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
«13» 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: « Методика захисту від мультиакаунтингу в онлайн-ігрових платформах »

Виконавець: студентка IV курсу, групи КБ-41

_____ **Антоніна ЮШКОВА**
(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-41** **Юшковій Антоніні Володимирівні**
(група) (прізвище ім'я по батькові)

Тема кваліфікаційної роботи Методика захисту від мультиакаунтингу в онлайн-ігрових платформах

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

Онлайн-ігрові платформи, API, інтернет шахрайства, цифрова верифікація, мультиакаунти

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно дослідити природу мультиакаунтингу в онлайн-гемблінгу, проаналізувати існуючі методи виявлення шахрайства, обґрунтувати вибір сервісу «Дія» для цифрової верифікації, реалізувати технічну інтеграцію, провести тестування на реальній платформі та оцінити ефективність впровадженого рішення.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Впроваджена інтеграція цифрової ідентифікації користувачів на онлайн-ігровій платформі.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 29 листопада 2024 року

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

Завдання прийняла до виконання _____ (підпис) Антоніна ЮШКОВА (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 – 10.12.2024	*виконано*
2	Аналіз літератури	10.12.2024 – 01.02.2025	*виконано*
3	Обґрунтування вибору рішення	03.02.2025 – 12.03.2025	*виконано*
4	Огляд основних характеристик та класифікацій ігрових онлайн-платформ	17.03.2025 – 28.03.2025	*виконано*
5	Аналіз мультиакаунтингу, як ключового інструмента схем шахрайства	03.04.2025 – 16.04.2025	*виконано*
6	Розробка програмної реалізації інтеграції цифрової ідентифікації користувачів.	21.04.2025 – 02.05.2025	*виконано*
7	Аналіз результатів впровадження інтеграції.	05.05.2025 – 26.05.2025	*виконано*
8	Оформлення пояснювальної записки	27.05.2025 – 27.05.2025	*виконано*
9	Підготовка до захисту кваліфікаційної роботи	28.05.2025 – 13.06.2025	*виконано*

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

Завдання прийняла до виконання _____ (підпис) Антоніна ЮШКОВА (ім'я, прізвище)

Термін подання кваліфікаційної роботи до ЕК 13 червня 2025 року

РЕФЕРАТ

Пояснювальна записка дипломної роботи складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків. Основний текст займає 55 сторінок, включаючи вступ, три розділи дипломної роботи, висновки та список джерел. У пояснювальній записці міститься 10 картинок та 2 додатки. Список використаних джерел містить 20 найменувань і займає 2 сторінки.

Метою роботи є розробка методики виявлення та запобігання мультиакаунтингу на онлайн-ігрових платформах з метою збереження чесності ігрового процесу та мінімізації шахрайства.

Для досягнення зазначеної мети поставлено наступні завдання:

- Дослідити особливості функціонування онлайн-ігрової платформи на прикладі онлайн- казино та відповідну нормативно-правову базу.
- Проаналізувати джерела інформації щодо шахрайства на онлайн-гемблінгових платформах, з акцентом на мультиакаунтинг.
- Визначити вразливості, що дозволяють користувачам здійснювати бонусне шахрайство.
- Ознайомитися з міжнародним досвідом протидії шахрайству в онлайн-гемблінгу.
- Оцінити наявні методи боротьби з мультиакаунтингом та ефективність процедур верифікації користувачів.
- Запропонувати рішення для зменшення або усунення мультиакаунтингу шляхом часткової чи повної інтеграції цифрової ідентифікації користувачів, зокрема через сервіс “Дія”.
- Обґрунтувати переваги та практичну доцільність впровадження запропонованого рішення.

Об’єктом дослідження є онлайн-ігрові платформи як середовище для взаємодії користувачів та здійснення ігрових транзакцій.

Предметом дослідження є методи аутентифікації, поведінкового аналізу користувачів і технічних засобів виявлення ознак мультиакаунтингу.

Практичною цінністю отриманих результатів є програмна реалізація інтеграції цифрової ідентифікації користувачів на онлайн-ігрових платформах.

Ключові слова: мультиакаунт, шахрайство, цифрова ідентифікація, онайлн-платформ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ІПН — Ідентифікаційний податковий номер

КМУ — Кабінет Міністрів України

КРАІЛ — Комісія з регулювання азартних ігор та лотерей

ОС — Операційна система

ПЗ — Програмне забезпечення

СОМ — Єдина система онлайн-моніторингу

ЄС — Європейський Союз

2FA — Two-Factor Authentication (Двофакторна автентифікація)

3DS — 3D Secure (Three-Domain Secure)

AI — Artificial Intelligence (Штучний інтелект)

AML — Anti-Money Laundering (Протидія відмиванню коштів)

API — Application Programming Interface (Інтерфейс прикладного програмування)

ARPU — Average Revenue Per User (Середній дохід на користувача)

AUSTRA — Australian Transaction Reports and Analysis Centre (Австралійський центр звітності та аналізу фінансових транзакцій)

BI — Business Intelligence (Бізнес-аналітика)

CAGR — Compound Annual Growth Rate (Середньорічний темп зростання)

FAQ — Frequently Asked Questions (Часті запитання)

FaceID — Технологія біометричної ідентифікації за обличчям

ID — Identifier (Ідентифікатор)

IP — Internet Protocol (Інтернет-протокол)

JSON — JavaScript Object Notation

KSA — Kansspelautoriteit (Гральний регулятор Нідерландів)

KYC — Know Your Customer (Знай свого клієнта)

MAC — Media Access Control (Адреса керування доступом до середовища)

ML — Machine Learning (Машинне навчання)

NFT — Non-Fungible Token (Незамінний токен)

OTP — One-Time Password (Одноразовий пароль)

PDF — Portable Document Format

PWA — Progressive Web Application (Прогресивний веб додаток)

RNG — Random Number Generator (Генератор випадкових чисел)

RTP — Return to Player (Повернення гравцеві)

URL — Uniform Resource Locator (Уніфікований локатор ресурсу)

UX — User Experience (Користувацький досвід)

VPN — Virtual Private Network (Віртуальна приватна мережа)

ВСТУП

У сучасному цифровому середовищі, де онлайн-гемблінг стрімко набирає популярності, питання безпеки користувачів і чесності гри виходить на перший план. Зростання кількості шахрайських схем вимагає пошуку нових ефективних механізмів ідентифікації, здатних забезпечити прозорість і довіру до платформи.

