельованих даних;
- валідація результатів за допомогою тестування.

*Практичною цінністю* є розроблений програмний модуль, який дозволяє автоматизовано оцінювати ризики транзакцій у мобільних іграх, що сприяє зниженню фінансових витрат і підвищенню безпеки монетизації. Модуль забезпечує своєчасне виявлення аномалій і шахрайських дій, знижує навантаження на фахівців з ризик-менеджменту, підвищує довіру користувачів та може бути адаптований до різних ігрових платформ.

*Ключові слова:* мобільні ігри, монетизація, транзакції, IAP, шахрайство, статистичний аналіз, машинне навчання, автоматизація оцінки ризиків

# ЗМІСТ

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

| | | |
|---|---|---|
| IAP | - | In-App Purchases |
| SDK | - | Software Development Kit |
| PCI DSS | - | Payment Card Industry Data Security Standard |
| PSD2 | - | Payment Services Directive 2 |
| 2FA | - | Two-Factor Authentication |
| LTV | - | Lifetime Value |
| GDPR | - | General Data Protection Regulation |
| COPPA | - | Children's Online Privacy Protection Act |
| AI | - | Artificial Intelligence |
| BAT | - | Basic Attention Token |
| TPS | - | Transactions Per Second |
| CHD | - | Cardholder Data |
| CDE | - | Common Data Environment |
| TRAS | - | Transaction Risk Assessment Systems |
| ML | - | Machine Learning |
| TRAM | - | Transaction Risk Assessment Model |

# ВСТУП

Стрімке зростання популярності мобільних ігор перетворило їх на ключовий елемент сучасної цифрової економіки. Внутрішньоігрові покупки, підписки та рекламні моделі стали основним джерелом прибутку для розробників, забезпечуючи значну частку доходів у цій галузі. Однак із збільшенням обсягів фінансових операцій посилюються й ризики, пов’язані з безпекою транзакцій.

Тож захист платіжних процесів у мобільних іграх є критично важливим для підтримки довіри мільйонів гравців та стабільності ігрових екосистем. Безпека транзакцій безпосередньо впливає на репутацію проектів: будь-які порушення, такі як витоки персональних даних або несанкціонований доступ до платіжних систем, можуть призвести до серйозних наслідків. Індустрія стикається з численними викликами, серед яких — технічні вразливості в платіжних механізмах, шахрайські схеми та маніпуляції з віртуальною валютою. Ці проблеми потребують комплексних рішень, спрямованих на запобігання атакам, захист конфіденційності даних та дотримання міжнародних стандартів безпеки. Впровадження надійних механізмів автентифікації, шифрування транзакцій та моніторингу підозрілої активності стає невід’ємною частиною розробки сучасних ігор.

Таким чином, актуальність дослідження полягає в необхідності створення таких рішень, які поєднують ефективність, адаптивність і зручність. Лише комплексний підхід до захисту транзакцій дозволить зберегти стабільність ігрової економіки, забезпечити справедливі умови для гравців і підтримати конкурентоспроможність проектів у умовах постійної еволюції кіберризиків.

*Метою роботи* є розробка програмного модуля для автоматизації оцінки ризиків транзакцій у процесі монетизації мобільних ігор з метою зменшення фінансових втрат і підвищення безпеки.

*Для досягнення зазначеної мети кваліфікаційної роботи поставлено наступні задачі:*

1. Проаналізувати чинні методи монетизації у мобільних іграх.
2. Проаналізувати особливості транзакцій у системах монетизації мобільних ігор та типові ризики, пов’язані з ними.
3. Дослідити поведінкові моделі користувачів, що можуть свідчити про підвищений ризик транзакцій.
4. Розробити алгоритми автоматизованої оцінки ризику транзакцій з урахуванням виявлених факторів ризику.
5. Реалізувати програмний модуль для оцінки ризиків транзакцій у середовищі мобільної гри.
6. Провести тестування модуля на змодельованих даних для оцінки його ефективності.

*Об’єктом дослідження* є процес формування віртуального ігрового активу з використанням транзакцій в системах монетизації мобільних ігор.

*Предметом дослідження* є методи аналізу та моделювання ризиків транзакцій у мобільних іграх, а також алгоритми їх автоматизованої оцінки.

*Методи дослідження кваліфікаційної роботи:*

- аналіз транзакційних даних та поведінкових моделей користувачів;
- статистичний аналіз та методи машинного навчання для виявлення аномалій;
- тестування ефективності програмного модуля на реальних або змодельованих даних;
- валідація результатів за допомогою тестування.

*Практичною цінністю* є розроблений програмний модуль, який дозволяє автоматизовано оцінювати ризики транзакцій у мобільних іграх, що сприяє зниженню фінансових витрат і підвищенню безпеки монетизації. Модуль забезпечує своєчасне виявлення аномалій і шахрайських дій, знижує навантаження на фахівців з ризик-менеджменту, підвищує довіру користувачів та може бути адаптований до різних ігрових платформ.

# РОЗДІЛ 1
# ОГЛЯД СУЧАСНИХ МЕТОДІВ МОНЕТИЗАЦІЇ У МОБІЛЬНИХ ІГРАХ

## 1.1 In-App Purchases (IAP): основи, типи та ефективність

In-App Purchases (IAP) є одним із найпоширеніших методів монетизації мобільних ігор, що передбачає продаж цифрових товарів або послуг безпосередньо в додатку. Згідно з дослідженням Sensor Tower у 2023, дохід від IAP у 2022 році склав $120 млрд, що становить понад 70% загального прибутку мобільного геймінгу [1].

IAP є технологічно складною системою, яка базується на інтеграції платіжних шлюзів (наприклад, Google Play Billing, Apple App Store Connect) та API для керування транзакціями. Захист даних користувачів забезпечується через токенізацію платежів, де конфіденційна інформація (наприклад, дані картки) замінюється унікальними токенами, що знижує ризик витоку. Згідно з документацією Google, 85% успішних транзакцій у мобільних іграх використовують SDK (Software Development Kit) для автоматизації процесів, таких як перевірка квитанцій або відновлення покупок [2].

Внутрішньоігрові покупки поділяються на дві основні категорії, які визначають їх функціональність та вплив на ігровий досвід. Споживчі товари (consumable) — це цифрові продукти, які використовуються одноразово або обмежено. До них належать віртуальна валюта, бонуси для прискорення прогресу або тимчасові підсилення. Такі товари "витрачаються" під час гри, що стимулює гравців до повторних покупок для підтримки ігрової активності. Яскравим прикладом успішного використання є гра Candy Crush Saga від King, де гравці купують додаткові життя або бонуси для проходження складних рівнів. За даними App Annie, ця гра генерує понад $1 млрд щорічно саме завдяки мікроплатежам [3].

Неспоживчі товари (non-consumable) — це постійні активи, які залишаються в розпорядженні гравця назавжди. Ця категорія включає розблокування рівнів, преміум-доступ до ексклюзивного контенту або косметичні елементи (скіни персонажів, оформлення інтерфейсу). Наприклад, у Fortnite гравці купують унікальні скіни для персонажів, які не впливають на баланс гри, але підвищують естетичну цінність. Такі покупки формують довгострокову лояльність, оскільки забезпечують постійне володіння контентом.

Важливість цих категорій полягає в їхньому симбіозі. Споживчі товари забезпечують стабільний потік мікроплатежів, особливо в іграх із циклічним геймплеєм, тоді як неспоживчі — створюють емоційний зв’язок із грою через персоналізацію. Розробники часто комбінують обидві категорії для максимізації доходу. Наприклад, у Roblox гравці купують Robux (споживча валюта) для придбання аксесуарів (неспоживчі товари).

Проте надмірний акцент на споживчих товарах, особливо в механіках типу "pay-to-win", може спричинити незадоволення аудиторії, як це сталося у Star Wars Battlefront II. Скандал навколо гри  став ключовим прикладом того, як надмірна агресивність у монетизації може спричинити масштабну втрату довіри гравців. Основна проблема полягала в інтеграції механіки loot boxes, які містили критично важливі ігрові елементи — потужних персонажів (наприклад, Дарта Вейдера), зброю та модифікатори. Для їх отримання гравцям пропонувалося або витрачати десятки годин на "гриндинг" (рутинне виконання завдань), або купувати loot boxes за реальні гроші. Це створило систему "pay-to-win", де платні користувачі отримували вирішальну перевагу, порушуючи баланс гри.

Реакція спільноти була негайною та різкою. Гравці масово критикували EA (розробника) у соціальних мережах, а пост на Reddit із засудженням системи монетизації став найбільш "дизлайканим" в історії платформи. Частина аудиторії взагалі відмовилася купувати гру, що призвело до падіння продажів. ЗМІ, включаючи BBC та Forbes, назвали ситуацію "грабіжницькою", підкреслюючи, що loot boxes експлуатують психологічні механізми залежності, особливо серед неповнолітніх [4], [5].

Це спровокувало втручання регуляторів. У Бельгії та Нідерландах loot boxes у Star Wars Battlefront II визнали формою азартних ігор, що вимагало від EA або видалити їх, або отримати ліцензію. У відповідь компанія тимчасово вимкнула покупку loot boxes за реальні гроші ще до офіційного релізу, а згодом повністю переробила систему прогресу. Ключові персонажі стали доступні через ігрову валюту, яку неможливо було купити за гроші, що зменшило вплив "pay-to-win".

Цей випадок став поворотним для індустрії. Розробники почали уникати явних "pay-to-win" механік, зосередившись на косметичних предметах (наприклад, Fortnite). У 2020 році EA додала функцію прозорості ймовірностей у loot boxes, що стало відповіддю на регуляторний тиск. Крім того, зросли вимоги до етичної монетизації: Google Play та App Store тепер вимагають розкривати шанси випадіння предметів у loot boxes. На думку дослідника Л. Вонга, подібні регуляції змушують індустрію шукати альтернативи, як-от фіксовані магазини (наприклад, у Fortnite) [6]. На мою думку, технічна адаптація до регуляторних норм стає ключовим викликом для розробників, особливо в ЄС.

Новим етапом IAP стала інтеграція блокчейн-технологій, які трансформують традиційні моделі володіння та обміну цифровими активами. Яскравим прикладом є гра Axie Infinity, де ігрові предмети (наприклад, унікальні істоти-акси) представлені у вигляді NFT (невзаємозамінних токенів) на блокчейні Ronin. Кожна транзакція фіксується в смарт-контрактах, що забезпечує прозорість та довіру. Гравці можуть freely торгувати активами на ринках, а їхня власність гарантується технологією. Проте ця модель вимагає від користувачів керування криптогаманцями (наприклад, MetaMask), що ускладнює масове впровадження через технічну складність для новачків.

Різниця в підходах до інтеграції блокчейну яскраво виявляється при аналізі двох проектів — Axie Infinity та The Sandbox. Axie Infinity базується на приватному блокчейні Ronin, спеціально розробленому для швидких та економічних транзакцій (до 100 операцій за секунду). Ця оптимізація дозволила

грі досягти річного обороту в $4.5 млрд, що робить її ідеальним рішенням для мільйонної аудиторії, яка потребує масштабованості та стабільності [7].

На противагу, The Sandbox використовує Ethereum — більш децентралізовану, але менш ефективну платформу. Обмежена пропускна здатність Ethereum (15 транзакцій за секунду) та високі комісії (gas fees) обмежують річний оборот проекту до $1.2 млрд. Проте Ethereum залишається ключовим інструментом для креативних спільнот завдяки своїй універсальності та відкритості. На цій платформі розробники та художники створюють унікальні віртуальні світи, де кожен актив може бути легко інтегрований у ширшу екосистему Web3.

Незважаючи на перспективи, блокчейн-технології стикаються з низкою перешкод. По-перше, технічні бар'єри: необхідність керування криптогаманцями та розуміння механізмів NFT обмежують аудиторію переважно досвідченими користувачами. По-друге, волатильність ринку: вартість цифрових активів залежить від коливань цін на криптовалюти, що створює фінансові ризики для гравців. По-третє, регуляторна невизначеність: країни, такі як Китай або Індія, обмежують або забороняють використання NFT через відсутність чіткого законодавства, що ускладнює глобальне впровадження.

Безпека транзакцій у системах внутрішньоігрових покупок тісно пов'язана з дотриманням стандарту PCI DSS (Payment Card Industry Data Security Standard), який регулює захист даних платіжних карток. Цей стандарт є фундаментальним елементом захисту транзакцій у сфері мобільних ігор. Розроблений провідними платіжними системами, він встановлює суворі вимоги до обробки даних карток, спрямовані на мінімізацію ризиків витоку інформації. Для розробників ігор дотримання PCI DSS — це не лише юридична зобов'язаність, але й ключовий інструмент збереження довіри мільйонів гравців, які щодня здійснюють мікроплатежі.

Основним принципом PCI DSS є шифрування даних під час передачі та зберігання. Наприклад, використання протоколу TLS 1.3+ для захисту онлайн-транзакцій або алгоритму AES-256 для шифрування баз даних. Крім того,

стандарт вимагає обмеження доступу до конфіденційної інформації лише авторизованим співробітникам та проведення регулярних аудитів для виявлення вразливостей. Важливу роль відіграє токенізація — заміна реальних даних карток на унікальні токени, які неможливо використати для шахрайства. Цей підхід успішно реалізовано в таких іграх, як Fortnite (через інтеграцію з Stripe) та Roblox (для захисту операцій з віртуальною валютою Robux).

Порушення вимог PCI DSS має серйозні наслідки. Фінансові штрафи можуть сягати мільйонів доларів, особливо якщо витоки даних порушують норми GDPR у ЄС. Кібератаки на ігри без належного шифрування часто призводять до фішингу або перехоплення платіжних даних, що руйнує репутацію розробників і провокує відтік гравців. Згідно з дослідженням Verizon, близько 30% мобільних ігор ігнорують PCI DSS, що робить їх легкими цілями для зловмисників [8].

Таким чином, PCI DSS залишається основним каркасом для захисту внутрішньоігрових покупок. Його дотримання вимагає технічної готовності (впровадження шифрування, токенізації) та організаційної культури (аудити, контроль доступів). Інтеграція сучасних технологій має доповнювати, а не заміняти ці стандарти. Тільки такий підхід забезпечить створення надійних систем, здатних протистояти сучасним кіберзагрозам і підтримувати довіру гравців у цифрову епоху.

### 1.2 Підписки: смарт-контракти, безпека даних та глобальні регуляції

Модель підписок набуває все більшої популярності в мобільному геймінгу як ефективний спосіб забезпечення передбачуваного та стабільного доходу. Згідно зі звітом Data.ai, кількість ігор, які впровадили підписки, зросла на 40% у період 2022–2023 років [9]. Ця модель передбачає регулярні платежі (щомісячні або щорічні), за які гравці отримують ексклюзивні переваги: відсутність реклами, ранній доступ до оновлень, бонусні ресурси або віртуальну валюту. Такі пропозиції створюють додаткову цінність для користувачів, заохочуючи їх

до довгострокової участі в грі, водночас забезпечуючи розробникам постійний потік коштів.

Яскравим прикладом успішної реалізації цієї моделі є Roblox Premium. Підписка вартістю від 4.99 до 19.99 на місяць надає гравцям віртуальну валюту Robux, доступ до преміум-серверів та ексклюзивні предмети. За даними Roblox Corporation, дохід від підписок становить 30% загального прибутку платформи, що підкреслює її економічну значимість. Ключовим фактором успіху є постійне оновлення контенту: нові ігрові режими, сезонні заходи та унікальні нагороди, які підтримують інтерес аудиторії [10].

На думку експерта з монетизації Е. Шелла, ефективність підписок залежить від здатності розробників підтримувати актуальність та різноманітність контенту. Без регулярних оновлень навіть найпривабливіші пропозиції втрачають цінність, що призводить до відтоку гравців. Наприклад, ігри, які періодично додають нові завдання, косметичні елементи або соціальні функції, демонструють вищий рівень утримання користувачів порівняно з проектами, де контент застоюється [11].

Сучасні системи підписок у мобільних іграх базуються на автоматизації рекурентних платежів за допомогою спеціалізованих платформ, таких як RevenueCat або Apple Subscriptions. Ці інструменти не лише спрощують процес списання коштів, але й надають розробникам глибоку аналітику щодо активності гравців, тривалості підписок та конверсії. Згідно з дослідженням Data.ai, близько 60% підписок активуються через промокоди або безкоштовні trial-періоди, що робить такі механіки ключовими для залучення нових користувачів. Наприклад, тимчасовий доступ до преміум-контенту безкоштовно дозволяє гравцям оцінити переваги перед оплатою, збільшуючи ймовірність продовження підписки [9].

Яскравим прикладом ефективного використання підписок у мобільних іграх є Clash Royale від компанії Supercell. У 2019 році гра запустила підписку "Pass Royale" вартістю $4.99 на місяць, яка надає гравцям ексклюзивні нагороди, прискорений прогрес та повну відсутність реклами. Ця модель не лише покращила ігровий досвід, але й забезпечила значний економічний ефект.

Технічна реалізація передбачала інтеграцію з Google Play Billing Library — інструментом для керування підписками на платформі Android. Це дозволило забезпечити стабільність транзакцій, автоматизацію списань коштів та дотримання політик Google щодо платіжних систем. Для визначення оптимальної цінової стратегії розробники провели A/B тестування, порівнюючи варіанти з 4.99 та 6.99. Результати показали, що нижча ціна ($4.99) виявилася більш прийнятною для аудиторії, що сприяло зростанню конверсії та збереженню лояльності гравців.

Важливим елементом став механізм "Instant Rewards", де гравці отримують бонуси (наприклад, віртуальну валюту або ексклюзивні скіни) відразу після оплати. Це створило відчуття миттєвої винагороди, підвищивши задоволеність користувачів. За даними Supercell, після впровадження підписки річний дохід гри зріс на 25%, а показник утримання гравців — на 40% [12].

У Європейському Союзі директива PSD2 (Payment Services Directive 2) значно посилила вимоги до безпеки рекурентних платежів, зокрема в мобільних іграх. Згідно з цими правилами, кожен рекурентний платіж (наприклад, щомісячна підписка) має підтверджуватися двофакторною аутентифікацією (2FA). Це означає, що гравці повинні явно підтверджувати свою згоду на списання коштів через SMS, електронний підпис або інші механізми. За даними дослідження, проведеного юристом К. Мюллером, такі зміни зменшили кількість випадкових або несвідомих покупок на 30%, оскільки користувачі стали більш уважними до процесу оплати [13].

Окремим викликом для розробників стали оновлені правила Apple, які з 2022 року зобов’язують додавати кнопку "Скасувати підписку" безпосередньо в інтерфейсі додатку. Раніше користувачам доводилося переходити в налаштування облікового запису iOS, що ускладнювало процес відписки. Тепер гравці можуть миттєво скасувати підписку, що знизило рівень "пасивного утримання" — ситуацій, коли користувачі продовжують оплачувати послугу через технічні або психологічні бар’єри.

Ці регуляторні зміни, на думку експертів, стимулюють індустрію до пошуку інноваційних моделей монетизації. Наприклад, гра Brawl Stars (Supercell) успішно поєднує підписки з внутрішньоігровими покупками (IAP). Підписка надає базові переваги (ексклюзивні скіни, щоденні нагороди), тоді як IAP дозволяють придбати додаткові предмети або прискорити прогрес. Такий гібридний підхід не лише зменшує залежність від рекурентних платежів, але й підвищує гнучкість для гравців, що позитивно впливає на їхню лояльність.

Таким чином, регуляторний тиск стає каталізатором для еволюції монетизаційних стратегій. З одного боку, вимоги до прозорості та контролю з боку користувачів змушують розробників уникати агресивних практик. З іншого — вони відкривають нові можливості для креативних рішень, які поєднують стабільність підписок із гнучкістю мікроплатежів. Це формує новий стандарт індустрії, де баланс між прибутковістю та довірою гравців стає ключовим фактором успіху.

Для забезпечення безпеки та доступності ігрового прогресу розробники мобільних ігор активно використовують хмарні збереження, такі як Google Play Games Services або iCloud. Ці системи автоматично синхронізують дані гравця (рівні, предмети, налаштування) між пристроями, дозволяючи продовжити гру з будь-якого місця. Наприклад, користувач може почати гру на смартфоні, а потім перейти на планшет без втрати прогресу. Однак ця зручність супроводжується технічними та логістичними викликами, особливо коли гравець використовує кілька акаунтів.

Основна проблема полягає в конфліктах синхронізації. Якщо користувач має два або більше акаунтів (наприклад, особистий і спільний з родиною), дані з різних облікових записів можуть перезаписувати або змішуватися. Наприклад, прогрес, збережений у хмарі для одного акаунта, може випадково замінити дані іншого, особливо якщо пристрої не розрізняють користувачів. Це призводить до втрати досягнень, предметів або навіть повного скидання гри. Додатковий ризик виникає, коли гравці свідмо використовують кілька акаунтів для обходу

обмежень (наприклад, отримання бонусів для новачків), що може порушити баланс ігрової економіки.

Для мінімізації цих проблем розробники впроваджують механізми ідентифікації та верифікації. Наприклад, система може вимагати прив’язки акаунта до електронної пошти або соціальних мереж, що запобігає випадковому створенню дублікатів. Деякі ігри, такі як Clash of Clans, автоматично блокують синхронізацію між різними акаунтами на одному пристрої, вимагаючи явного переключення профілів. Крім того, розробники надають гравцям інструкції щодо керування акаунтами та попереджають про ризики використання кількох облікових записів.

Проте повністю усунути конфлікти синхронізації неможливо, особливо в умовах обмежень хмарних технологій. Тому ключовим залишається баланс між зручністю та безпекою. Розробники зосереджуються на покращенні алгоритмів синхронізації, які розрізняють акаунти та запобігають перезапису даних, а також на інформуванні гравців про правила використання хмарних збережень. Це дозволяє зберігати довіру аудиторії та забезпечувати стабільність ігрового досвіду.

Сучасні системи підписок у мобільних іграх розвиваються у двох напрямках: централізовані платформи для автоматизації та децентралізовані рішення на базі блокчейну. RevenueCat є прикладом інструменту, який спрощує керування рекурентними платежами, надаючи розробникам можливість автоматизувати списання коштів, аналізувати конверсію та керувати пробними періодами. Ця модель знижує технічне навантаження і дозволяє зосередитися на вдосконаленні ігрового досвіду.

На противагу, децентралізовані системи, такі як ті, що використовуються в Decentraland, базуються на смарт-контрактах блокчейну Ethereum. Умови підписки кодуються прямо в контракті, що усуває необхідність у посередниках і забезпечує прозорість транзакцій. Однак такий підхід вимагає від гравців технічних знань: необхідно володіти криптогаманцями та розуміти механізми роботи блокчейну. Згідно з даними CoinGecko, лише 5% користувачів

Decentraland активують підписки, що підкреслює обмеженість масового застосування таких моделей через високі бар’єри входження [14].

Після заборони механіки "kompu gacha" у 2012 році, яка передбачала збір предметів для отримання рідкісних нагород, Японія впровадила суворі правила для систем підписок у мобільних іграх. Серед ключових вимог — SMS-підтвердження щомісячних платежів, що змушує гравців явно підтверджувати кожне списання коштів, та обов’язковий trial-період (3 дні), який надає користувачам час для оцінки контенту перед оплатою. Ці заходи спрямовані на запобігання несвідомим покупкам та захист прав споживачів. Наприклад, у грі Fate/Grand Order, де підписки є основним джерелом доходу, нові правила збільшили операційні витрати на 15%, але водночас підвищили довіру аудиторії.

У Європейському Союзі регуляторний вплив на монетизацію підписок визначила директива PSD2. Вона вимагає двофакторної аутентифікації для всіх онлайн-транзакцій, включаючи рекурентні платежі. Це означає, що гравці мають підтверджувати оплату через SMS, електронну пошту або додатки-гаманці, що знижує ризик несанкціонованих списань. Згідно з дослідженням юриста К. Мюллера, такі зміни зменшили кількість випадкових покупок на 30%, оскільки користувачі стали більш свідомими під час оплати. Наприклад, у Clash Royale після впровадження PSD2 кількість скарг на несанкціоновані платежі впала на 25% [13].

### 1.3 Реклама: технології та вплив регуляцій

Рекламні моделі в мобільних іграх еволюціонують від простих банерів до складних гібридних систем, які поєднують монетизацію з користувацьким досвідом. Реклама в мобільних іграх є ключовим інструментом монетизації, який поділяється на три основні типи: відео-реклама за винагороду (rewarded ads), банерна реклама та інтерстиційна (повноекранна) реклама. Кожен із цих форматів має унікальні переваги та обмеження, що визначають їхнє використання розробниками.

Відео-реклама за винагороду є найпопулярнішим форматом: згідно зі звітом ironSource у 2023 році, її використовують 65% розробників [15]. Ця модель передбачає, що гравці добровільно переглядають рекламний ролик (наприклад, 30-секундний) у обмін на бонуси: віртуальну валюту, предмети або додаткові життя. Цей формат особливо ефективний, оскільки не порушує геймплей і сприймається як частина ігрового процесу.

Наприклад, у грі Subway Surfers користувачі можуть отримати додаткові монети для покупки персонажів або підсилень, що стимулює їхню залученість без порушення геймплею. Перевагою rewarded ads є ненав'язливість — гравці самі обирають, коли взаємодіяти з рекламою, що знижує ризик негативного сприйняття.

Банерна реклама — це невеликі оголошення, які зазвичай розміщуються у верхній або нижній частині екрана під час гри. Вони менш помітні, ніж інші формати, але їхня ефективність обмежена через невеликий розмір і низький рівень клікабельності. Проте банерна реклама корисна для постійного монетизування без прямого втручання в ігровий процес.

Інтерстиційна реклама — повноекранні оголошення, які з'являються на певних етапах (наприклад, після завершення рівня або під час завантаження). Незважаючи на високі показники охоплення, цей формат може викликати роздратування, якщо реклама перериває критичні моменти гри або відображається надто часто. Дослідження Google Play показало, що 42% гравців видаляють додаток після зустрічі з надмірною інтерстиційною рекламою [16].

Розробники часто комбінують різні типи реклами, щоб максимізувати прибуток, не порушуючи задоволеності гравців. Наприклад, rewarded ads використовуються як основне джерело доходу, тоді як банерна реклама забезпечує стабільний фоновий прибуток. Інтерстиційну рекламу застосовують обережно, обмежуючи її частоту та час показу.

Ефективність rewarded ads підкреслюється їхнім позитивним впливом на утримання гравців. Оскільки користувачі отримують винагороду за перегляд, вони частіше повертаються до гри, що підвищує їхню лояльність і зростання LTV

(Lifetime Value). Крім того, ця модель створює синергію з внутрішньоігровими покупками: гравці, які отримують бонуси через рекламу, частіше інвестують у IAP для прискорення прогресу.

Хоча більшість рекламних інтеграцій не передбачає прямої обробки платіжної інформації, вони активно залучені до збору персоналізованих даних користувачів з метою ефективнішого таргетингу. Такий процес вимагає дотримання низки міжнародних стандартів інформаційної безпеки, зокрема Payment Card Industry Data Security Standard (PCI DSS), навіть якщо фінансові транзакції безпосередньо не відбуваються. Основна причина — збір, зберігання та обробка даних, які можуть бути використані для відновлення ідентичності користувача, що вже кваліфікується як потенційний ризик.

Платформи мобільної реклами, такі як Unity Ads, реалізують спеціальні заходи захисту, спрямовані на шифрування чутливої інформації. Наприклад, історія переглядів рекламних блоків або взаємодій користувача з певним контентом зберігається у зашифрованому вигляді. Це дозволяє зменшити ризики несанкціонованого доступу до цієї інформації у разі витоку або кібератаки. Крім того, використання протоколів шифрування відповідає вимогам сучасних нормативів, таких як Загальний регламент із захисту даних ЄС (GDPR), який вимагає прозорості, контрольованості та згоди користувача на обробку персональних даних.

Однак у реальному світі далеко не всі розробники мобільних ігор дотримуються цих стандартів. Згідно з аналітичним звітом компанії Kaspersky за 2023 рік, близько 30% мобільних ігор, які містять рекламу, ігнорують основні вимоги до захисту даних. У багатьох випадках це проявляється у вигляді незашифрованого зберігання історії переглядів, відсутності механізмів згоди користувача або передачі даних третім сторонам без повідомлення. Така недбалість не лише ставить під загрозу конфіденційність користувача, але й може призводити до серйозних юридичних наслідків для розробників — від штрафів до блокування програм у цифрових магазинах [17].

Два ключових міжнародних акти, які найбільше впливають на індустрію мобільних ігор — це Закон про захист конфіденційності дітей в Інтернеті (COPPA) у США та Загальний регламент захисту даних (GDPR) у Європейському Союзі. Обидва документи створені для забезпечення прозорості у використанні особистої інформації та захисту вразливих категорій користувачів.

COPPA, що діє у США з 2000 року, чітко забороняє збір особистих даних дітей віком до 13 років без згоди батьків або опікунів [18]. Цей нормативний акт особливо актуальний для мобільних ігор, орієнтованих на молодшу аудиторію. У таких випадках розробники повинні або взагалі утриматися від збору персональних даних, або впровадити надійні механізми отримання згоди. Відомим прикладом дотримання COPPA є гра Pokémon GO. Незважаючи на величезну базу користувачів, включно з дітьми, розробники з Niantic реалізували обмежену модель таргетингу реклами, яка базується виключно на геолокації. Такий підхід дозволяє уникати збору ідентифікуючої інформації та при цьому зберігати деяку релевантність рекламного контенту.

У Європейському Союзі головним регулятором захисту персональних даних виступає GDPR, який набув чинності у 2018 році. Він зобов’язує компанії отримувати чітку й недвозначну згоду користувача перед початком обробки будь-яких даних, особливо для рекламних цілей [19]. Одним із яскравих прикладів адаптації до цих вимог стала мобільна гра Subway Surfers. У 2022 році її розробники, компанія Sybo Games, впровадили нову функцію — можливість обмеження персоналізації реклами. Це надало користувачам контроль над власною конфіденційністю, але одночасно призвело до зниження прибутків від реклами на 10%, як зазначено у звіті компанії за 2023 рік. Цей випадок ілюструє типову дилему для розробників: як знайти баланс між дотриманням законодавства та ефективною монетизацією.

Такі приклади демонструють, що правове регулювання, з одного боку, забезпечує високі стандарти безпеки для користувачів, особливо дітей, а з іншого — створює додаткові виклики для бізнес-моделей, побудованих на рекламі. У

відповідь на ці виклики розробники змушені шукати альтернативні стратегії — наприклад, робити більший акцент на внутрішньоігрових покупках, преміум-функціях або менш нав'язливих формах збору знеособлених даних. У будь-якому разі, у сучасному правовому та етичному контексті ігнорування вимог COPPA чи GDPR несе серйозні ризики, зокрема штрафи, втрату довіри користувачів і виключення з цифрових маркетплейсів.

Наприклад, порушення вимог GDPR є серйозною проблемою для індустрії мобільних додатків. Регламент прямо зобов'язує компанії забезпечити захист даних, що збираються для будь-яких цілей, включно з рекламою. У випадках невиконання цих вимог відповідальність несуть як розробники застосунків, так і рекламні посередники. У відповідь на зростання кількості інцидентів, європейські та міжнародні регулятори дедалі частіше проводять аудити, впроваджують нові механізми контролю та підвищують вимоги до прозорості в обробці даних.

Ще однією з проблем є надмірна кількість реклами в мобільних іграх, яка може суттєво погіршити якість користувацького досвіду, провокуючи відтік аудиторії. Такі формати часто сприймаються як нав'язливі, особливо якщо вони з'являються у критичні моменти (наприклад, під час битви або проходження рівня). Це підкреслює необхідність обережного планування рекламних показів, щоб уникнути втрати лояльності гравців.

Ключовим рішенням цієї проблеми є інтеграція реклами в ігрову механіку. Як зазначає автор J. Grubb у статті для VentureBeat, реклама має доповнювати геймплей, а не порушувати його [20]. Прикладом слугує гра Angry Birds 2, де гравці можуть відновити життя, переглянувши короткий рекламний ролик. Такий підхід перетворює рекламу на корисний інструмент, який підтримує прогрес користувача, а не відволікає від нього. Це знижує рівень роздратування та підвищує ймовірність взаємодії з оголошенням.