Актуальність роботи полягає в тому, що мультиакаунтинг залишається однією з наймасштабніших та найскладніших форм шахрайства в онлайн-гемблінгу. З розвитком технологій зловмисники використовують усе більш витончені методи маскування та експлуатації бонусних систем, що створює серйозні фінансові, юридичні та репутаційні ризики для операторів. Існуючі підходи до виявлення дублюючих акаунтів виявляються недостатньо ефективними через обмеженість традиційних технічних засобів. Отже, актуальним є впровадження цифрової верифікації через сервіс “Дія”, як ефективного інструменту боротьби з шахрайством.

На сьогоднішній день, захист ігрової платформи від шахрайських дій є одним з головних пріоритетів у сфері iGaming. І хоча індустрія активно впроваджує інструменти на кшталт IP-фільтрації, device fingerprinting, cookies та поведінкового аналізу, більшість із цих рішень легко обходяться або дають високий рівень хибних спрацьовувань. Саме тому зростає потреба у надійних методах верифікації, які дозволять підтвердити унікальність кожного акаунта ще на етапі реєстрації.

Одним із перспективних рішень є інтеграція з державним сервісом цифрової ідентифікації громадян «Дія», який дозволяє не лише перевірити достовірність особи, але й автоматично блокувати повторні реєстрації на основі ІПН, паспортних даних чи вікових обмежень. Такий підхід забезпечує не лише технічний захист, а й відповідає вимогам відповідальної гри та чинного законодавства.

Тому метою роботи є розробка методики виявлення та запобігання мультиакаунтингу на онлайн-ігрових платформах з метою збереження чесності ігрового процесу та мінімізації шахрайства.

Об’єктом дослідження є онлайн-ігрові платформи

Предметом дослідження є методи верифікації користувачів для запобігання ознак мультиакаунтингу.

Методи дослідження: Аналіз, методи машинного навчання та проведення тестування методики на реальних даних платформи.

РОЗДІЛ 1
КОМПЛЕКСНИЙ АНАЛІЗСЕРЕДОВИЩФУНКЦІОНУВАННЯ ОНЛАЙН-ГЕМБЛІНГУ ТА ЗАГРОЗ ШАХРАЙСТВА

1.1 Загальна характеристика ігрових онлайн-платформ

Ігрова платформа - це комбінація програмного та апаратного забезпечення за допомогою якого користувачі мають доступ до ігрового контенту. Такі платформи є посередником між гравцем і безпосередньо провайдером контенту, що дає змогу користувачам завантажувати, запускати, зберігати та взаємодіяти з іншими гравцями в середині гри тощо.

Ігрові онлайн-платформи є ядром цифрової розважальної індустрії. Вони обслуговують мільйони користувачів щодня та функціонують як високонавантажені інформаційні системи з критичними вимогами до захисту даних, аналітики, ідентифікації та довіри.

Основні типи ігрових онлайн-платформ:

Платформи цифрової дистрибуції відеоігор:

1. Steam;
2. Epic Games Store;
3. GOG, Origin, Ubisoft Connect, Battle.net;
4. Microsoft Store, Mac App Store.

Консольні екосистеми

1. PlayStation Network (PSN);
2. Xbox Live / Game Pass;
3. Nintendo eShop.

Платформи онлайн-казино

1. First Casino;
2. Cosmolot;
3. Slots City;
4. Gorilla;

5. BetKing;
6. Parimatch.

Структура та функціональні можливості

Онлайн-казино - це сайт або спеціальна програма, яка дозволяє грати в азартні ігри в Інтернеті. [1]

1. Інтерфейс користувача (Front-end)

Являє собою веб інтерфейс або мобільний додаток, через який гравець безпосередньо взаємодіє з платформою.

Складається у більшості випадків із: каталогу слотів і ігор, розділу бонусних та кешбек програм, особистого кабінету гравця, історії ставок та поповнень аккаунту, каси та технічну підтримку з ботом або відділом підтримки напряму.

2. Сервери грального контенту

Відповідає за під'єднання ігрових провайдерів до платформі онлайн-казино. У більшості випадків онлайн-казино використовують агрегатори , які забезпечують доступ до сотень і більше слотів від різних студій через один єдиний API.

Будь який провайдер зберігає математичну модель гри на своєму власному сервері коли як клієнт на віході виводить лише анімацію.

3. Бекенд сервер онлайн-казно (Back-office)

Являє собою центральну систему управління, адміністрування та логіки роботи онлайн-казино. Складається із:

- CRM системи для керування користувачами, бонусами, e-mail чи SMS розсилки.
- Система звітності у вигляді аналітики даних ставок, доходів та конверсії.
- Облік транзакцій на продукті (депозити, виведення, бонуси, тощо).
- Управління ризиками у вигляді моніторингу аномалій у іграх.
- Керування лімітами та інструментами самовиключення.

4. Фінансовий модуль

Компонентом взаємодії з платіжними системами (платіжні системи, криптовалюта, ApplePay, GooglePay, терміналами, платіжні термінали самообслуговування, тощо) та виконує:

- прийом депозитів;
- виведення коштів;
- обробка бонусних та реальних рахунків;
- верифікацію платежів та виведення;
- розрахунок вейджеру (умови відіграшу).