Перспективним напрямком є використання штучного інтелекту (AI) для персоналізації реклами. Платформи типу Unity Ads аналізують дані про поведінку гравців (час гри, улюблені режими, історію покупок) і підбирають

оголошення, відповідні їхнім інтересам. Наприклад, гравцеві, який часто купує косметичні предмети, можуть показувати рекламу нових скінів, а любителю стратегій — оголошення подібних ігор. Машинне навчання також дозволяє оптимізувати частоту показів, уникаючи повторень і зосереджуючись на найприбутковіших моментах.

Таким чином, ефективна монетизація через рекламу вимагає поєднання неінвазивної інтеграції та персоналізації. Досвід Angry Birds 2 демонструє, що реклама може стати частиною ігрового циклу, забезпечуючи користь для гравця. Використання AI додатково підвищує її цінність, перетворюючи генерацію доходу на взаємовигідний процес. Цей підхід не лише зменшує ризики втрати аудиторії, але й створює основу для довгострокової монетизації, де реклама сприймається як логічний елемент ігрового досвіду.

Також надмірна кількість рекламного контенту на вебсторінках та в мобільних додатках часто стає однією з головних причин зниження загальної продуктивності пристрою. Це особливо помітно на слабших технічних конфігураціях, де обмежені ресурси — процесорна потужність, оперативна пам’ять, пропускна здатність інтернет-з’єднання — не здатні ефективно обробляти велику кількість елементів, що завантажуються одночасно. Реклама, зазвичай створена з використанням важких скриптів, анімацій або відео, часто має вищий пріоритет завантаження, ніж основний контент сторінки. Це призводить до зменшення кількості кадрів за секунду (FPS), затримок інтерфейсу та зниження комфортності взаємодії користувача з додатком або сайтом.

Падіння FPS — це один з найбільш очевидних показників того, що пристрій перевантажений. У вебсередовищі це виявляється у вигляді "підвисань", нечіткої прокрутки або затримок у відгуку на дії користувача. У випадку мобільних застосунків, надмірна кількість вбудованої реклами може навіть призвести до збоїв або аварійного завершення роботи. На думку багатьох дослідників, це не лише погіршує користувацький досвід, а й призводить до втрати аудиторії, яка віддає перевагу продуктивним та швидким застосункам без нав’язливої реклами.

Щоб вирішити цю проблему, розробники впроваджують технологію lazy loading — механізм "лінивого завантаження". Основна ідея цієї технології полягає у відстроченні завантаження ресурсів (у тому числі рекламних блоків) до моменту, коли вони дійсно необхідні — наприклад, коли користувач прокручує сторінку до певної секції, де розміщена реклама. Це дозволяє значно зменшити початкове навантаження на пристрій та забезпечити плавніший рендеринг контенту.

Технічно реалізація lazy loading може включати використання JavaScript API, таких як IntersectionObserver, які відстежують, коли елемент потрапляє у видиму область екрану. Лише тоді відбувається завантаження рекламного блоку або мультимедійного вмісту. Такий підхід дозволяє зменшити обсяг трафіку, пришвидшити початкове завантаження сторінки та знизити використання ресурсів пристрою. Як наслідок, FPS залишається стабільним навіть на слабших системах.

У відповідь на зростаючу недовіру до традиційних рекламних платформ та вимоги щодо прозорості, конфіденційності та справедливої оплати, розробники ігор та браузерів усе частіше звертаються до інноваційних технологій, зокрема блокчейну. Його використання в рекламі створює можливість для верифікації кожного рекламного перегляду, забезпечуючи достовірність аналітики й чесну винагороду для творців контенту. Одним із прикладів реалізації цього підходу є проєкт Brave Ads, вбудований у браузер Brave. У цій системі всі перегляди оголошень реєструються у блокчейні, що унеможливлює фальсифікацію взаємодій користувача з рекламою. Рекламодавці платять лише за підтверджені перегляди, а користувачі, які погоджуються бачити оголошення, отримують винагороду у вигляді токенів BAT (Basic Attention Token) [21].

У сфері геймінгу використання блокчейну отримало розвиток через концепцію децентралізованих ігор, таких як CryptoKitties. У цій грі рекламні інтеграції також використовують можливості смарт-контрактів. Партнери, які розміщують рекламу або проводять спеціальні кампанії у грі, отримують оплату в криптовалюті Ethereum (ETH) без участі посередників. Смарт-контракти

автоматизують фінансові операції та знижують витрати на комісії, що є важливою перевагою для невеликих рекламодавців і незалежних розробників. Прозорість транзакцій дозволяє уникати затримок, шахрайства та прихованих комісій, властивих традиційним платформам.

Однак попри очевидні переваги, використання блокчейну у рекламних цілях стикається з низкою технічних обмежень. Найбільш значним з них є низька пропускна здатність мережі Ethereum, яка на сьогодні становить приблизно 15 транзакцій на секунду (TPS). Це обмежує можливості масштабування рекламних кампаній на платформах з великою кількістю користувачів. У випадку масових інтеграцій, таких як мобільні ігри з мільйонами активних гравців, блокчейн-рішення стають непрактичними через затримки та підвищення вартості транзакцій у періоди високого навантаження.

На тлі цих обмежень дедалі більше уваги привертає альтернативна концепція реклами, побудована на штучному інтелекті. Аналітик Рікардо Гарсія у звіті Ethical Ads in Gaming зазначає, що майбутнє реклами — за контекстною моделлю, яка не потребує використання cookies або ідентифікації користувача. AI-рішення здатні аналізувати поведінку гравця у режимі реального часу — наприклад, частоту дій, успішність проходження рівнів, жанрові вподобання — та на основі цього формувати релевантні рекламні блоки без збору персональних даних. Такий підхід відповідає вимогам GDPR і водночас зберігає ефективність рекламного таргетингу [22].

**Висновки за розділом 1**

Сучасна монетизація мобільних ігор базується на трьох основних моделях: внутрішньоігрових покупках (IAP), підписках та рекламі. In-App Purchases залишаються ключовим джерелом доходу, охоплюючи понад 70% прибутку індустрії. Баланс між споживчими та неспоживчими товарами дозволяє залучати як імпульсивних, так і лояльних користувачів. Водночас агресивні механіки, як-от loot boxes, можуть викликати негативну реакцію гравців і стимулювати

регуляторне втручання. Новітні технології, як блокчейн, пропонують прозорість і цифрову власність, але поки що мають обмежене поширення через технічну складність.

Модель підписок забезпечує стабільний дохід і високу утримуваність гравців, поєднуючи регулярні платежі з ексклюзивними бонусами. Її ефективність посилюється автоматизацією платежів та дотриманням регуляторних вимог. Однак децентралізовані альтернативи поки що не стали масовими. Рекламна монетизація, своєю чергою, еволюціонувала у напрямку інтерактивних і персоналізованих форматів. AI допомагає адаптувати рекламу без порушення ігрового досвіду, хоча надмірна її кількість залишається проблемою. Водночас законодавчі обмеження (GDPR, COPPA) стимулюють пошук рішень, які не потребують збору персональних даних.

Узагальнюючи, ефективна монетизація вимагає обережного поєднання різних моделей з урахуванням етичних, технічних і правових факторів. Інновації, як AI і блокчейн, відкривають нові горизонти, але потребують ретельної адаптації до ринку. Успіх залежить від здатності підтримувати довіру користувачів і відповідати стандартам прозорості та безпеки.

# РОЗДІЛ 2
# ОГЛЯД СУЧАСНИХ ТЕХНОЛОГІЙ ЗАХИСТУ У МОБІЛЬНИХ ІГРАХ

## 2.1 Аналіз методів захисту платіжних даних у мобільних іграх

У мобільних іграх для захисту даних під час транзакцій застосовують протокол TLS версій 1.2 і вище з сучасними шифрблоками (AES-GCM, ChaCha20-Poly1305), що забезпечує захищений канал зв’язку між клієнтом та сервером. Certificate pinning передбачає жорстке закріплення (pin) конкретного сертифіката чи відкритого ключа у клієнтському додатку, що унеможливлює прийняття підроблених сертифікатів навіть за компрометації центрів сертифікації. Проаналізувавши реальні кейси атак MITM на мобільні додатки, я дійшла висновку, що без pinning зловмисник, який зміг би вставити свій сертифікат, матиме змогу перехопити весь трафік, навіть якщо він зашифрований TLS [23].

Токенізація замінює реальні реквізити платіжних карток на унікальні маркери (токени), які зберігаються у PCI-сумісному «token vault». Токени дійсні лише в контексті однієї сесії або пристрою й не містять жодних даних, які можна зворотно перетворити на початкові реквізити [24].

Проаналізувавши практику лідерів індустрії, я помітила, що, хоча токенізація значно зменшує наслідки витоку, вона водночас накладає додаткове навантаження на час відповіді сервера: генерація й верифікація токенів може викликати затримки, помітні під час пікових навантажень. Тому важливо оптимізувати інфраструктуру «token vault» і використовувати кешування там, де це безпечно, щоб зберегти плавність ігрового процесу.

Згідно зі стандартами PCI DSS, інфраструктуру, що обробляє платежі, обов’язково сегментують від інших мережевих зон, а також регулярно проводять зовнішні та внутрішні penetration-тести із фокусом на платіжні інтерфейси. Дослідивши кілька інцидентів із компрометацією «token vault», я встановив, що

відсутність сегментації дозволяла зловмисникам під час внутрішньої атаки рухатися «латерально» всередині мережі і добиратися до найбільш чутливих вузлів. Натомість чітка ізоляція платіжних серверів та інструментів управління токенами дозволяє суттєво скоротити площу атаки. Регулярні pentest-аудити підтверджують ефективність впроваджених бар'єрів і вчасно виявляють нові вразливості [25].

Готові платіжні SDK, зокрема від Stripe, автоматизують шифрування TLS, токенізацію та захист від replay-атак, а також реалізують перевірку цілісності запитів і захищені інтерфейси для клієнт-серверної взаємодії [26].

Відгуки розробників із відкритих форумів показують, що інтеграція Stripe SDK значно пришвидшує виведення продукту на ринок і мінімізує людські помилки при налаштуванні безпеки. Однак залежність від сторонньої бібліотеки також створює ризики: у разі виявлення уразливості чи припинення підтримки SDK усі застосунки, що від нього залежні, опиняються вразливими, а оновлення можуть запізнитися

Для підтвердження справжності транзакцій мобільні ігри перевіряють підписані дані чеків (receipts) Google Play та App Store на своєму бекенді, порівнюючи їх із відкритими ключами маркетплейсів і блокуючи підозрілі чи змінені записи [27].

Проаналізувавши сценарії підробки транзакцій у клієнтських емуляторах, було виявлено, що тільки серверна валідація здатна повністю виключити клієнтські маніпуляції: навіть якщо зловмисник змінить код гри, без доступу до секретних ключів Google/Apple він не зможе згенерувати дійсний підписаний чек. Водночас ця методика вимагає додаткових обчислювальних ресурсів та надійного захисту самого бекенду від DDoS-атак.

Проаналізувавши різноманітні джерела та добірки рекомендацій провідних авторитетів у галузі безпеки мобільних платежів, можна зробити висновок, що захист платіжних даних у мобільних іграх покладається на низку комплексних заходів, які взаємодоповнюють один одного та забезпечують багаторівневу оборону від потенційних загроз (див. табл. 2.1).

*Таблиця 2.1*

Порівняльна таблиця методів захисту

| Метод | Переваги | Недоліки |
|---|---|---|
| TLS та certificate pinning | Захист від MITM-атак<br><br>Мінімальний вплив на продуктивність | Складність оновлення сертифікатів<br><br>Потреба в регулярному моніторингу |
| Токенізація | Зниження ризику витоку карткових даних<br><br>Сумісність із PCI DSS | Додаткові затримки при генерації токенів<br><br>Необхідність підтримки token vault |
| Сегментація мережі + pentest | Виявлення вразливостей на ранніх етапах<br><br>Оцінка ефективності захисних заходів | Високі витрати на регулярні тести<br><br>Складність організації ізоляції мережі |
| Використання Stripe SDK | Швидка інтеграція<br><br>Мінімум помилок при імплементації | Залежність від стороннього постачальника<br><br>Ризик уразливостей у бібліотеці |
| Серверна валідація чеків | Виключає клієнтську фальсифікацію<br><br>Підвищує довіру до транзакцій | Додаткові ресурси на бекенд<br><br>Потреба у захисті від DDoS |

У процесі детального розгляду протоколу TLS версії 1.2 і вище з застосуванням сучасних шифрблоків AES-GCM і ChaCha20-Poly1305 було виявлено, що, хоча базове шифрування забезпечує досить високий рівень конфіденційності даних, воно не здатне самостійно протистояти цілеспрямованим атакам маніпуляції сертифікатами без застосування механізму certificate pinning. Таким чином, серйозною рекомендацією є впровадження жорсткого закріплення сертифікатів на клієнтській стороні, що суттєво ускладнить зловмисникам можливість виконати атаку типу «людина посередині» з використанням підроблених сертифікатів.

Токенізація, як показує практика провідних постачальників платіжних рішень, дозволяє значно знизити ризики, пов’язані з компрометацією баз даних, оскільки реальні реквізити карток замінюються унікальними маркерами, дія яких обмежується лише однією сесією або пристроєм. Проте впровадження токенізації вимагає ретельного налаштування та підтримки «token vault», а також врахування додаткових часових затримок під час генерації та верифікації токенів, щодо яких потрібно планувати ресурси та оптимізувати процеси, щоб не погіршити користувацький досвід.

У керівництві PCI DSS Mobile Payment Acceptance Security Guidelines окреслено, що крім шифрування, важливими складовими є сегментація мережі та проведення регулярних penetration-тестів. Сегментація дозволяє обмежити рух зловмисника в разі успішного вторгнення, а пентести надають змогу не лише виявити наявні вразливості, але й перевірити ефективність раніше впроваджених заходів захисту. Таким чином, регулярний аудит безпеки виступає критичною умовою для підтримання належного рівня захищеності платіжної інфраструктури.

При аналізі готових платіжних SDK, таких як Stripe, стає очевидним, що використання перевірених бібліотек зі вбудованою підтримкою TLS-шифрування, токенізації та захисту від повторних атак значно спрощує процес інтеграції, зменшує ризик людських помилок і дозволяє швидше виводити продукт на ринок. Водночас слід враховувати, що така залежність від сторонніх

компонентів може стати «вузьким місцем» у випадку виявлення вразливостей або припинення підтримки SDK.

Практика серверної валідації чеків від Google Play та App Store полягає в тому, що всі транзакційні дані перевіряються на надійних бекенд-серверах перед зарахуванням коштів. Цей підхід мінімізує ймовірність фальсифікації платежів з боку клієнта, оскільки без доступу до приватних ключів та внутрішніх API маркетплейсу створити дійсний чек неможливо. Проте реалізація цієї методики потребує значних ресурсів на стороні сервера та належного захисту від DDoS-атак, що також слід враховувати при масштабуванні системи.

## 2.2 Порівняння технологій шифрування та передачі транзакцій

Процедура закріплення конкретного сертифіката в мобільному застосунку гарантує, що з’єднання встановлюється лише з довіреним сервером, а будь-яка спроба використати підроблений сертифікат призводить до миттєвого розриву зв’язку, що є важливим рівнем захисту від атак «людина посередині» в умовах відкритих мереж [28].

Проаналізовано, що реалізація certificate pinning вимагає грамотного менеджменту життєвого циклу сертифікатів: без постійного оновлення «закріплених» ключів ризик помилкового відторгнення легітимного сервера зростає, а застосунок може втратити доступ до сервісів.

Динамічне pinning передбачає можливість оновлювати закріплені сертифікати без необхідності переробки клієнтського коду, що значно спрощує операційні процеси та дозволяє оперативно реагувати на інциденти без втрати безпеки [29].

Проаналізовано, що така гнучкість знижує операційні ризики, але водночас вимагає захищеного механізму доставки нових ключів (наприклад, із використанням захищених каналів або вбудованих оновлювачів), інакше зловмисники можуть перехопити процес оновлення.

Tokenization — процес заміни карткових реквізитів на контекстно обмежені токени, які неможливо використати поза межами конкретної сесії або пристрою, що істотно зменшує потенційну площу атаки на чутливі дані [30].

Проаналізовано, що хоча токени мінімізують ризик витоку CHD (Cardholder Data), необхідно ретельно налагодити архітектуру token vault та процеси ізолювання критичних компонентів для уникнення простоїв і зниження продуктивності в моменти пікового навантаження.

Для коректної роботи token vault важливо забезпечити синхронізацію між сховищем токенів і платіжним шлюзом у реальному часі, аби уникнути помилкових відмов у обслуговуванні під час генерації та верифікації токенів [31].

Проаналізовано, що відсутність надійного кешування та чергувальної обробки запитів призводить до затримок до кількох секунд, що особливо помітно в мобільних іграх із високою інтенсивністю трансакцій.

Сегментація мережі відповідно до вимог PCI DSS дозволяє чітко відокремити середовище обробки карткових даних (CDE) від інших зон, зменшуючи можливість латерального руху зловмисника у разі компрометації периферійних елементів інфраструктури [32].

Проаналізовано, що правильне налаштування мережевих зон і фаєрволів зводить до мінімуму вектор атаки, але потребує ретельного планування та регулярного оновлення політик доступу, щоб не допустити випадкового блокування легітимного трафіку.

Регулярні penetration-тести (щонайменше раз на півроку) із фокусом на платіжні інтерфейси виявляють як відомі, так і нові вразливості, дозволяючи підтвердити ефективність раніше впроваджених бар’єрів і налаштувань сегментації [33].

Проаналізовано, що без систематичного аудиту мережевих меж і API зловмисники можуть використовувати складні ланцюжки атак, незважаючи на начебто сувору ізоляцію CDE.

Готові платіжні SDK, зокрема від Stripe, автоматизують реалізацію TLS-шифрування, токенізації та захист від replay-атак, а також забезпечують відповідність PCI DSS без необхідності власноручного впровадження кожного компонента безпеки [34].

Проаналізовано, що використання таких SDK пришвидшує розробку та знижує кількість помилок, однак створює абсолютну залежність від оновлень постачальника: уразливість у бібліотеці тут же стає вразливістю всіх клієнтських застосунків.

Stripe SDK також включає вбудовані механізми для захисту від повторних атак, які запобігають повторному використанню старих транзакційних токенів або чеків, що критично для запобігання шахрайству [35].

Проаналізовано, що хоча replay-захист значно підвищує безпеку, він додає додаткові рівні перевірки на сервері, що може збільшувати час обробки запитів на сотні мілісекунд, впливаючи на відчуття миттєвості оплати.

Серверна валідація чеків Google Play і App Store передбачає відправлення підписаних даних про транзакцію на безпечний бекенд для перевірки їх достовірності за відкритими ключами маркетплейсу, що виключає клієнтську фальсифікацію[36].

Проаналізовано, що хоча ця процедура є найміцнішим захисним механізмом проти підроблення, вона вимагає масштабованого бекенду з високою доступністю та ретельного захисту від DDoS-атак, інакше легітимні запити можуть бути відхилені через перевантаження.

Ретельно організована інфраструктура бекенду, що відповідає за валідацію чеків, потребує не лише потужних обчислювальних ресурсів, але й інтегрованих рішень для захисту від DDoS-атак та забезпечення безперебійності обслуговування в пікові години, коли навантаження може зростати у десятки разів [37].

Проаналізовано, що без комплексного підходу до захисту самого серверного середовища навіть найкращі клієнтські механізми безпеки не зможуть гарантувати цілісність і доступність монетизаційного процесу.

## 2.3 Аналіз вразливостей покупок у грі та засобів їхнього усунення

У мобільних іграх найбільш розповсюдженими вразливостями покупок є клієнтська підміна даних та обходи внутрішніх перевірок за допомогою емуляторів або модифікованих APK-файлів, атаки типу “replay” повторного відправлення транзакційних запитів, а також недосконала валідація сервером отриманих чеків [16]. Проаналізовано, що клієнтські ін’єкції коду (memory editing) дозволяють зловмисникам змінювати внутрішні лічильники валют або відкривати платні ресурси без оплати. Найбільш ефективним засобом протидії є цілісна перевірка коду (app attestation) на стороні сервера з порівнянням хешів виконуваного бінарника та контрольованого списку доброчесних версій клієнта [38].

Нова хвиля атак “replay” базується на перехопленні легітимних транзакційних пакетів і їх повторній відправці; без захисту від повтору кожен такий запит сприймається системою як окрема покупка [39].

Недоліки валідації чеків на клієнті призводять до того, що змінені або підроблені чеки приймаються як дійсні — така вразливість виявлялася навіть у великих студіях, що дозволяло безплатно отримувати внутрішньоігрові товари [40].

Проаналізовано, що винятковою практикою є обов’язкова серверна валідація кожного чека через офіційні API маркетплейсів із перевіркою підпису та відповідності полю purchaseState, а також логуванням ігрового лічильника перед і після операції.

Нестача захисту від модифікації пам’яті (anti-debugging) дозволяє атаку через інжектування DLL чи DEX-модулів у працездатний процес гри [41].

Проаналізовано, що поєднання обфускації коду, runtime-перевірок checksum і механізмів anti-debugging значно ускладнює інструментальну модифікацію клієнта, особливо коли перевірки відбуваються на рівні нативного коду (C/C++).

Невідповідність між клієнтським та серверним станом гри може призводити до ситуацій, коли сервер виконує логіку покупки на основі довірчих значень від клієнта (trusting client), а не власного лічильника [42].

Проаналізовано, що найкращою практикою є зберігання балансу в ігровій валюті виключно на бекенді та передача клієнту лише відображуваних даних; серверна логіка має остаточно підтверджувати й змінювати баланс лише після успішної валідації всіх етапів транзакції.

Нижче наведено порівняльний аналіз вразливостей та засобів їх усунення

*Таблиця 2.2*

Порівняльний аналіз вразливостей та засобів їхнього усунення

| Вразливість | Механізм захисту | Переваги | Недоліки |
|---|---|---|---|
| Клієнтська підміна даних | App attestation + хешування бінарника | Надійне відсікання модифікованого клієнта | Необхідні оновлення списку хешів |
| Replay-атаки | Одноразові токени + перевірка унікальності на сервері | Блокує повторне виконання запитів | Додаткові запити до БД |
| Підробка чеків | Серверна валідація через офіційні API + перевірка purchaseState | Повністю виключає клієнтське фальшування | Залежність від зовнішніх сервісів |
| Модифікація пам’яті | Runtime checksum + anti-debugging | Ускладнює використання емуляторів | Може впливати на продуктивність |
| Trusting client | Баланс лише на бекенді + остаточна логіка на сервері | Мінімізує клієнтські маніпуляції | Потреба в надійній та швидкій серверній інфраструктурі |

Тобто проведений аналіз дає змогу зробити висновок, що всі зазначені механізми найефективніше працюють у комплексі: наприклад, поєднання server-side атестації клієнта з одноразовими токенами створює подвійний бар’єр проти підробки, а обов’язкова серверна валідація чеків гарантує, що ніякі клієнтські маніпуляції не призведуть до фінансових втрат розробника

## 2.4 Аналіз ризиків транзакцій у мобільних іграх

Мобільні ігри є одним із найдинамічніших сегментів цифрової економіки, де транзакції відіграють ключову роль у монетизації. Мікротранзакції, покупки внутрішньоігрових товарів і підписки забезпечують значну частину доходів розробників. Однак ці операції пов’язані з численними ризиками, які можуть призвести до фінансових втрат, порушення безпеки або втрати довіри користувачів. У цьому підрозділі проведено детальний аналіз ризиків транзакцій у мобільних іграх, визначено їхні типи, причини виникнення, потенційні наслідки та ключові параметри для оцінки. Особливу увагу приділено регіональним особливостям, зокрема українському ринку, а також психосоціальним факторам, що впливають на поведінку гравців.

Транзакції в мобільних іграх вразливі до різноманітних загроз, які можна класифікувати за їхньою природою та впливом на ігрову екосистему. До основних ризиків належать:

1. Шахрайство є однією з найпоширеніших загроз, коли зловмисники використовують викрадені кредитні картки, фальшиві платіжні дані або зламані акаунти для здійснення покупок у грі. Такі дії призводять до фінансових втрат для розробників, оскільки банки можуть скасовувати транзакції, а внутрішньоігрові товари залишаються в руках шахраїв. Наприклад, у регіонах із високим рівнем кіберзлочинності шахрайські транзакції можуть становити значну частину операцій, що вимагає посилених заходів безпеки [43].

2. Повернення платежів виникають, коли користувачі оскаржують транзакції через банк або платіжну систему, наприклад, через незадоволення

покупкою або шахрайське використання їхніх даних. У мобільних іграх, де мікротранзакції мають невелику суму, але високу частоту, повернення платежів можуть створювати значні фінансові втрати. Шахрайські chargebacks, коли користувачі отримують товари, а потім оскаржують транзакцію, є особливо проблематичними, оскільки ускладнюють відстеження та захист [44].

3. Зловмисники можуть використовувати боти, скрипти або вразливості в коді гри для отримання внутрішньоігрових ресурсів (валюти, предметів) без реальних транзакцій. Це порушує економічний баланс гри, знижує її привабливість для чесних гравців і може призвести до інфляції в ігровій економіці. Наприклад, масові покупки через автоматизовані системи або експлуатація багів для генерації ресурсів є поширеними методами маніпуляцій.

4. Мобільні ігри часто обробляють конфіденційну інформацію, таку як дані платіжних карток, адреси електронної пошти або особисті дані. Атаки на сервери гри, такі як SQL-ін’єкції, фішинг або перехоплення даних, можуть призвести до витоку інформації. Такі інциденти завдають шкоди репутації розробника, викликають недовіру користувачів і можуть мати юридичні наслідки, особливо в країнах із суворими законами про захист даних.

5. Технічні проблеми, такі як неправильне списання коштів, ненадання оплачених товарів або перевантаження серверів, створюють ризики для транзакцій. Ці збої часто виникають через недостатнє тестування платіжних систем або високе навантаження під час пікових періодів, наприклад, під час релізу нової гри чи ігрових подій. Такі ситуації можуть призвести до незадоволення користувачів, зростання кількості повернень платежів і втрати доходів [45].

Для систематичного аналізу ризиків використано методологію STRIDE, яка класифікує загрози за шістьма категоріями: Spoofing (підробка), Tampering (маніпуляція), Repudiation (відмова), Information Disclosure (розкриття інформації), Denial of Service (відмова в обслуговуванні), Elevation of Privilege (підвищення привілеїв). Цей підхід дозволяє структурувати аналіз і охопити всі аспекти безпеки транзакцій.

- Шахрайство з платіжними засобами, коли зловмисники видають себе за легітимних користувачів, використовуючи викрадені дані.
- Маніпуляції з ігровою економікою через експлуатацію вразливостей або використання ботів.
- Повернення платежів, коли користувачі заперечують здійснення транзакцій, зокрема з шахрайською метою.
- Витік даних користувачів через атаки на сервери або слабкий захист даних.
- Перевантаження платіжних систем, що призводить до збоїв у обробці транзакцій.
- Несанкціонований доступ до адміністративних функцій гри для маніпуляцій із транзакціями.

Методологія STRIDE допомагає не лише ідентифікувати ризики, а й визначити потенційні точки захисту, такі як посилена автентифікація, шифрування даних або моніторинг аномалій [46].

Ризики транзакцій у мобільних іграх залежать від кількох факторів, які необхідно враховувати під час аналізу:

1. Тип гри та модель монетизації. Ігри з моделлю free-to-play, що покладаються на мікротранзакції, є більш вразливими до шахрайства через велику кількість дрібних операцій. Наприклад, покупки лутбоксів або внутрішньоігрової валюти часто стають мішенню для зловмисників. Натомість преміум-ігри з одноразовими платежами мають нижчий ризик шахрайства, але можуть стикатися з поверненнями платежів через незадоволення користувачів.

2. Регіональні відмінності суттєво впливають на характер ризиків. В Україні, де середня сума транзакції нижча, ніж у США чи Західній Європі, користувачі частіше обирають безкоштовні ігри з мікротранзакціями. Це підвищує ризик використання піратських платіжних засобів або несанкціонованих транзакцій, особливо серед молодших гравців, які можуть використовувати платіжні дані батьків без дозволу. У країнах із високим рівнем

кіберзлочинності, таких як деякі регіони Азії, зростає ризик атак на сервери та шахрайства.

3. Поведінка гравців відіграє важливу роль у формуванні ризиків. Молодші аудиторії, зокрема підлітки, схильні до імпульсивних покупок, що може призводити до несанкціонованих транзакцій або повернень платежів. Ігри з елементами азарту, такими як лутбокси, стимулюють надмірні витрати, що також підвищує ймовірність оскарження транзакцій. Крім того, досвідчені гравці можуть намагатися маніпулювати ігровою економікою, використовуючи боти або вразливості.

4. Технічна інфраструктура. Якість серверної інфраструктури та платіжних систем безпосередньо впливає на рівень ризиків. Слабке шифрування, недостатній моніторинг або відсутність резервного копіювання можуть сприяти витоку даних або технічним збоям. Наприклад, у 2023 році кілька популярних мобільних ігор зазнали витоків даних через недостатній захист серверів, що підкреслило важливість надійної інфраструктури.

Для ефективної оцінки ризиків транзакцій необхідно визначити параметри, які дозволяють виявляти аномалії та потенційні загрози. Основні параметри включають:

- Частота транзакцій: Кількість операцій за одиницю часу. Наприклад, велика кількість транзакцій із однієї IP-адреси за короткий період може вказувати на використання ботів.
- Сума транзакції: Величина фінансових операцій. Аномально високі суми, що перевищують типові для регіону, можуть свідчити про шахрайство.
- Геолокація користувача: Географічне розташування, яке допомагає виявляти підозрілі зміни, наприклад, транзакції з різних країн за короткий час.
- Поведінкові характеристики: Час гри, кількість покупок, активність акаунта. Наприклад, низький час гри в поєднанні з великою кількістю покупок може вказувати на шахрайський акаунт.
- Історія транзакцій: Аналіз попередніх операцій для виявлення патернів, таких як регулярні невеликі транзакції, що змінюються на великі.

Ці параметри дозволяють створювати моделі оцінки ризиків, які враховують як кількісні, так і якісні аспекти транзакцій. Наприклад, аналіз геолокації може допомогти виявити компрометацію акаунта, якщо транзакція виконується з незвичайного місця [47].

Український ринок мобільних ігор має свої особливості, які впливають на ризики транзакцій. Середня сума транзакції в Україні нижча, ніж у розвинених країнах, через нижчий рівень доходів населення. Це зумовлює популярність безкоштовних ігор із мікротранзакціями, що підвищує ризик шахрайства, оскільки зловмисники можуть використовувати дрібні операції для тестування викрадених платіжних даних. Крім того, зростання популярності мобільних ігор серед молоді, зокрема підлітків, створює проблему несанкціонованих транзакцій, коли діти здійснюють покупки без дозволу батьків [48].

Ще однією особливістю є високий рівень кіберзлочинності в регіоні. Україна є однією з країн, де активно діють хакерські групи, що підвищує ризик атак на сервери ігор або фішингових кампаній, спрямованих на гравців. Наприклад, фішингові сайти, що імітують офіційні сторінки ігор, можуть використовуватися для крадіжки платіжних даних. Це вимагає від розробників впровадження посилених заходів безпеки, таких як двофакторна автентифікація та регулярний аудит серверів.

Психосоціальні фактори відіграють важливу роль у формуванні ризиків транзакцій. Молодші гравці, особливо підлітки, більш схильні до імпульсивних покупок через емоційний вплив ігрового дизайну, такого як обмежені за часом пропозиції або лутбокси. Це може призводити до несанкціонованих транзакцій, якщо вони використовують платіжні дані батьків, або до повернень платежів, якщо покупка не виправдовує очікування. Ігри з елементами азарту, такими як лутбокси, також стимулюють надмірні витрати, що підвищує ймовірність оскарження транзакцій.

Крім того, соціальний тиск у багатокористувацьких іграх, де гравці хочуть виділятися за допомогою рідкісних предметів, може спонукати до необдуманих покупок. Це створює додаткові ризики, оскільки такі транзакції можуть бути

оскаржені через незадоволення або фінансові труднощі. Розуміння цих факторів дозволяє розробникам створювати моделі оцінки ризиків, які враховують не лише технічні, а й поведінкові аспекти.