5. Модель верифікації та KYC (Know Your Customer)

Платформа має вбудовану систему обробки та перевірки особи за:

- документами (паспорт, водійське посвідчення,свідотство про народження, тощо);
- селфі верифікація;
- перевірка по ІПН;
- інтеграції зі сторонніми сервісами такими як ДІЯ, BankID, тощо.

6. Антифрод системи та система безпеки

Інтеграція автоматизованих систем виявлення підозрілої активності та поведінки користувачів:

- виявлення мультиакаунтів (Cookie, deviceID,IP-аналіз);
- блокування бонусних шахраїв;
- логування та сповіщення про будь які аномалії;
- модулі 3DS, Captcha, GEOIP-обмеження.

7. Модули підтримки користувачів (Customer Support)

- Live-чат напряму з персоналом відділу підтримки або ботом;
- історія звернень ;
- FAQ для всіх користувачів.

8. Маркетинговий модуль (Утримання уваги користувача (user engagement))

- наповнення та регулярне оновлення реферальних програм;

- промокоди, welcome-бонуси, фріспіни;
- Ланцюжок Push-повідомлень, e-mail маркетинг;
- Персональні пропозиції та промо-акції.

9. Система аналітики (BI)

Забезпечує повну глибоку статистику для відстеження життевого циклу гравців на продукті, сегментацію, поведінкові шаблони, ефективність акцій і бонусів та конверсій з усіх джерел трафіку.

Основні функції онлайн-казино

Платформи онлайн-гемблінгу забезпечують повний цикл ведення та обслуговування користувача на платформі від реєстрації до обробки фінансових транзакцій, підтримки та аналізу. Основні функції онлайн-казино можна поділити на умовні блоки, які безперервно взаємодіють одне з одним у режимі реального часу [1].

1. Реєстрація та автентифікація користувача

Базовий функціонал, який забезпечує створення унікального облікового запису та присвоєння йому індивідуального номеру у системі онлайн-казино для кожного гравця. Реєстрація може відбутися за допомогою:

A. номера телефону;
B. e-mail адреси;
C. соціальних мереж;
D. BankID чи інші схожі сервіси.

Після створення аккаунту гравець проходить автентифікацію - через логін та пароль, але дедалі частіше сучасні платформи онлайн-казино впроваджують двофакторну аутентифікацію (2FA) та цифрову ідентифікацію через BankID та ДІЯ.

2. Поповнення рахунку та виведення коштів

Фінансовий функціонал онлайн-казино забезпечує поповнення та виведення коштів через різноманітні платіжні системи: банківські картки, крипто-гаманці, LiqPay, ApplePay, GooglePay тощо.

Також присутні функції:

- Обробка платежів з урахуванням та дотриманням AML-вимог.
- Постійний контроль бонусних та реальних рахунків гравців.
- Облік та зберігання всіх історій транзакцій клієнта у особистому кабінеті.
- Захист за допомогою 3D-secure.

3. Запуск та обробка ігор

Центральний функціонал у забезпеченні доступу безпосередньо до ігрового контерну: слотів, live-ігор, рулеток, карткових ігор, тощо.

Система повинна:

A. надавати доступ до ігор всіх підключених провайдерів;

B. передавати запити до серверів ігрових провайдерів ;

C. зберігати історію результатів та ігрову сесію;

D. забезпечувати коректну роботу механік RTP та RNG.

4. Розрахунок ставок та нарахування виграшів

Цей функціонал працює у режимі реального часу та відповідає за підтвердження результатів обертань, нарахування виграшів, безперешкодному оновленню балансу користувачів та врахування будь яких бонусних обмежень (вейджерів, максимумів, тощо).

5. Система бонусів та лояльності

В онлайн-казино реалізується складна бонусна політика:

- вітальні пакети;
- фріспіни;
- відсутність вейджеру;
- кешбек;
- промокоди;
- VIP-програми;
- тимчасові і сезонні акції.

Функції лояльності зазвичай включають у себе рівні акаунтів користувачів, накопичувальні бали та індивідуальні пропозиції, які або автоматично

формуються та надаються гравцям або присвоюються VIP-менеджерами на основі поведінки та ігрової статистики гравця.

6. Підтримка гравця (Support & Customer Service)

Всі платформи онлайн-казино мають цілодобову онлайн підтримку гравців, яка включає в себе онлайн чат (боти та реальні менеджери з підтримки користувачів), e-mail звернення, Telegram/WhatsApp/Viber-ботів, гаряча лінія підтримки для звичайних та VIP користувачів.

Завдяки цій важливій системі, яка критично впливає на довіру і залученість гравців вдається повернути до 73% гравців, які по якимось причинам перестають грати.

7. Система безпеки та антифрод

Захист гравців та платформи забезпечується з безпосередньою допомогою:

1. Виявлення підозрілої активності та поведінки;
2. Блокування мультиакаунтів;
3. Аналіз логів;
4. Обмеження за допомогою IP/GEO/device;

8. Аналітика та моніторинг.

Внутрішня аналітика дозволяє онлайн казино платформам:

A. Відстежувати поведінку гравців;

B. Виявляти шахрайські схеми;

C. Проводити A/B тестування;

D. Оптимізувати UX;

E. Формувати звітність по доходам, утриманню та ефективності акцій продукту.

Загалом функції онлайн-казино охоплюють не лише сам гральний процесс, але й всі супутні бізнес процеси, що дозволяють платформі ефективно працювати та відповідати вимогам протидії шахрайству.

Види онлайн азартних ігор

Ігрові онлайн платформи, а зокрема онлайн казино, мають широкий спектр представлених азартних ігор. Перелік цих ігор складається з ігор з різним геймплеєм, проте вони мають однаковий сенс. Ці ігри класифікуються за різною механікою, рівнем ризику та можливостями у виграшу [2].

Основні види та категорії найпопулярніших азартних ігор серед гравців по всьому світу:

1. Слоти (Slot Games)

Слотові ігри є найпопулярнішим видом азартних ігор у світі онлайн-казино.

Вони запам’ятовуються простотою, яскравим дизайном та динамікою і великим вибором тем на будь який смак.