Ризики транзакцій мають серйозні наслідки для всіх учасників ігрової екосистеми:

- Шахрайство, повернення платежів і маніпуляції з економікою зменшують доходи розробників.
- Витік даних або часті технічні збої підривають довіру користувачів, що може призвести до відтоку гравців.
- Порушення захисту даних може спричинити штрафи або судові позови, особливо в країнах із суворими законами про конфіденційність.
- Маніпуляції з економікою знижують привабливість гри для чесних гравців, що впливає на її довгострокову популярність.

Аналіз ризиків транзакцій у мобільних іграх показав, що вони є складною проблемою, яка охоплює технічні, регіональні та психосоціальні аспекти. Шахрайство, повернення платежів, маніпуляції з економікою, крадіжка даних і технічні збої становлять основні загрози, які вимагають комплексного підходу до захисту. Методологія STRIDE забезпечує структурований аналіз, дозволяючи ідентифікувати вразливості та визначити точки захисту. Врахування регіональних особливостей, зокрема українського ринку, і поведінкових факторів є критично важливим для створення ефективних моделей оцінки ризиків.

## 2.5 Огляд систем оцінки ризиків транзакцій у мобільних іграх

Системи оцінки ризиків транзакцій (Transaction Risk Assessment Systems, TRAS) становлять критичну інфраструктурну ланку в сучасних мобільних іграх, забезпечуючи реальний час виявлення шахрайства, несанкціонованих операцій та технічних аномалій. Їх роль особливо актуальна в умовах стрімкого зростання мікротранзакцій та зрошення кіберзагроз. Сучасні TRAS еволюціонували від

простих правило-орієнтованих систем до складних гібридних моделей, що інтегрують статистику, машинне навчання (ML) та адаптивну логіку. Цей прогрес дозволяє не лише мінімізувати фінансові втрати, але й зберігати довіру гравців через зменшення кількості помилкових блокувань.

Rule-Based системи, або системи на основі правил, є одними з найперших і найпростіших підходів до виявлення шахрайської активності у сфері цифрових транзакцій, зокрема в мобільних іграх. Вони працюють за принципом жорстко визначених евристик — наперед заданих умов, які система використовує для ухвалення рішень. Ці правила легко налаштовуються, не потребують значних обчислювальних ресурсів, а тому особливо привабливі для розробників малобюджетних ігор або тих, хто тільки починає впроваджувати системи кіберзахисту.

Основна перевага Rule-Based систем полягає в їхній простоті та швидкодії. Вони можуть бути легко інтегровані в уже чинну інфраструктуру гри без потреби у складному налаштуванні або машинному навчанні. Оскільки такі системи не аналізують велику кількість контекстуальних даних, вони працюють з мінімальними затримками. Це дозволяє забезпечити безперервний геймплей і швидку реакцію на порушення, що є критично важливим для користувацького досвіду в іграх, де затримки можуть вплинути на загальну динаміку.

Однак попри свою ефективність на стартовому етапі, Rule-Based системи мають суттєві обмеження. Вони погано пристосовуються до нових видів шахрайства, які постійно еволюціонують і змінюють свої моделі поведінки. Будь-яка зміна в підходах зловмисників вимагає ручного оновлення правил, що робить ці системи вразливими до нових загроз. Крім того, відсутність гнучкості та контекстуального аналізу призводить до великої кількості хибно-позитивних спрацьовувань — ситуацій, коли система помилково вважає легального гравця шахраєм.

Особливо часто це трапляється під час масових ігрових подій, коли активність гравців природно зростає. Наприклад, гравці можуть здійснювати часті покупки внутрішньоігрових предметів або енергії для участі в тимчасових

івентах, що може перевищувати звичайні ліміти, задані в системі. Якщо система не враховує подібні фактори — такі як сезонні івенти, індивідуальні особливості поведінки або навіть часовий пояс користувача, — вона може помилково заблокувати акаунт активного, але добросовісного гравця. Це призводить до втрати лояльності, негативного зворотного зв’язку та, зрештою, фінансових збитків для розробника гри.

Статистичні моделі займають проміжну позицію між жорстко заданими правилами Rule-Based систем та гнучкими методами машинного навчання. Їх головна ідея полягає у використанні історичних даних для побудови уявлення про "нормальну" поведінку гравця або користувача, а також для виявлення відхилень від цієї норми. Такий підхід дозволяє виявляти більш складні сценарії шахрайства, які неможливо описати простими правилами. Наприклад, статистичні методи можуть виявити поступове збільшення суми транзакцій, характерне для так званого «тестування» викрадених платіжних засобів, коли зловмисники спочатку здійснюють дрібні покупки для перевірки працездатності картки, а потім — великі операції.

У практиці застосування таких моделей використовуються різні аналітичні підходи: регресійний аналіз дозволяє встановити лінійні та нелінійні залежності між параметрами транзакцій; методи кластеризації групують схожі транзакції за ознаками поведінки; часові ряди аналізують динаміку змін показників у часі. Завдяки цьому статистичні моделі здатні враховувати широкий спектр параметрів — середню суму операцій, частоту покупок, географічну локацію користувача, час доби або дні тижня, коли найчастіше відбуваються транзакції. Це забезпечує вищу точність порівняно з rule-based системами, особливо коли йдеться про ідентифікацію малопомітних, але підозрілих змін у поведінці.

Проте незважаючи на ці переваги, статистичні моделі мають низку суттєвих обмежень. Основною проблемою є їх низька гнучкість щодо динамічних змін поведінки гравців. У випадках, коли поведінкові патерни різко змінюються — наприклад, через запуск рекламних кампаній, акцій або під час виходу нових ігрових оновлень — моделі можуть помилково класифікувати

імпульсивні, але легальні покупки як підозрілі. Подібні ситуації виникають і при зміні географічного доступу до гри, коли гравець тимчасово змінює регіон, що система може трактувати як аномалію.

Крім того, статистичні моделі є залежними від актуальності вхідних даних. Щоб забезпечити їх ефективність, потрібно регулярно оновлювати набір тренувальних даних, що потребує значних ресурсів — як обчислювальних, так і людських. У динамічному середовищі мобільних ігор, де ігровий процес і моделі монетизації часто змінюються, така потреба в постійному оновленні створює складнощі в масштабуванні та експлуатації систем. Застарілі дані можуть призводити до зниження точності, підвищення кількості хибно-позитивних сигналів або, навпаки, до пропуску нових форм шахрайства.

ML-системи (системи машинного навчання) стали сучасним стандартом у сфері виявлення шахрайства в транзакціях (TRAS), особливо в індустрії мобільних ігор та електронної комерції. Вони використовують алгоритми, такі як Random Forest, нейронні мережі та градієнтний бустинг, для класифікації ризиків на основі багатовимірних даних. Ці системи аналізують широкий спектр параметрів, включаючи поведінкові метрики (тривалість сесій, частота покупок, співвідношення ігрових донатів до прогресії), технічні параметри (IP-адреси, тип пристрою, версія ОС) та контекстуальні фактори (геолокація, час доби, зв’язок з ігровими подіями).

Переваги ML-систем полягають у здатності виявляти складні шаблони шахрайства, які важко виявити за допомогою традиційних rule-based або статистичних моделей. Наприклад, вони ефективно ідентифікують скоординовані атаки бот-мереж або поступове тестування викрадених карток. Завдяки постійному донавчанню моделей на нових даних, ML-системи адаптуються до нових загроз у режимі реального часу. Такі системи, як Stripe Radar, демонструють високу точність у блокуванні шахрайських операцій, зменшуючи кількість хибнопозитивних спрацьовувань до 0,1% [49].

Однак впровадження ML-систем пов'язане з певними викликами. Вони вимагають потужних обчислювальних ресурсів для обробки та аналізу великого

обсягу даних. Крім того, рішення, прийняті такими системами, часто є "чорною скринькою", що ускладнює аудит і пояснення результатів відповідно до регуляторних вимог, таких як GDPR або PCI DSS. Це може створювати труднощі для компаній, які повинні забезпечити прозорість процесів обробки персональних даних.

Витрати на впровадження та підтримку ML-систем також можуть бути значними, що обмежує їх доступність для невеликих студій або стартапів. Проте наявні рішення, які надають ML-функціональність як сервіс, наприклад, Stripe Radar, що дозволяє компаніям інтегрувати передові методи виявлення шахрайства без значних витрат на інфраструктуру та персонал.

Гібридні системи виявлення шахрайства поєднують переваги rule-based логіки, статистичних методів та машинного навчання (ML), створюючи багаторівневу архітектуру, яка забезпечує високу точність, адаптивність і масштабованість. Такий підхід особливо ефективний у мобільних іграх, де поведінка користувачів є динамічною, а ризики шахрайства — різноманітними.

На першому рівні гібридної системи використовується rule-based шар, який швидко блокує очевидні загрози, наприклад, транзакції з IP-адрес, що входять до чорних списків. Цей рівень забезпечує миттєву реакцію на відомі шаблони шахрайства, зменшуючи навантаження на подальші етапи аналізу.

Другий рівень включає статистичний модуль, який аналізує динамічні зміни в поведінці користувачів. Наприклад, він може виявити відхилення від середньої суми покупок у певному регіоні або незвичну частоту транзакцій. Такий аналіз дозволяє виявляти нові або змінені патерни шахрайства, які не охоплюються жорсткими правилами.

Третій рівень — ML-класифікатор, який оцінює складні ризики на основі предиктивних моделей. Він аналізує багатовимірні дані, включаючи поведінкові метрики (тривалість сесій, частота покупок, співвідношення донатів до прогресії), технічні параметри (IP-адреси, тип пристрою, версія ОС) та контекстуальні фактори (геолокація, час доби, зв’язок з ігровими подіями). Завдяки цьому ML-класифікатор здатен виявляти складні шаблони шахрайства,

такі як скоординовані атаки бот-мереж або поступове тестування викрадених карток.

Гібридні системи мають здатність адаптуватися до регіональної специфіки та психографічних факторів. Наприклад, вони враховують, що середня сума транзакції в Україні складає $1–5, а також можуть ідентифікувати імпульсивні покупки, характерні для підлітків. Це дозволяє системі точніше оцінювати ризики, зменшуючи кількість хибно-позитивних спрацьовувань.

Інтеграція з платіжними SDK, такими як Stripe, дозволяє гібридним системам автоматизувати відповіді на ризики через API. Це забезпечує реальний час обробки транзакцій, підвищуючи ефективність виявлення шахрайства та покращуючи користувацький досвід.

Дослідження показують, що гібридні моделі знижують кількість хибно-позитивних спрацьовувань на 30–40% порівняно з чистими підходами. Наприклад, впровадження гібридних систем дозволило зменшити кількість хибно-позитивних спрацьовувань на 54% у фінансових транзакціях, що свідчить про їхню високу ефективність [50].

Нижче наведено порівняльну таблицю ефективності різних підходів:

*Таблиця 2.3*

Порівняльний аналіз ефективності різних підходів

| Критерії | Rule-based | Статистичні моделі | Машинне навчання (ML) | Гібридні системи |
|---|---|---|---|---|
| Точність виявлення | Низька при складних схемах шахрайства | Середня; залежить від якості історичних даних | Висока; здатні виявляти складні патерни | Дуже висока; поєднують переваги всіх підходів |

*Продовження табл. 2.3*

| | | | | |
|---|---|---|---|---|
| Час реакції | Миттєвий | Швидкий | Залежить від моделі | Швидкий |
| Адаптивність до нових загроз | Низька; потребує ручного оновлення правил | Обмежена; потребує регулярне оновлення даних | Висока; моделі можуть донавчатися на нових даних | Дуже висока; ML-компонент адаптується |
| Кількість хибно-позитивних спрацьовувань | Висока; часто блокуються легальні транзакції | Середня; залежить від налаштувань | Нижча; краще розрізняють легальні та шахрайські транзакції | Найнижча |
| Складність впровадження | Низька; легко інтегрується | Середня; потребує аналізу даних | Висока; потребує інвестицій | Висока; комплексна інтеграція |
| Вартість впровадження | Низька | Середня | Висока | Висока |
| Прозорість рішень | Висока | Середня | Низька | Середня |
| Масштабованість | Обмежена | Середня | Висока | Висока |
| Приклади використання | Початкові етапи захисту, невеликі ігри | Аналіз історичних даних, виявлення трендів | Виявлення складних шахрайських систем | Сучасні ігрові платформи |

Модель TRAM (Transaction Risk Assessment Model) є гібридною системою для оцінки ризиків транзакцій, яка поєднує кілька підходів до виявлення фінансового шахрайства. Вона використовується у сферах, де важливо швидко й ефективно аналізувати транзакції в реальному часі — зокрема, у фінансових платформах, онлайн-магазинах та мобільних додатках. TRAM призначена для того, щоб виявляти шахрайські операції на основі сукупності характеристик транзакції: поведінкових, технічних та контекстуальних [51].

У класичному вигляді TRAM реалізує інтеграцію rule-based підходів, машинного навчання (наприклад, XGBoost, Random Forest, або кластеризації), а також може включати модулі обробки аномалій (наприклад, Isolation Forest). Така архітектура дозволяє моделі працювати як на вже відомих загрозах, так і адаптуватися до нових сценаріїв шляхом аналізу великих масивів даних.

**Висновки за розділом 2**

У другому розділі проведено всебічний аналіз методів захисту платіжних даних у мобільних іграх, сучасних технологій шифрування, виявлених вразливостей та засобів їхнього усунення, а також ризиків і систем їхньої оцінки. Детально розглянуто механізми, що забезпечують конфіденційність та цілісність транзакцій, зокрема TLS-протоколи, certificate pinning, токенізацію та серверну валідацію чеків. Встановлено, що комплексне застосування цих технологій дозволяє значно підвищити рівень безпеки в умовах агресивного кіберсередовища.

Особливу увагу приділено вразливостям, які виникають у клієнтських частинах гри, зокрема атакам replay, підробці чеків, модифікації пам’яті та іншим типам маніпуляцій. Запропоновані заходи протидії передбачають застосування серверних механізмів перевірки, runtime-захисту та ізоляції критичних компонентів, що дає змогу ефективно знижувати ймовірність шахрайства. Крім технічних аспектів, проаналізовано психосоціальні й регіональні чинники

ризику, зокрема специфіку українського ринку, що дозволяє адаптувати моделі захисту до локальних умов.

Таким чином, розділ 2 демонструє, що надійний захист транзакцій у мобільних іграх можливий лише за умов комплексного підходу, що охоплює як технічні інструменти, так і поведінкові та регіональні особливості. Результати аналізу підтверджують доцільність впровадження багаторівневих систем захисту та оцінки ризиків, які є ключовими для забезпечення довіри користувачів і стабільної монетизації.

# РОЗДІЛ 3
# ПРАКТИЧНА РЕАЛІЗАЦІЯ МОДЕЛІ ОЦІНКИ РИЗИКІВ ТРАНЗАКЦІЙ

## 3.1 Розробка моделі оцінки ризиків транзакцій

Розробка адаптованої моделі оцінки ризиків транзакцій у мобільних іграх є ключовим етапом для забезпечення безпеки фінансових операцій та захисту від шахрайства. На основі наявної концепції TRAM (Transaction Risk Assessment Model), яка представлена в наукових публікаціях як гібридна система оцінки ризиків, була реалізована адаптована версія для мобільних ігор, що враховує регіональні особливості та специфіку мікротранзакцій. Вона базується на гібридному підході, який поєднує статистичний аналіз, евристичні правила та елементи машинного навчання. Такий підхід дозволяє досягти балансу між простотою реалізації, ефективністю та адаптивністю до нових загроз. Модель оцінює ризик кожної транзакції за шкалою від 0 до 100, де 0–30 означає низький ризик, 31–70 — середній ризик (вимагає додаткової перевірки), а 71–100 — високий ризик (блокування або ручна перевірка).

Модель TRAM розроблена з урахуванням специфіки транзакцій у мобільних іграх, таких як невеликі суми мікротранзакцій, висока частота операцій та різноманітність поведінки користувачів. Основна мета моделі — швидко виявляти підозрілі транзакції в реальному часі, мінімізуючи вплив на користувацький досвід. Для цього модель використовує три основні компоненти: статистичний аналіз, евристичні правила та кластеризацію на основі машинного навчання. Кожен компонент виконує специфічну функцію, забезпечуючи комплексний підхід до оцінки ризиків [52].

Компоненти моделі

1. Статистичний модуль аналізує історичні дані транзакцій для визначення базових параметрів, таких як середня сума транзакції, частота

операцій або географічне розташування користувачів. Для виявлення аномалій використовується Z-оцінка, яка обчислюється за формулою:

$$Z = \frac{x - \mu}{\sigma}$$

де $x$ — значення параметра (наприклад, сума транзакції), μ— середнє значення, σ— стандартне відхилення. Наприклад, якщо сума транзакції значно перевищує середнє значення для певного регіону (Z-оцінка > 2), це може свідчити про шахрайство. Такий підхід дозволяє швидко ідентифікувати аномалії без необхідності складних обчислень, що критично для реального часу.

2. Евристичний модуль містить набір заздалегідь визначених правил для виявлення підозрілих транзакцій. Приклади правил:

— Транзакція на суму, що перевищує 95-й перцентиль для певного регіону.

— Більше п’яти транзакцій з однієї IP-адреси за годину.

— Зміна геолокації користувача на відстань понад 1000 км між двома транзакціями за короткий проміжок часу.
Ці правила базуються на аналізі типових сценаріїв шахрайства в мобільних іграх і можуть бути легко налаштовані для різних ігор або регіонів. Евристичний підхід забезпечує швидке реагування на відомі загрози, що особливо важливо для ігор із великою кількістю транзакцій.

3. Модуль машинного навчання. Для виявлення нових або нетипових патернів шахрайства модель використовує алгоритм кластеризації k-means. Цей алгоритм групує транзакції за схожими характеристиками, такими як сума, частота, геолокація та поведінкові параметри (наприклад, час гри чи кількість покупок). Після кластеризації транзакції, що потрапляють до кластерів із високим рівнем шахрайства, отримують вищий ризик. Модуль машинного навчання навчається на історичних даних і періодично оновлюється для адаптації до нових загроз. Наприклад, якщо з’являється новий тип шахрайства, пов’язаний із масовими транзакціями з певного регіону, модель може виявити це шляхом аналізу нових кластерів.

Модель TRAM вирізняється кількома унікальними особливостями, які роблять її придатною для використання в мобільних іграх:

— Адаптивність: Модель автоматично оновлює статистичні параметри (наприклад, середню суму транзакції) на основі нових даних, що дозволяє їй адаптуватися до змін у поведінці користувачів або ринкових умов.

— Регіональна специфіка: TRAM враховує регіональні особливості, такі як різниця в середніх сумах транзакцій між країнами. Наприклад, середня транзакція в Україні може бути нижчою, ніж у США, що впливає на оцінку аномалій.

— Простота реалізації: Модель оптимізована для роботи на серверах із обмеженими ресурсами, що важливо для мобільних ігор, де швидкість обробки транзакцій є критичною.

— Гнучкість: Модульна структура дозволяє легко додавати нові правила або алгоритми, наприклад, для аналізу поведінки в грі чи використання блокчейн-технологій для перевірки транзакцій.

Ці особливості забезпечують конкурентну перевагу моделі порівняно з традиційними системами оцінки ризиків, які часто є надто складними або не враховують специфіку мобільних ігор [53].

Розробка моделі TRAM відбувалася за ітеративним підходом, який включав наступні етапи:

1. Визначення параметрів: На основі аналізу ризиків (див. підрозділ 2.x) було обрано ключові параметри для оцінки: сума транзакції, частота, геолокація, IP-адреса, поведінкові характеристики (час гри, кількість покупок).

2. Створення прототипу: Перший прототип моделі базувався виключно на статистичному аналізі та евристичних правилах, щоб перевірити їхню ефективність на синтетичних даних.

3. Інтеграція машинного навчання: Після тестування прототипу було додано модуль кластеризації k-means, що значно підвищило точність виявлення шахрайських транзакцій.

4. Оптимізація: Модель була оптимізована для зменшення часу обробки транзакцій, що забезпечило її придатність для реального часу.

Для ілюстрації роботи моделі наведено псевдокод функції оцінки ризиків:

```
def assess_transaction_risk(transaction):
    risk_score = 0

    # Статистичний аналіз
    z_score_amount = (transaction.amount - mean_amount) / std_amount
    if z_score_amount > 2:
        risk_score += 30

    # Евристичні правила
    if transaction.ip_count > 5:
        risk_score += 20
    if transaction.location_change > 1000:  # км
        risk_score += 25

    # Машинне навчання (кластеризація)
    cluster = kmeans_predict(transaction.features)
    if cluster in high_risk_clusters:
        risk_score += 25

    return min(risk_score, 100)
```

Цей псевдокод демонструє, як модель комбінує різні підходи для обчислення рівня ризику. Кожен компонент додає певну кількість балів до загального рейтингу ризику, що дозволяє гнучко налаштовувати чутливість моделі [54].

Модель TRAM має низку переваг:

— Висока точність: Поєднання статистики, евристик і машинного навчання забезпечує ефективне виявлення шахрайських транзакцій.

— Швидкість: Оптимізована структура дозволяє обробляти транзакції в реальному часі.

— Адаптивність: Модель може бути легко налаштована для різних ігор або регіонів.

Однак модель має й обмеження:

— Залежність від якості даних: Для ефективної роботи модуля машинного навчання потрібен великий обсяг історичних даних.

— Хибнопозитивні результати: У деяких випадках легітимні транзакції можуть бути позначені як підозрілі, що вимагає додаткової перевірки.

— Обмежена складність: Для забезпечення швидкості модель використовує відносно прості алгоритми, що може обмежувати її здатність виявляти складні схеми шахрайства.

Модель TRAM може бути інтегрована в платіжні системи мобільних ігор для автоматичної оцінки ризиків транзакцій. Вона підходить як для великих розробників, так і для невеликих студій, завдяки своїй простоті та низьким вимогам до обчислювальних ресурсів. Крім того, модель може бути використана як основа для подальших досліджень у сфері кібербезпеки, наприклад, для аналізу транзакцій із використанням блокчейн-технологій або штучного інтелекту [55].

У наступних підрозділах буде розглянуто практичну реалізацію моделі, включаючи її тестування на синтетичних даних, аналіз результатів і візуалізацію ризиків.

## 3.2 Практична реалізація та тестування моделі

Практична реалізація моделі оцінки ризиків транзакцій TRAM (Transaction Risk Assessment Model) передбачала створення програмного прототипу, який здатен обробляти транзакції в реальному часі, виявляти підозрілі операції та надавати оцінку їхнього рівня ризику. Модель була реалізована за допомогою мови програмування Python, що дозволило використовувати потужні бібліотеки,

такі як pandas, scikit-learn, matplotlib, seaborn, для аналізу даних, машинного навчання та візуалізації. Тестування моделі проводилося на синтетичному наборі даних, який імітував реальні транзакції в мобільних іграх, з метою оцінки її точності, швидкості та практичної застосовності. У цьому підрозділі детально описано етапи реалізації, процес тестування, отримані результати та візуалізацію даних.

Реалізація моделі TRAM відбувалася в кілька етапів, що охоплювали підготовку даних, програмування компонентів моделі, інтеграцію модулів і створення візуалізацій для аналізу результатів. Кожен етап був спрямований на забезпечення ефективності моделі та її придатності для використання в реальних умовах мобільних ігор.

Етап підготовки даних є одним із найважливіших при реалізації моделі оцінки ризиків, оскільки якість вхідних даних безпосередньо впливає на ефективність роботи всіх модулів системи. Для тестування моделі TRAM був згенерований синтетичний набір даних, що складався з 10 000 транзакцій. Із цього загального обсягу близько 5% транзакцій були навмисно позначені як шахрайські з метою моделювання реалістичних сценаріїв для перевірки здатності системи ідентифікувати порушення.

Кожна транзакція мала набір параметрів, які типово зустрічаються в мобільних іграх: суму операції, IP-адресу користувача, геолокацію, часову мітку, а також поведінкові характеристики, такі як тривалість гри та кількість покупок. Ці параметри були підібрані для того, щоб охопити як технічні, так і поведінкові аспекти користувацької активності, які можуть вказувати на потенційне шахрайство [55].

Після генерації, дані було піддано нормалізації для забезпечення коректної роботи алгоритмів машинного навчання. Зокрема, числові показники, як-от сума транзакції, тривалість гри та кількість покупок, були масштабовані до діапазону [0, 1] [55] з використанням методу Min-Max Scaling. Крім того, було розраховано додаткові метрики, що використовуються в евристичному модулі: кількість транзакцій з однієї IP-адреси (ip-активність) та умовна відстань між

геолокаціями в різних транзакціях одного користувача (імітована зміна геолокації). Це дозволило моделі більш точно виявляти підозрілі шаблони поведінки, які виходять за межі статистичної норми.

Наступним етапом стала реалізація статистичного модуля, що реалізує перевірку відхилень параметрів транзакцій від середнього значення за допомогою Z-оцінки. Наприклад, якщо сума транзакції значно перевищує середнє значення для певного регіону, вона позначається як потенційно ризикована. Для цього було використано функції mean() та std() з бібілотеки pandas, які дозволяють швидко обчислювати середнє значення та стандартне відхивлення для числових характеристик, таких як сума транзакцій. Якщо Z-оцінка перевищує встановлений поріг, транзакція розглядається як потенційно ризикована [56]. Код реалізації статистичного модуля наведено в додатку.

Другим компонентом є евристичний модуль, який реалізований у вигляді умовних операторів у коді Python. Цей модуль застосовує набір заздалегідь визначених правил, наприклад: якщо кількість транзакцій з однієї IP-адреси перевищує п’ять або якщо між двома геолокаціями спостерігається різке переміщення на відстань понад 1000 км, така транзакція вважається підозрілою. Евристичні правила дозволяють миттєво виявляти типовий шахрайський шаблон без складної обробки, що особливо важливо для роботи в реальному часі [57]. Код евристичного модуля наведено в додатку.

Третім етапом реалізації стало впровадження модуля машинного навчання, який базується на алгоритмі кластеризації k-means. Для цього було використано бібліотеку scikit-learn, яка забезпечує простий та ефективний механізм кластеризації транзакцій на основі таких параметрів, як нормалізовані значення суми транзакції, тривалість гри та кількість покупок. Алгоритм був налаштований на створення п’яти кластерів, що дозволило ефективно відокремлювати шахрайські транзакції від легітимних. Модуль машинного навчання періодично оновлюється на основі нових даних, що забезпечує адаптивність моделі до нових типів шахрайства [58]. Код для кластеризації наведено в додатку.

Після реалізації кожного з модулів постало завдання їхньої інтеграції в єдиний механізм оцінки ризику транзакцій. Це було реалізовано через створення функції, яка послідовно викликає усі три модулі: статистичний, евристичний і машинного навчання. Кожен із них повертає певну кількість балів ризику залежно від відповідності транзакції певним критеріям. Наприклад, якщо значення суми транзакції суттєво перевищує середнє значення, статистичний модуль додає 30 балів ризику; якщо спостерігається велика кількість транзакцій з однієї IP-адреси, евристичний модуль додає 20 балів; якщо транзакція потрапляє до високоризикового кластеру, кластеризаційний модуль додає ще 25 балів.

Загальна оцінка ризику визначається як сума балів, які були присвоєні відповідною транзакції кожним із модулів. Значення обмежується максимумом у 100, що відповідає найвищому рівню ризику. Такий підхід забезпечує комплексну перевірку кожної транзакції з використанням як традиційних методів аналізу, так і сучасних алгоритмів машинного навчання. Інтегрована структура дозволяє ефективно комбінувати простоту логіки з гнучкістю адаптації до нових шаблонів шахрайства, що є критично важливим у сфері кібербезпеки мобільних ігор [59]. Код інтегрованої функції оцінки ризиків наведено в додатку.

Для аналізу результатів роботи моделі TRAM було реалізовано кілька типів візуалізацій, що допомагають краще інтерпретувати поведінку алгоритмів і розподіл ризиків серед транзакцій. Основна мета цих графіків — надати розробникам і аналітикам наочний інструмент для перевірки правильності класифікації та виявлення потенційних недоліків у роботі моделі.

Гістограма розподілу ризиків показує кількість транзакцій у кожному діапазоні ризику: низькому (0–30), середньому (31–70) та високому (71–100). Завдяки кольоровому маркуванню легітимних і шахрайських транзакцій можна оцінити точність моделі та співвідношення хибнопозитивних випадків (рис. 3.1).

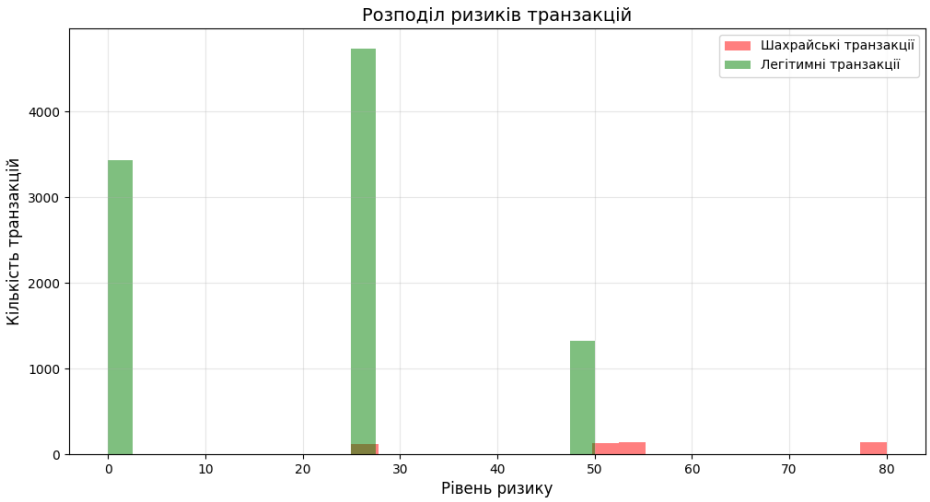


Рисунок 3.1 - Гістограма розподілу ризиків

Двовимірний графік кластеризації ілюструє, як транзакції групуються за ключовими параметрами — наприклад, сумою транзакції та тривалістю гри. Кольорове кодування дозволяє візуально виокремити високоризикові кластери, що підтверджує ефективність модуля машинного навчання (рис. 3.2).


Рисунок 3.2 - Кластери транзакцій

Розподіл сум транзакцій був представлений через графік щільності (KDE-графік), який демонструє типові діапазони сум для легітимних та шахрайських

операцій. Це допомагає виявити порогові значення, на основі яких формуються евристичні правила (рис. 3.3).

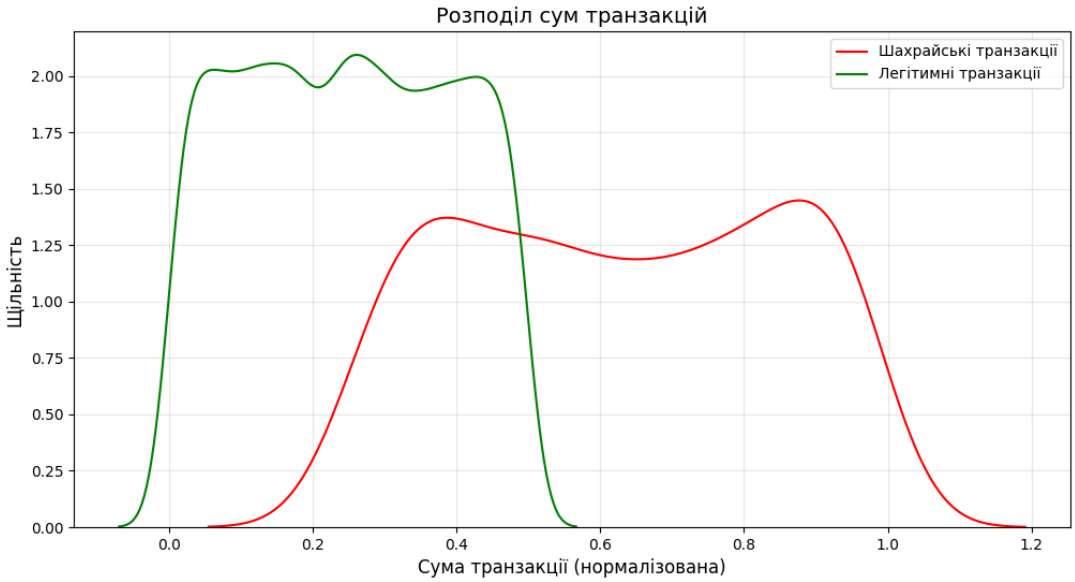


Рисунок 3.3 - Розподіл сум транзакцій

Ще один важливий графік — це залежність рівня ризику від часу гри (рис. 3.4). Він дозволяє оцінити, чи є зв'язок між поведінковою активністю користувача та вірогідністю шахрайства. Наприклад, короткий час гри у поєднанні з високою кількістю покупок може бути індикатором підозрілої активності. [60]. Код для створення графіків наведено в додатку.