Основні характеристики:

A. Барабани та лінії виплат;

B. Наявність бонусних раундів , фріспінів, множників виграшу;

C. Фіксований або прогресивний джекпот;

D. Волатильність (частота та розмір виграшу).

Найпопулярніші приклади слотів: Sugar Rush, Book of Ra, The Dog House, Gates of Olympus, Sun of Egypt, Thunder Coin, Supreme Hot, Crazy Monkey.

2. Настільні ігри (Table Games)

Не менш популярна категорія ігор в онлайн-казино о якої входять класичні казино ігри адаптовані під віртуальний інтерфейс:

- Рулетка (європейська, американська, французька);
- Блекджек;
- Баккара;
- Покер (відеопокер або емуляція живої гри).

У цих іграх важливу роль у прозорості та чесності результатів забезпечує генератор випадкових чисел (RNG).

3. Live-Казино (Live-Casino)

Окрема категорія ігор з можливістю взаємодіяти в реальному часі через відеотрансляцію з живим дилером. Даний тип ігор зацікавлює користувача тим,

що він має зв’язок з живими людьми, а не лише з цифровим форматом гри. Цей тип ігор реалізується через окремих провайдерів, таких як Evolution Gaming, Pragmatic Live, Ezugi тощо.

Фішки Live-Казино:

A. Справжні столи та дилери;

B. Можливість спілкуватись через чат з дилером та іншими гравцями;

C. Жива гра з іншими учасниками;

D. Повна імітація оффлайн-казино.

4. Ігри миттєвого виграшу (Instant Win)

Прості, швидкі ігри, які не потребують ніяких специфічних навичок та підходять для будь якого, рівня ознайомленості з платформою онлайн-казино, гравця.

- Скетч-карти;
- Колесо фортуни;
- Турбоміни (Turbo Mines);
- Краш-ігри (Crash Games).

Таку популярність ігри здобули завдяки своїй короткій тривалості сесії та швидке виведення результатів.

5. Крипто-ігри

Доволі новий вид ігор, який ще не доступний на всіх ігрових онлайн-казино платформах, але стрімко набирає популярність серед молодих гравців.

Дедалі більше казино що працюють на базі блокчейну або приймають ставки в криптовалюті впроваджують такий вид ігор.

1. Provably Fair-ігри (зі 100% прозорістю гри та результатів);
2. Краш-ігри (наприклад Aviator);
3. Ігри з NFT механікою.

Моделі ліцензування та регуляції

Легальна діяльність будь якого онлайн-казино неможлива без отримання відповідної ліцензії, що є офіційним дозволом на проведення азартної діяльності

в інтернеті. Ліцензування виконує функції юридичної легітимації та захисту прав споживачів, встановлюючи правила, обмеження та механізми контролю за діяльністю операторів [3].

Види ліцензій:

1. Локальна (національна) - ліцензія, яка видається регулятором країни в якій зареєстрована онлайн ігрова-платформа і діє лише в її юрисдикції. В Україні це був спочатку КРАІЛ (У зв'язку з набранням чинності постановою Кабінету Міністрів України від 25 березня 2025 року № 336 «Про ліквідацію Комісії з регулювання азартних ігор та лотерей» з 1 квітня 2025 року, КРАІЛ припиняє свою діяльність.) [4], наразі Державне агентство України ПлейСіті (Постанова КМУ від 21 березня 2025 р. № 314 "Про центральний орган виконавчої влади, що реалізує державну політику у сфері організації та проведення азартних ігор та лотерейній сфері") [5].

2. Офшорна - компанія отримує ліцензію зі спрощеними умовами (Кюрасао, Мальта, Гібралтар) для глобальної діяльності або з обмеженим доступом до якихось конкретних країн.

Приклади регуляторів:

- Україна: Державне агентство України ПлейСіті — ліцензування азартних ігор від 21 березня 2025 р, суворі вимоги до KYC/AML [5].
- Мальта: Malta Gaming Authority (MGA) — один із найавторитетніших регуляторів у Європі.
- Кюрасао: менш жорстке регулювання, популярне серед невеликих операторів через нижчі витрати.
- Великобританія: UK Gambling Commission — сувора юрисдикція з високим рівнем захисту прав гравців.

Вимоги до ліцензіатів:

Більшість з ліцензійних режимів включає в себе та передбачає [5]:

- Обов'язкову перевірку всіх користувачів (наявність встановленого законодавством для гри віку особою, верифікація безпосередньо документів для перевірки відповідних параметрів)

- Забезпечення повного захисту персональних даних та фінансової інформації користувачів платформи.
- Обов’язкове використання сертифікованого та ліцензійного ПЗ (гарантії чесності слотів, RNG, тощо).
- Наявність та виконання політик відповідальної гри у поєднанні з можливістю самовиключення гравців.
- Регулярна та безперешкодна фінансова звітність перед регулятором.

1.2 Основні види шахрайства та способи їх реалізації

З розвитком технологій розвиваються і шахрайські схеми та маніпуляції. Такі платформи, як онлайн-казино найбільше стикаються із величезним спектром шахрайських схем щодня. Ці дії не завжди формально порушують правила платформи але тим не менш призводять до значних втрат не тільки з боку платформи а й для операторів. Найнебезпечнішим та фундаментальним шахрайським методом був і залишається мультиакаунтинг, який слугує основою для багатьох інших видів маніпуляцій в онлайн-казино платформах [6].

Експлуатація технічних вразливостей

Окрім поведінкових зловживань і маніпуляцій з боку недобросовісних користувачів онлайн-платформ із бонусами чи балансами, значну загрозу становить експлуатація технічних вразливостей та “дір” у програмному забезпеченні, логіці роботи слотів і механіці збереження стану гри. Ці вразливості дозволяють шахраям обходити ігрові правила, зокрема отримувати необгрунтовані виграші або впливати на хід гри без формального порушення правил з боку користувача [6].