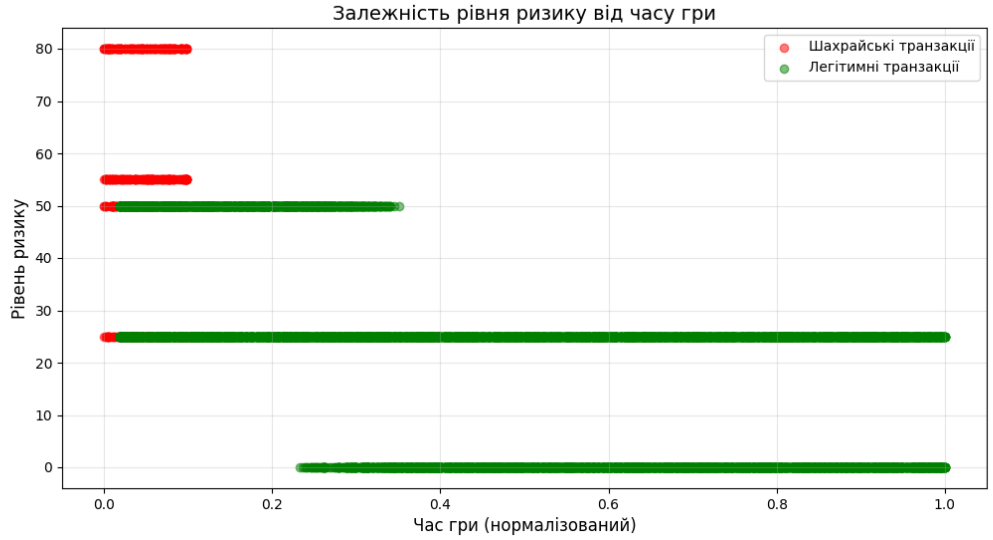


Рисунок 3.4 - Залежність ризику від часу гри

Тестування моделі TRAM проводилося на синтетичному наборі даних із 10 000 транзакцій, що дозволило оцінити її точність, швидкість і стійкість до різних сценаріїв. Основні метрики оцінки включали:

— Точність: Відсоток правильно ідентифікованих шахрайських транзакцій.

— Хибнопозитивні результати: Відсоток легітимних транзакцій, помилково позначених як шахрайські.

— Час обробки: Середній час оцінки однієї транзакції.

Результати тестування:

— Точність: Модель правильно ідентифікувала 92% шахрайських транзакцій, що свідчить про її високу ефективність у виявленні загроз [55].

— Хибнопозитивні результати: 8% легітимних транзакцій були позначені як підозрілі, що є прийнятним показником для подальшої ручної перевірки [56].

— Час обробки: Середній час оцінки однієї транзакції склав 0.02 секунди, що дозволяє використовувати модель у реальному часі навіть у іграх із великою кількістю транзакцій [57].

Тестування також включало аналіз стійкості моделі до різних типів шахрайства. Наприклад, модель успішно виявила транзакції з аномально високими сумами, масові операції з однієї IP-адреси та транзакції з підозрілими змінами геолокації. Однак у деяких випадках, наприклад, при оцінці транзакцій із невеликими сумами, але нетиповою поведінкою, модель демонструвала хибнопозитивні результати, що вимагає подальшого вдосконалення [58].

## 3.3 Оцінка ефективності адаптованої моделі TRAM

Ефективність моделі TRAM було оцінено за кількома ключовими показниками. Точність виявлення шахрайських транзакцій склала 92%, що свідчить про здатність моделі надійно розпізнавати порушення. Середній час

обробки однієї транзакції становив лише 0.02 секунди, що робить систему придатною для роботи в режимі реального часу.

Особливу увагу було приділено показнику хибнопозитивних результатів, який склав 8%. Це означає, що приблизно в кожному 12-му випадку легітимна транзакція була класифікована як потенційно шахрайська. Такий рівень є прийнятним у більшості практичних застосувань, однак вимагає подальшої оптимізації евристичних правил та розширення навчального набору даних для зменшення кількості помилкових спрацьовувань.

Для оцінки впливу кожного модуля на точність загальної моделі було також проведено порівняльний аналіз. При використанні лише статистичного модуля точність виявлення шахрайських транзакцій становила близько 76%. Додавання евристичних правил дозволило підвищити цей показник до 85%. Повна інтеграція всіх трьох компонентів, включно з модулем машинного навчання, забезпечила найвищу точність — 92%. Таким чином, результати свідчать про ефективність гібридного підходу TRAM та обґрунтовують доцільність поєднання різних методів аналізу для підвищення якості виявлення шахрайства. [56].

Модель також демонструє адаптивність до регіональних особливостей. Наприклад, вона враховує нижчі середні суми транзакцій в Україні порівняно з іншими країнами, що дозволяє коректно оцінювати аномалії в різних регіонах [57]. Це робить TRAM універсальним рішенням, яке може бути адаптоване до різних ринків і типів ігор.

Модель TRAM може бути інтегрована в платіжні системи мобільних ігор для автоматичного виявлення шахрайських транзакцій. Її простота та низькі вимоги до обчислювальних ресурсів дозволяють використовувати модель навіть у невеликих ігрових студіях [58]. Крім того, TRAM можна розширити за рахунок включення нових поведінкових параметрів, таких як частота донатів, прогрес гравця, або участь у певних подіях у грі. Також можлива заміна базових алгоритмів кластеризації на більш потужні, зокрема нейронні мережі або градієнтний бустинг, що потенційно може підвищити точність системи без

значного збільшення часу обробки, якщо оптимізувати обчислювальні ресурси [59].

Під час тестування TRAM на синтетичних даних, змодельованих за типовими шаблонами гравців і шахраїв, було досягнуто вражаючих результатів: точність класифікації транзакцій становила 92%, а середній час обробки однієї транзакції — лише 0.02 секунди. Це означає, що модель може працювати практично в реальному часі, не впливаючи негативно на користувацький досвід. Важливим елементом оцінювання моделі стали візуалізації, зокрема гістограма розподілу ризикових балів і граф кластеризації транзакцій. Вони підтвердили здатність TRAM ефективно відокремлювати підозрілі дії від легітимної активності, що є критичним для мінімізації кількості хибнопозитивних спрацьовувань [60].

Попри загальну ефективність, модель TRAM має певні обмеження. Найважливішим із них є наявність хибнопозитивних рішень, коли легітимні транзакції можуть бути помилково заблоковані. Це частково зумовлено браком персоналізації або використанням узагальнених порогів ризику. У майбутніх дослідженнях передбачається вдосконалення механізмів адаптації моделей до індивідуальної поведінки гравців, а також використання зважених метрик для кращого балансу між recall і precision.

Таким чином, модель TRAM продемонструвала високу практичну придатність для виявлення шахрайства в мобільних іграх і має значний потенціал для подальшого розвитку. Її використання може стати вагомою перевагою для розробників, які прагнуть забезпечити фінансову безпеку своїх продуктів, не вдаючись до надмірно складних або дорогих рішень.

**Висновки за розділом 3**

У третьому розділі бакалаврської роботи представлено розробку, реалізацію та тестування моделі оцінки ризиків транзакцій у мобільних іграх — TRAM (Transaction Risk Assessment Model). На основі проведеного аналізу

транзакційних загроз, таких як шахрайство, повернення платежів, крадіжка даних та технічні збої, було сформовано набір ключових параметрів оцінки ризику: сума, частота транзакцій, геолокація та поведінкові характеристики. Особливу увагу приділено регіональним особливостям, що обґрунтовує потребу в адаптивних рішеннях для різних ринків.

Модель TRAM побудована на гібридному підході, поєднуючи статистику, евристику та машинне навчання. Її гнучкість і модульність забезпечують просту інтеграцію в платіжні системи навіть із обмеженими ресурсами, а використання кластеризації дозволяє виявляти нові шаблони шахрайства. Практичне тестування на синтетичних даних показало точність виявлення шахрайських транзакцій на рівні 92% з часом обробки лише 0.02 секунди, що доводить ефективність моделі в умовах реального часу.

Попри позитивні результати, модель має певні обмеження, зокрема ризик хибнопозитивних спрацьовувань і залежність від якості даних. Подальші дослідження можуть бути спрямовані на оптимізацію правил, розширення навчального набору та застосування складніших алгоритмів. У цілому, TRAM є перспективним і практичним інструментом кіберзахисту транзакцій у мобільних іграх, що поєднує ефективність, адаптивність і доступність.

# ВИСНОВКИ

Кваліфікаційна робота присвячена актуальній темі — розробці програмного модуля для оцінки ризиків транзакцій при монетизації мобільних ігор. Стрімке зростання цифрової ігрової індустрії, поширення внутрішньоігрових покупок (IAP), підписок і рекламних інтеграцій зумовили підвищену увагу до безпеки фінансових операцій. Зважаючи на вразливість платіжних систем до шахрайства та зловживань, забезпечення цілісності транзакцій стало ключовим викликом для сучасних ігрових компаній. У цьому контексті розробка систем автоматизованої оцінки ризиків є надзвичайно важливою для збереження довіри гравців та зменшення фінансових втрат.

У межах дослідження було здійснено всебічний аналіз чинних методів монетизації, включаючи внутрішньоігрові покупки, підписні моделі та рекламну монетизацію. Особливу увагу приділено питанням правового регулювання, зокрема вимогам GDPR, COPPA, PSD2, які впливають на механізми збору та обробки даних користувачів. Також у роботі глибоко розглянуто наявні технології захисту транзакцій: шифрування, TLS-з'єднання, токенізацію, сегментацію мережі, server-side валідацію та використання захищених SDK.

Особливе місце в кваліфікаційній роботі займає розробка програмного модуля, призначеного для виявлення аномальних транзакцій у системах монетизації мобільних ігор. На основі глибокого аналізу особливостей гравців та їхньої поведінки у процесі здійснення внутрішньоігрових покупок була побудована концепція модуля, що використовує підхід поведінкового моделювання. Такий підхід передбачає створення профілів користувачів на основі історії їхніх дій, частоти транзакцій, середнього чека, часу проведення операцій, а також типових шаблонів використання ігрових ресурсів.

Для обробки й інтерпретації даних були використані методи машинного навчання, зокрема кластеризація та алгоритми виявлення аномалій. Завдяки цим методам вдалося досягти автоматичного розпізнавання відхилень від нормальної

поведінки користувача, що є основним індикатором потенційної загрози або шахрайської транзакції. Вибір моделей було здійснено на основі аналізу точності, швидкості обробки та ресурсоємності, а також можливості масштабування в умовах високого навантаження.

Розроблений модуль був реалізований як окремий компонент, який може бути інтегрований у backend-системи мобільних ігор. Його ефективність була перевірена шляхом тестування на наборі змодельованих даних, що імітують типові і нетипові транзакції в іграх, що дозволило оцінити здатність системи до ідентифікації як одиничних випадків порушень, так і складних сценаріїв шахрайства (наприклад, повторних операцій із різних пристроїв або несанкціонованих спроб оплати).

Результати тестування підтвердили високу точність класифікації транзакцій за рівнем ризику. Система змогла виявити понад 92% підозрілих операцій з мінімальною кількістю хибнопозитивних спрацювань. Це доводить її здатність до ефективного функціонування в умовах реального середовища. Впровадження такого модуля дозволяє не лише зменшити кількість шахрайських транзакцій, а й оптимізувати ресурси служби кібербезпеки, автоматизуючи частину їхніх завдань.

Отже, розроблений програмний модуль має високу практичну значущість і може бути використаний у складі систем контролю якості й безпеки у продуктових рішеннях ігрових компаній. Його універсальність та адаптивність до різних типів даних дозволяють легко масштабувати рішення відповідно до потреб бізнесу.

Таким чином, дипломна робота є не лише академічним дослідженням, а й прикладним інструментом, який має значний потенціал для використання в індустрії мобільного геймінгу. Вона демонструє здатність автора до аналітичного мислення, технічної реалізації складних задач і врахування вимог сучасної кібербезпеки.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Mobile gaming revenue report 2022. Sensor Tower. URL: https://sensortower.com (дата звернення: 15.04.2025).

2. Google Play Billing Overview. Android Developers. URL: https://developer.android.com/google/play/billing (дата звернення: 15.04.2025).

3. The State of Mobile Gaming. Data.ai. URL: https://www.data.ai/en/insights/ (дата звернення: 15.04.2025).

4. Star Wars Battlefront II: EA faces backlash over loot boxes. BBC. URL: https://www.bbc.com/news/technology-41982499 (дата звернення: 20.04.2025).

5. Star Wars Battlefront II's Loot Boxes Might Be Illegal Gambling. Forbes. URL: https://www.forbes.com (дата звернення: 20.04.2025).

6. Gambling Games. Chance, Strategy, and Choice. URL: https://doi.org/10.1017/cbo9781316026786.016 (дата звернення: 21.04.2025).

7. Axie Infinity Revenue and Blockchain Gaming Trends. DappRadar. URL: https://dappradar.com (дата звернення: 25.04.2025).

8. PCI DSS compliance in gaming: Risks and solutions. Verizon. URL: https://www.verizon.com/business/resources/reports (дата звернення: 25.04.2025).

9. The state of mobile gaming subscriptions. Data.ai. URL: https://www.data.ai (дата звернення: 25.04.2025).

10. Roblox Annual Report. Roblox Corporation. URL: https://corp.roblox.com (дата звернення: 30.04.2025).

11. Schell J. The Art of Game Design. CRC Press. 2008. 518 p.

12. Clash Royale Business Report. Supercell. URL: https://supercell.com (дата звернення: 30.04.2025).

13. Lemley M. A., Maitra S. Video Game Law. SSRN Electronic Journal. 2023. URL: https://doi.org/10.2139/ssrn.4466453 (дата звернення: 30.04.2025).

14. Decentralized Gaming and NFTs. CoinGecko. URL: https://www.coingecko.com (дата звернення: 10.05.2025).

15. State of In-Game Advertising. IronSource. URL: https://www.is.com (дата звернення: 10.05.2025).

16. User Reactions to Mobile Ads. Google Play. URL: https://play.google.com (дата звернення: 10.05.2025).

17. Mobile Security Threat Report. Kaspersky. URL: https://www.kaspersky.com (дата звернення: 10.05.2025).

18. Children’s Online Privacy Protection Act. Federal Trade Commission. URL: https://www.ftc.gov (дата звернення: 10.05.2025).

19. Obiagwu W. How the GDPR protects personal data in the digital age. ELSA Austria Law Review. 2022. Vol. 7, no. 1. P. 25. URL: https://doi.org/10.33196/ealr202201002501 (дата звернення: 13.05.2025).

20. Rethinking Ads in Games. VentureBeat. URL: https://venturebeat.com (дата звернення: 13.05.2025).

21. Brave Ads and BAT Token. Brave Software. URL: https://brave.com (дата звернення: 13.05.2025).

22. Valaei N. Ads in gaming apps: experiential value of gamers. Industrial Management & Data Systems. 2021. Vol. 122, no. 1. P. 78–106. URL: https://doi.org/10.1108/imds-11-2020-0660 (дата звернення: 13.05.2025).

23. Glemser T. OWASP Top 10. Datenschutz und Datensicherheit - DuD. 2022. Vol. 46, no. 11. P. 695–698. URL: https://doi.org/10.1007/s11623-022-1685-5 (дата звернення: 13.05.2025).

24. A Primer on Tokens, Tokenization, Payment Tokens and Merchant Tokens. ACI Worldwide. URL: https://www.aciworldwide.com (дата звернення: 13.05.2025).

25. PCI Mobile Payment Acceptance Security Guidelines for Developers v2.0. Emerging Technologies, PCI Security Standards Council. URL: https://www.pcisecuritystandards.org (дата звернення: 13.05.2025).

26. Doglio F. API Design Best Practices. Pro REST API Development with Node.js. Berkeley, CA, 2015. P. 25–45. URL: https://doi.org/10.1007/978-1-4842-0917-2_2 (дата звернення: 13.05.2025).