В такі технічні вразливості входять вже розглянуті зловживання збереженим станом гри (Save State Exploit), маніпуляції механікою не-Live рулеткою, помилки в розрахунках коефіцієнтів виплат та повторній запуск бонусних механік слотів. Також сюді відносяться неконтрольоване кешування результатів гри, через використання клієнтами платформ або браузерних версій

слотів, у яких стан гри кешується локально [6]. Це дозволяє створити вразливість на стороні користувача шляхом:

a. Відновлення сесії збереженим станом до програшу.

b. Маніпулювання локальними файлами або скриптами, які повторно запускають виграшну комбінацію.

c. Створення умов для повторного виграшу без взаємодії з серверною логікою онлайн-платформи.

Використання ботів та скриптів

Інструменти для шахрайських активності у вигляді автоматизованих програм - ботів та скриптів, розробляють для обходу системи безпеки, автоматизації рутинних дій або для массового виконання маніпуляцій, які вручну реалізувати користувачу складно або неможливо.

1. Автоматизація мультиакаунтингу

Один із найпопулярніших способів використання автоматизованих бот систем, пов'язаний зі створенням та управлінням десятків або сотень акаунтів одночасно. За допомогою бот-інструментів шахраї:

1. Автоматично реєструють аккаунти (з підставними або вкраденими даними);

2. Активують бонуси;

3. Грають у слоти на мінімальних ставках;

4. Виводять часткові виграші та створюють новий аккаунт у разі блокування.

Цей цикл повторюється до безкінечності щодня і виявлення таких дій ускладнюється підміною IP-адрес, device ID, cookie та user-agent.

2. Сканування слотів на бонусні стани

Спеціальні скрипти, які спеціалізуються на скануванні ігрових слотів, зокрема на виявлення ситуацій накопиченого бонусу, фріспінів у слоті або сприятливу статистику для запуску [7].

Це надає змогу:

1. Заходити одразу у “прогріті” слот;

2. Використовувати бонус-хантинг;

3. Автоматично визначати найвигідніші для гри моменти.

Це максимально знижує ризики втрат для зловмисників і значно збільшує прибуток від такого роду маніпуляцій.

3. Автограй та оптимізація виграшу

Категорія ботів, які імітують поведінку людини, реального користувача але грають без її безпосередньої участі [7]. Основні сценарії включають в себе:

1. Прокручування слотів на мінімальних ставказ для відмивання бонусного вейджеру;

2. Автоматичний вихід при зміні RTP;

3. Перемикання між слотами залежно від результатів сесії;

4. Контроль зміни балансу.

Деякі із просунутих скриптів навіть надають змогу аналізувати історії гри та імітувати “чесну поведінку”, щоб уникнути блокування.

4. Скрипти для обходу обмежень

Окремі види скриптів орієнтовані на обхід технічних та поведінкових обмежень, таких як обмеження кількості IP на один ігровий аккаунт, ліміти на депозити чи бонуси та обмеження кількості пристроїв з активною ігровою сессією [7].

Такі скрипти зачасту інтегрують у парі з антидетект-браузерами, що дозволяє створювати ізольовані середовища з унікальними параметрами браузера, ОС, мови тощо.

Соціальна інженерія та фішинг

У контексті онлайн-ігрової платформи, ці техніки використовуються як для атак безпосередньо на саму платформу, так і для зловживання довірою гравців до продукту, з метою отримання несанкціонованого доступу до їх облікових записів або фінансів [8].

1. Фішінг через сайти “дзеркала” або підроблені

Найпопулярніший спосіб реалізування це створення копії реальної офіційної платформи. Реєструється схожий домен імені але з підміною чи

заміною символів у ньому, для візуальної непомітності, копіюють інтерфейс та заохочують користувачів ввести логін, паролі або платіжні дані. Після збору інформації зловмисники:

a. Заходять на справжній аккаунт користувача;

b. Змінюють реквізити виводу коштів;

c. Виводять або переводять гроші на інші акаунти;

d. Використовують акаунти у подальших шахрайських схемах.

2. Шахрайські схеми з виграшами та “подарунками”

Формують підставні ситуації, в яких користувачу або групі повідомляють про виграш або бонус, однак для його отримання потрібно пройти верифікацію, заповнити анкету або здійснити “технічний платіж” (наприклад в 1 гривню). В результаті чого, зловмисник отримує доступ до даних платіжних карт та облікових записів на платформі.

3. Соціальна інженерія через підтримку або адміністрацію

Зловмисники видають себе за співробітників служби підтримки онлайн-казино в чатах, пошті або мессенджерах. Вони переконують користувача:

a. Надати доступ до особистого кабінету;

b. Надіслати скан паспорту або банківської карти;

c. Встановити “оновлення”, яке на ділі буде у вигляді шкідливого ПЗ;

d. Вказати одноразовий пароль або код підтвердження (OTP).

1.3 Міжнародний досвід боротьби з шахрайством

Міжнародна практика демонструє, що ефективна боротьба з шахрайством можлива лише за умови наявності незалежних регуляторних органів для онлайн-казино платформ, які мають чітко визначити повноваження контролю функцій та механізмів регулювання секцій. У більшості розвинених юрисдикцій гемблінг є строго регульованою на законодавчому рівні сферою, де контроль покладається на державні спеціалізовані органи [9].

Регуляторні органи та їх повноваження

Велика Британія – UK Gambling Commission (UKGC)

UKGC вважається одним із найавторитетніших та найвпливовіших регуляторів у всьому світі. Її повноваження включають ліцензування онлайн та офлайн операторів, перевірка їх фінансової стабільності, аудит ПЗ та RNG, контроль за виконанням стандартів відповідальної гри та накладання штрафів і анулювання ліцензій.

UKGC веде активну боротьбу з шахраями, через впровадження обов’язкової верифікації особи, співпрацю з правоохоронними органами та зобов’язанням операторів використовувати антишахрайські алгоритми на своїх платформах.

Мальта – Malta Gaming Authority (MGA)

MGA видає ліцензії онлайн-казино, які мають міжнародну дію, та здійснює постійний моніторинг діяльності операторів. Її повноваження охоплюють перевірку технічної надійності всіх платформ, контроль бонусних та акційних політик, аудит джерел фінансування компаній, миттєве реагування на скарги від гравців та введення механізмів захисту від мультиакаунтингу. MGA вимагає інтеграції AML-процедур (боротьба з відмиванням коштів) та підтримки прозорої фінансової звітності.

Канада – Alcohol and Gaming Commission of Ontario (AGCO)

AGCO являється канадським провінційним регулятором, що з 2022 року керує ринком онлайн-гемблінгу. Особливістю моделі є створення єдиного ліцензійного простору з державним контролем платіжної інфраструктури. AGCO вимагає повної прозорості гравців (KYC/AML), звітності у режимі реального часу, розкриття алгоритмів розрахунку ставок та впровадження технологій боротьби з скриптами та бот-системами.

Інші приклади:

•Швеція (Spelinspektionen) - зобов'язує обов'язкову реєстрацію у національному реєстрі гравців та централізовану систему самовиключення.

•Італія (ADM) – використання державних серверів логування для кожної транзакції без виключень.

•Нідерланди (KSA) – контроль усієї рекламної політики платформи, суворі обмеження на бонуси та акції, щомісячні звітності операторів.

Усі регуляторні моделі орієнтуються на ідентифікацію гравця, прозорість операцій та впровадження цифрових механізмів контролю для зменшення ризику мультиакаунтингу, бонусних шахрайств та відмивання коштів.

Методи виявлення шахрайства

Метод побудований на розпізнаванні унікальних параметрів пристрою: тип ОС, браузер, роздільна здатність екрану, шрифти, мови, часова зона тощо. Навіть при зміні IP-адреси, зловмисник може були ідентифікваний за “цифровим відбитком” пристрою. [10]

1. Технічні методи ідентифікації користувачів

В цю категорію підпадають технології, що дозволяють розпізнати особу користувача незалежну від його намагань її приховати.

a. Device Fingerprinting;

b. IP/Geo-аналітика;

c. Перевірка cookies та браузерних слідів.

Ці методи гарно працюють проти новачків але легко обходяться досвідченими зловмисниками за допомогою VPN сервісів, антидетект-браузерів і віртуальних машин [10].

2. Поведінковий аналіз і алгоритми на основі штучного інтелекту

Основа складається з аналізу структури ігор, частоти кліків та тривалості ігрових сесії. Виявлення однотипних шаблонів у ставках, реєстраціях та бонусній активності на аккаунтах. ML/AI-платформи, що навчаються на основі великих масивів даних. Цей підхід дозволяє знаходити складні комбінації шахрайств, які складно розпізнати стандартними чи класичними методами і схемами.

3. Використання чорних списків та глобальних БД

Міжнародні регулятори обмінюються інформацією про зловмисників через міжнародні бази даних. Наприклад оператор Британії може отримати

сигнал про гравця, який був заблокований у Швеції чи Італії за мультиакаунтинг. Спільні бази KYC та реєстри самовиключення гравців (GamStop, ROFUS) серед ліцензійних операторів можуть бути корисними у випадках міжнародних масових використання схем шахрайства.

Співпраця між країнами та обмін даними

У контексті глобалізації онлайн-казино, коли користувачі безперешкодно з будь якої точки світу отримують доступ до гральних платформ, міжнародна співпраця стає предметом першочергового значення. Жодна з країн не зможе ефективно протистояти кіберзлочинності та шахрайським схемам у сфері азартних ігор без взаємодії між державними органами, регуляторами та іншими платформами [11].

На сьогодні в світі існують організації які координують зусилля у боротьбі з онлайн-шахрайством:

1. European Gaming and Betting Association (EGBA) - покриває координації між європейськими операторами та сприяє обміну інформації про шахрайські дії.

2. Interpol Cybercrime Directorate - має окремі підрозділи сформовані для протидії та боротьби з фінасовими кібершахрайствами, включаючи азартні ігри.

3. FATF (Financial Action Task Force) - контролює дотримання AML, що тісно пов'язане з виявленням гральних шахрайських схем в онлайн-игрових платформах.

Використання міжнародних технічних стандартів

Для того щоб забезпечити сумісність систем захисту між країнами дедалі більше операторів впроваджують єдині формати логування транзакцій, уніфіковані шаблони поведінкового аналізу та взаємне визнання верифікаційних результатів (через впровадження однакових систем підтвердження документів) [11].

Приклади масштабних шахрайських схем у сфері онлайн-гемблінгу

1. США — Справа LockPoker (2013–2015) - Онлайн-покер-рум LockPoker не виплачував виграші гравцям, накопичивши понад $15 мільйонів боргів. Гравці скаржилися на місяці затримок виплат і відсутність відповіді від адміністрації, наслідками стало припинення діяльності сайту у 2015 році, залишивши тисячі користувачів без коштів та судові позиви проти керівництва [12].

2. Швеція — Масовий мультиакаунтинг і бонус-хантинг (2021) - Після введення суворих обмежень на бонуси для нових гравців багато користувачів почали обходити систему, створюючи мультиакаунти або використовуючи нелегальні сайти, що призвело до масштабного шахрайства. Фінансові втрати досягли $15 000 000, після чого регулятор Spelinspektionen запровадив обов'язкову верифікацію через BankID та посилив нагляд за бонусною політикою платформ [13].

3. Велика Британія — Боти на GGPoker (2020) - На платформі GGPoker виявили гравців, які використовували ботів та вигравали проти реальних гравців, збираючи виграші у неконкурентний спосіб. Фінансові збитки платформи становили $1 100 000, після чого платформа запровадила додаткові інструменти виявлення шахрайства та оновила політику безпеки [14].