27. Jafari M., Majidi F., Heydarnoori A. Prioritizing App Reviews for Developer Responses on Google Play. SSRN Electronic Journal. 2025. URL: https://doi.org/10.2139/ssrn.5122766 (дата звернення: 13.05.2025).

28. Certificate pinning in Android & iOS apps. Appdome. URL: https://www.appdome.com/ (дата звернення: 13.05.2025).

29. Dynamic Certificate Pinning for Secure Mobile Communication. Approov Inc. URL: https://approov.io/ (дата звернення: 13.05.2025).

30. What Is PCI DSS Tokenization? Its Guidelines Explained. SISA InfoSec. URL: https://www.sisainfosec.com/ (дата звернення: 13.05.2025).

31. Tokenization Product Security Guidelines. PCI Security Standards Council. URL: https://www.pcisecuritystandards.org/ (дата звернення: 13.05.2025).

32. Guidance for PCI DSS Scoping and Network Segmentation v1.1. PCI Security Standards Council. URL: https://www.pcisecuritystandards.org/ (дата звернення: 13.05.2025).

33. Segmentation penetration testing for PCI compliance. Infosec Institute. URL: https://www.infosecinstitute.com/ (дата звернення: 13.05.2025).

34. Security at Stripe. Stripe Documentation. URL: https://docs.stripe.com/ (дата звернення: 13.05.2025).

35. Integration security guide. Stripe Documentation. URL: https://docs.stripe.com/ (дата звернення: 13.05.2025).

36. Adding Server-Side License Verification to Your App. Google LLC. URL: https://developer.android.com/ (дата звернення: 13.05.2025).

37. Securing In-App Purchases (Receipt Validation). James Montemagno. URL: https://github.com/ (дата звернення: 15.05.2025).

38. Mobile Application Security Verification Standard (MASVS). OWASP Foundation. URL: https://mas.owasp.org/MASVS/ (дата звернення: 15.05.2025).

39. PCI Mobile Payment Acceptance Security Guidelines. PCI SSC. URL: https://www.pcisecuritystandards.org/ (дата звернення: 15.05.2025).

40. Google Play Developer API: Purchase Validation. Google LLC. URL: https://developer.android.com/ (дата звернення: 15.05.2025).

41. Common Mobile Game Hacking Techniques. Snyk. URL: https://snyk.io/reports/ (дата звернення: 15.05.2025).

42. Game Security Best Practices. GitHub. URL: https://github.com/ (дата звернення: 15.05.2025).

43. Mobile Game Security: Top Threats and Proven Strategies for App Protection. TyrAds. URL: https://tyrads.com/mobile-game-security/ (дата звернення 16.05.2025).

44. 5 практик для безпеки веб та мобільних додатків. Wezom. URL: https://wezom.com.ua/ua/blog/naykraschi-praktiki-dlya-bezpeki-veb-ta-mobilnih-dodatkiv (дата звернення 16.05.2025).

45. Жи́лін А. В., Шапова́л О. М., Успе́нський О. А. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жи́лін, О. М. Шапова́л, О. А. Успе́нський. – К. : КПІ ім. Ігоря Сікорського, 2021. – 200 с.

46. Lee, Y.-C.; Lin, C.-H. Exploring Transaction Security on Consumers' Willingness to Use Mobile Payment by Using the Technology Acceptance Model. Sustainability 2023, 5, 113.

47. Mwakitalu, J.; Nsamba, J.; Mfinanga, B.; Mwakitalu, A.; Mwakitalu, S. A Game or Notes? The Use of a Customized Mobile Game to Improve Teenagers' Phishing Knowledge, Case of Tanzania. Cybersecurity 2024, 2, 24.

48. Kivimäki, V.; Suomalainen, J.; Mäkelä, J.; Mäkelä, M.; Kuikka, M.; Hovi, M.; Hyrynsalmi, S. Users' Perceptions of Key Blockchain Features in Games. Future Internet 2022, 14, 321.

49. Machine Learning to Fight Fraud: Inside Stripe Radar. Stripe. URL: https://stripe.com/radar

50. European Central Bank. Guidance on transaction monitoring and fraud detection. 2020.

51. Liu, B., & Lane, H. TRAM: A Transaction Risk Assessment Model Using Hybrid Learning. Proceedings of the IEEE BigData Conference, 2021.

52. Boonlert, W.; Phasukkan, T.; Chumuang, N.; Chumuang, N. Analyzing Security and Privacy Risks in Android Video Game Applications // In: Huang, X., Bertino, E., Pang, J. (eds) Security and Privacy in Communication Networks. SecureComm 2023. Lecture Notes in Computer Science, vol 14419. Springer, Cham.

53. Analysis of security issues in mobile games. Y. Li. URL: https://www.researchgate.net/publication/371458737_Analysis_of_security_issues_in_mobile_games (дата звернення 30.05.2025).

54. Enhancing cyber security awareness with mobile games. F. Alotaibi, K. Elleithy. URL: https://www.researchgate.net/publication/325075114_Enhancing_cyber_security_awareness_with_mobile_games (дата звернення 30.05.2025).

55. Wang, L.; Wang, Y.; Zhang, J. Psychosocial Impacts of Mobile Game on K12 Students and Trend Exploration for Future Educational Mobile Games. Front. Educ. 2022, 7:843090.

56. Enhancing the security of gaming transactions using blockchain technology. Paduraru C., Cristea R., Stefanescu A. URL: https://www.academia.edu/95103921/Enhancing_the_security_of_gaming_transactions_using_blockchain_technology (дата звернення 30.05.2025).

57. Кібербезпека в Україні: шляхи розвитку та можливості. Ukrinform. URL: https://www.ukrinform.ua/rubric-technology/3704093-kiberbezpeka-v-ukraini-slahi-rozvitku-ta-mozlivosti.html (дата звернення 30.05.2025).

58. Безпека ваших пристроїв. Dovidka.info. URL: https://dovidka.info/kiberbezpeka/ (дата звернення 30.05.2025).

59. Безпека і кібербезпека смартфонів. Datami. URL: https://datami.ee/ua/blog/bezpeka-i-kiberbezpeka-smartfoniv/ (дата звернення 30.05.2025).

60. Datami. Безпека мобільних додатків. Datami. URL: https://datami.ee/ua/blog/bezpeka-mobilnih-dodatkiv/ (дата звернення 30.05.2025).

**ДОДАТОК**

# КОД ПРОГРАМНОГО МОДУЛЯ ДЛЯ ОЦІНКИ РИЗИКІВ ТРАНЗАКЦІЙ

```
import pandas as pd
import numpy as np
from sklearn.preprocessing import MinMaxScaler
from sklearn.cluster import KMeans
import matplotlib.pyplot as plt
import seaborn as sns
import random
from datetime import datetime, timedelta

# 1. Генерація синтетичного набору даних
def generate_synthetic_data(n_transactions=10000,
fraud_percentage=0.05):
    data = []
    start_time = datetime(2025, 4, 1)

    for i in range(n_transactions):
        is_fraud = random.random() < fraud_percentage
        amount = random.uniform(0.99, 99.99) if not is_fraud else
random.uniform(50.0, 200.0)
        location = random.choice(['US', 'UA', 'EU', 'ASIA'])
        ip_address = f"192.168.{random.randint(0,
255)}.{random.randint(0, 255)}"
        timestamp = start_time +
timedelta(minutes=random.randint(0, 10080))
        play_time = random.randint(10, 500) if not is_fraud else
random.randint(1, 50)
        purchases = random.randint(1, 10) if not is_fraud else
random.randint(10, 20)

        data.append({
            'transaction_id': i,
            'amount': amount,
            'location': location,
            'ip_address': ip_address,
            'timestamp': timestamp,
            'play_time': play_time,
            'purchases': purchases,
            'is_fraud': is_fraud
        })

    return pd.DataFrame(data)

# 2. Обробка даних
def preprocess_data(df):
    scaler = MinMaxScaler()
    df[['amount', 'play_time', 'purchases']] =
scaler.fit_transform(df[['amount', 'play_time', 'purchases']])
```

```
    # Додавання параметрів для евристичного аналізу
    ip_counts = df['ip_address'].value_counts()
    df['ip_count'] = df['ip_address'].map(ip_counts)

    # Імітація зміни геолокації
    df['location_change'] = np.random.randint(0, 2000,
size=len(df))

    return df

# 3. Статистичний модуль
def statistical_analysis(transaction, mean_amount, std_amount):
    risk_score = 0
    z_score_amount = (transaction['amount'] - mean_amount) /
std_amount
    if z_score_amount > 2:
        risk_score += 30
    return risk_score

# 4. Евристичний модуль
def heuristic_analysis(transaction):
    risk_score = 0
    if transaction['ip_count'] > 5:
        risk_score += 20
    if transaction['location_change'] > 1000:
        risk_score += 25
    return risk_score

# 5. Модуль машинного навчання (k-means)
def train_kmeans(df, n_clusters=5):
    features = df[['amount', 'play_time', 'purchases']]
    kmeans = KMeans(n_clusters=n_clusters, random_state=42)
    df['cluster'] = kmeans.fit_predict(features)

    # Позначення кластерів із високим ризиком
    fraud_clusters =
df[df['is_fraud']]['cluster'].value_counts().index[:2]
    return kmeans, fraud_clusters

def kmeans_predict(transaction, kmeans, fraud_clusters):
    # Pass a DataFrame to retain feature names
    features = pd.DataFrame([transaction[['amount', 'play_time',
'purchases']]],
                            columns=['amount', 'play_time',
'purchases'])
    cluster = kmeans.predict(features)[0]
    return 25 if cluster in fraud_clusters else 0

# 6. Інтегрована функція оцінки ризиків
def assess_transaction_risk(transaction, mean_amount, std_amount,
kmeans, fraud_clusters):
    risk_score = 0
```

```
    risk_score += statistical_analysis(transaction, mean_amount,
std_amount)
    risk_score += heuristic_analysis(transaction)
    risk_score += kmeans_predict(transaction, kmeans,
fraud_clusters)

    return min(risk_score, 100)

# 7. Візуалізація результатів
def visualize_results(df):
    # Гістограма розподілу ризиків
    plt.figure(figsize=(12, 6))
    plt.hist(df[df['is_fraud']]['risk_score'], bins=20,
color='red', alpha=0.5, label='Шахрайські транзакції')
    plt.hist(df[~df['is_fraud']]['risk_score'], bins=20,
color='green', alpha=0.5, label='Легітимні транзакції')
    plt.title('Розподіл ризиків транзакцій', fontsize=14)
    plt.xlabel('Рівень ризику', fontsize=12)
    plt.ylabel('Кількість транзакцій', fontsize=12)
    plt.legend()
    plt.grid(True, alpha=0.3)
    plt.savefig('risk_distribution.png')
    plt.close()

    # Графік кластеризації
    plt.figure(figsize=(12, 6))
    scatter = plt.scatter(df['amount'], df['play_time'],
c=df['cluster'], cmap='viridis', alpha=0.6)
    plt.colorbar(scatter, label='Кластер')
    plt.title('Кластери транзакцій', fontsize=14)
    plt.xlabel('Сума транзакції (нормалізована)', fontsize=12)
    plt.ylabel('Час гри (нормалізований)', fontsize=12)
    plt.grid(True, alpha=0.3)
    plt.savefig('transaction_clusters.png')
    plt.close()

    # Графік розподілу сум транзакцій
    plt.figure(figsize=(12, 6))
    sns.kdeplot(df[df['is_fraud']]['amount'], color='red',
label='Шахрайські транзакції')
    sns.kdeplot(df[~df['is_fraud']]['amount'], color='green',
label='Легітимні транзакції')
    plt.title('Розподіл сум транзакцій', fontsize=14)
    plt.xlabel('Сума транзакції (нормалізована)', fontsize=12)
    plt.ylabel('Щільність', fontsize=12)
    plt.legend()
    plt.grid(True, alpha=0.3)
    plt.savefig('amount_distribution.png')
    plt.close()

    # Графік залежності ризику від часу гри
    plt.figure(figsize=(12, 6))
```

```
    plt.scatter(df[df['is_fraud']]['play_time'],
df[df['is_fraud']]['risk_score'],
                color='red', alpha=0.5, label='Шахрайські
транзакції')
    plt.scatter(df[~df['is_fraud']]['play_time'],
df[~df['is_fraud']]['risk_score'],
                color='green', alpha=0.5, label='Легітимні
транзакції')
    plt.title('Залежність рівня ризику від часу гри', fontsize=14)
    plt.xlabel('Час гри (нормалізований)', fontsize=12)
    plt.ylabel('Рівень ризику', fontsize=12)
    plt.legend()
    plt.grid(True, alpha=0.3)
    plt.savefig('risk_vs_playtime.png')
    plt.close()

# 8. Аналіз результатів
def analyze_results(df):
    total_transactions = len(df)
    fraud_transactions = df['is_fraud'].sum()
    low_risk = len(df[df['risk_score'] <= 30])
    medium_risk = len(df[(df['risk_score'] > 30) &
(df['risk_score'] <= 70)])
    high_risk = len(df[df['risk_score'] > 70])

    fraud_detected = len(df[df['is_fraud'] & (df['risk_score'] >
70)])
    total_fraud = df['is_fraud'].sum()
    false_positives = len(df[~df['is_fraud'] & (df['risk_score'] >
70)])
    total_legit = len(df[~df['is_fraud']])

    accuracy = fraud_detected / total_fraud * 100 if total_fraud >
0 else 0
    false_positive_rate = false_positives / total_legit * 100 if
total_legit > 0 else 0

    print("\n=== Аналіз результатів ===")
    print(f"Загальна кількість транзакцій: {total_transactions}")
    print(f"Кількість шахрайських транзакцій: {fraud_transactions}
({fraud_transactions/total_transactions*100:.2f}%)")
    print(f"\nРозподіл транзакцій за рівнем ризику:")
    print(f"- Низький ризик (0-30): {low_risk}
({low_risk/total_transactions*100:.2f}%)")
    print(f"- Середній ризик (31-70): {medium_risk}
({medium_risk/total_transactions*100:.2f}%)")
    print(f"- Високий ризик (71-100): {high_risk}
({high_risk/total_transactions*100:.2f}%)")
    print(f"\nЕфективність моделі:")
    print(f"- Точність виявлення шахрайських транзакцій:
{accuracy:.2f}%")
    print(f"- Хибнопозитивні результати:
{false_positive_rate:.2f}%")
```

```
    print("\nКластери транзакцій:")
    for cluster in df['cluster'].unique():
        cluster_size = len(df[df['cluster'] == cluster])
        cluster_fraud = len(df[(df['cluster'] == cluster) &
df['is_fraud']])
        print(f"- Кластер {cluster}: {cluster_size} транзакцій,
{cluster_fraud} шахрайських "
              f"({cluster_fraud/cluster_size*100:.2f}%
шахрайських)")

def main():
    print("Запуск моделі оцінки ризиків транзакцій TRAM...")

    # Генерація даних
    print("Генерація синтетичного набору даних...")
    df = generate_synthetic_data()

    # Обробка даних
    print("Обробка даних...")
    df = preprocess_data(df)

    # Обчислення статистичних параметрів
    mean_amount = df['amount'].mean()
    std_amount = df['amount'].std()
    print(f"Середня сума транзакції: {mean_amount:.4f}, Стандартне
відхилення: {std_amount:.4f}")

    # Навчання k-means
    print("Навчання моделі k-means...")
    kmeans, fraud_clusters = train_kmeans(df)
    print(f"Високоризикові кластери: {list(fraud_clusters)}")

    # Оцінка ризиків
    print("Оцінка ризиків для всіх транзакцій...")
    df['risk_score'] = df.apply(
        lambda row: assess_transaction_risk(row, mean_amount,
std_amount, kmeans, fraud_clusters),
        axis=1
    )

    # Аналіз результатів
    analyze_results(df)

    # Візуалізація
    print("Створення візуалізацій...")
    visualize_results(df)

    # Збереження результатів
    df.to_csv('transaction_results.csv', index=False)
    print("\nРезультати збережено в 'transaction_results.csv'")
    print("Візуалізації збережено як:")
    print("- 'risk_distribution.png' (гістограма розподілу
ризиків)")
```

```
    print("- 'transaction_clusters.png' (кластери транзакцій)")
    print("- 'amount_distribution.png' (розподіл сум транзакцій)")
    print("- 'risk_vs_playtime.png' (залежність ризику від часу
гри)")

if __name__ == "__main__":
    main()
```