4. Філіппіни — Live-казино та змови дилерів (2019) - Співробітники Live-казино (дилери) співпрацювали зі злочинцями, передаючи їм сигнали про карти або результат гри, дозволяючи ставити «всліпу» та вигравати. Фінансові втрати досягли рекордних $20 000 000, внаслідок чого були відправлені за грати понад 20 операторів та до справи були залучені органи міжнародної поліції [15].

5. Австралія — Розслідування проти Sportsbet (2022) - Користувачі створювали підставні акаунти, використовували VPN та технічні прогалини для багаторазового отримання бонусів і обходу лімітів ставок. Фінансові збитки оцінюють у районі $2 300 000. Після втручання AUSTRAC компанія Sportsbet зобов'язалася дотримуватись правил боротьби з відмиванням грошей [16].

1.4 Нормативно-правове регулювання в Україні

Ринок азартних ігор в Україні набирає стрімких обертів в останні роки і продовжує зростати завдяки ухваленню спеціального законодавства, спрямованого на легалізацію азартної діяльності, регулювання та контролю в сфері.

Центральну роль у цьому відіграють профільні закони, урядові постанови, а також зміна регуляторного органу, яка відбулася у березні 2025 року [17].

Законодавча база легалізації онлайн-гемблінгу

Основним законодавчим актом, що регулює діяльність у сфері азартних ігор, є Закон України №768-IX «Про державне регулювання діяльності щодо організації та проведення азартних ігор» [18]. Цей документ встановлює правові засади функціонування ринку гемблінгу, визначає перелік дозволених видів діяльності, вимоги до ліцензування, відповідальність організаторів та учасників.

Відповідно до Статті 2 Закону, дозволеними є такі форми азартних ігор:

1. Казино у гральних закладах;
2. Казино в мережі Інтернет;
3. Букмекерська діяльність;
4. Ігрові автомати;
5. Онлайн-покер.

Також визначено вимоги до віку гравців, механізми захисту прав споживачів, фінансові умови ведення бізнесу, включаючи податкові аспекти. Доповненням до закону є Постанова КМУ №1341 від 21 грудня 2020 року, яка затверджує ліцензійні умови діяльності в онлайн-гемблінгу [19].

Повноваження, вимоги та функції ПлейСіті

До 1 квітня 2025 року функції регулятора виконувала КРАІЛ (Комісія з регулювання азартних ігор та лотерей). Однак згідно з Постановою КМУ №336 від 25 березня 2025 року, вона була ліквідована [17].

Новим центральним органом виконавчої влади, що реалізує державну політику у сфері азартних ігор, стало Державне агентство України “ПлейСіті” (Постанова КМУ №314 від 21 березня 2025 р.) [3].

До функцій ПлейСіті належать:

1. ліцензування суб’єктів господарювання у сфері гемблінгу;
2. ведення реєстрів ліцензіатів;
3. здійснення моніторингу дотримання вимог законодавства;
4. взаємодія з правоохоронними органами та розробка нормативних ініціатив.

ПлейСіті також координує діяльність із захисту прав гравців, ведення реєстру самообмежених осіб (лудоманів) та цифрову ідентифікацію [3].

Боротьба з шахрайством та відповідальність за порушення

Законодавство України передбачає низку норм щодо попередження шахрайства та зловживань у сфері азартних ігор. Серед основних напрямів боротьби обов’язкова верифікація користувачів, заборона участі особам до 21 року, вимоги до безпечної гри, фінансовий моніторинг джерел походження коштів та аудит і контроль провайдерів софту.

Порушення ліцензійних умов тягне за собою відповідальність: анулювання ліцензії, штрафи (до 6,5 млн грн), тимчасове блокування платформи. Крім того, передбачено адміністративну та кримінальну відповідальність у разі доведення умисного шахрайства.

1.5 Економічні та соціальні наслідки шахрайств на ігрових онлайн-платформах

Зловмисні дії користувачів та третіх осіб у сфері гемблінгу та безпосередньо у сфері онлайн-казино мають значний економічний та соціальни впливи, які спричиняють втрати, що загрожуть стабільності оператора і в цілому підривають довіру до всієї індустрії.

Економічні втрати для операторів

1. Фінансові збитки від шахрайства з бонусами - схеми з використанням мультиакаунтингу та бонус-хантингом дозволяють шахраям багаторазові використання вітальних бонусів, не приносячі прибутку платформам.

2. Виведення виграшу до відіграшу - через недосконаліть механізму верифікації або вейджерів, на платформах створюється можливість виводу частини коштів з бонусів без виконання умов.

3. Витрати на боротьбу з шахрайством - впровадження систем захисту, верифікаційних сервісів, розробка антифрод-алгоритмів та підтримка команди аналітиків.

4. Ризик штрафів або втрати ліцензії - у випадках невиконання чи не повного дотримання регуляторних вимог або масштабного зловживання з боку гравців.

5. Втрати від експлуатації технічних вразливостей - помилки в механіці ігор або платіжних системах, можуть призводити до некоректних списань, подвоєння ставок тощо.

Соціальні наслідки

1. Підрив довіри гравців, поширення інформації про шахрайства або вразливість, що в результаті знижує лояльність користувачів та репутацію бренду.

2. Зростання лудоманії, через ризик розвитку залежності гравців, які використовують шахрайські схеми, а особливо при заохоченні фейковою інформацією, щодо можливості великих фейкових виграшів [20].

3. Маніпуляція статистикою та рейтингами, через вплив фейкових акаунтів на оцінку ігор, бонусів, рейтингів платформ тощо.

4. Загальне зниження репутації рику, через посилення безпеки і ускладнення проходження процедури для звичайних користувачі (затримка у верифікації, виплатах тощо).

Наслідки для користувачів.

Складнення доступу до платформи - з метою боротьби проти шахрайства, платформи змушені запроваджувати багаторівневу верифікацію, що може затягувати час реєстрації гравця або заблокувати обліковий запис до моменту підтвердження особи. Додаткові перевірки при спробі виведення коштів можуть спричиняти затримку у виплатах і викликати незадоволення серед чесних користувачів.

Масові блокування і підозри - через алгоритми протидії та виявлення мультиакаунтів, можуть помилково блокуватись аккаунти реальних гравці, які не мають відношення до шахрайств але користувались тим самим пристроєм, мережею, що і зловмисники. Гравці можуть потрапити до “чорних списків” без можливості в подальшому довести свою невинуватість, що в майбутньому шкодить репутації платформи та бренду в цілому.

Погіршення умов для гри - через стрімке використання в шахрайських цілях, бонусна політика стає суворішою і оператори обмежують щедрі пропозиції, щоб мінімізувати зловживання, що означає менше акцій та вигідних умов для потенційно нових і постійних гравців.

Зниження довіри до індустрії - поширення шахрайств створює відчуття небезпеки та несправедливості, через що нові користувачі відмовляються від реєстрації або залишають платформу.

Системні наслідки для держави та ринку

Онлайн-шахрайства мають не тільки локальний ефект для операторів чи гравців, а й широкі системні наслідки які напряму пересікаються з державними інтересами, економікою та репутацією ринку.

Зниження надходжень до державного бюджету

Втрати від податків зменшують базу оподаткування через використання мультиакаунтингу або зловживання бонуснох політикою платформ, завдаючи збитків не тільки операторам. Це напряму впливає на надходження до бюджету з урахуванням того, що гемблінг-індустрія є одним із знакових джерел наповнення бюджету. У разі блокування або позбавлення ліцензії операторів, зростає частка нелегального неоподаткованого ринку [2].

Репутаційні ризики для країни. Масове поширення шахрайств створює негативний імідж державного регулювання, навіть якщо формально закони діють. Це ускладнює залучення інвестицій та привабливість українського ринку для міжнародних компаній, через це можна втратити міжнародну довіру у сфері захисту цифрових прав споживачів та протидії кібершахрайству.

Необхідні витрати на державний контроль. Боротися з шахрайством вимушені не тільки самі платформи та оператори, а й державні структури, які витрачають державні ресурси на моніторинг, аудит, розробку нормативно-правової бази та контроль за верифікацією користувачів. Ці навантаження на бюджет та розподілення ресурсів, які могли бути спрямовані на інші державні пріоритетні напрямки.

1.6 Тенденції розвитку онлайн-гемблінгу в Україні та світі

Світовий ринок онлайн-гемблінгу стрімко демонструє зростання, зумовлене рівнем розвитку технологій та зміною ставлення до сфери азартних ігор у багатьох країнах світу. За даними аналітичних компаній, об'єм глобального ринку азартних ігор онлайн зросте до $150 млрд у 2027 році та при цьому сукупний річний темп зростання (CAGR) до 2027 року складе 11,03%, що свідчить про її активну еволюцію [6].

Глобальні тенденції

Масове впровадження мобільного гемблінгу - основний потік онлайн-гемблінгу припадає на мобільні пристрої, зокрема смартфони, тож оператори зосереджують зусилля на розробці мобільних додатків і PWA (Progressive Web Apps) [6].

Впровадження криптовалют і блокчейну - більше платформ дозволяють поповнення і виведення коштів через Bitcoin, Ethereum, USDT та інші криптовалюти, а деякі казино повністю побудовані на технології блокчейн, що забезпечує прозорість розіграшів і неможливість підтасування [6].

Розвиток нішевих ігор та social gambling - зростає популярність казуальних ігор з азартними елементами, які не всюди підпадають під юридичну класифікацію азартних, що формує окремий сегмент соціального гемблінгу (social gambling), гравці витрачають гроші на «фішки», які не конвертуються в реальні виграші [6].

Легалізація та стандартизація

Після легалізації онлайн-гемблінгу в Україні у 2020 році, країна зробила важливий крок до створення прозорого, контрольованого та прибуткового ринку азартних ігор. Ухвалення Закону України №768-IX "Про державне регулювання діяльності щодо організації та проведення азартних ігор" започаткувало правову основу для діяльності онлайн-казино, букмекерів та залів ігрових автоматів.

Ключові моменти легалізації:

1. Визначені на законодавчому рівні види дозволеної діяльності.
2. Запроваджено систему ліцензування з чіткими умовами для операторів платформ.
3. Єдина система онлайн-моніторингу (СОМ), що забезпечує контроль за кожною грою в режимі реального часу.
4. Відповідальність за порушення, зокрема за недотримання вимог AML/KYC, вікового цензу.

Органи регулювання:

До 2025 року функції виконував КРАІЛ, з 1 квітня 2025 року (згідно з Постановою КМУ №336) [17] його повноваження передані новоствореному органу — Державному агентству України "ПлейСіті", згідно з Постановою КМУ №314 від 21.03.2025 [5].

Стандартизація ринку:

1. Всі оператори зобов'язані застосовувати сертифіковане ПЗ, прозорі RNG-системи та провайдерів з ліцензією.
2. Встановлюються єдині вимоги верифікації гравців, боротьби з лудоманією та захисту персональних даних користувачів онлайн-ігрових платформ.

3. Активне впровадження механізму цифрової ідентифікації користувачів на платформах, що підвищить безпеку.

Перспектива для розвитку

Україна має значний потенціал для розвитку онлайн-гемблінгу, враховуючи як внутрішній попит, так і стратегічне географічне розташування. Проте подальше зростання залежить від ефективного регулювання, технологічної модернізації та довіри користувачів.

Очікувані тренди:

1. Поглиблення цифрової трансформації - використання е-послуг, біометрії, BankID та сервісів цифрової ідентифікації користувачів для боротьби з шахрайством.

2. Залучення іноземних інвесторів та посилення міждержавної співпраці - за рахунок прозорих правил та конкурентних умов в межах ЄС, для боротьби з транснаціональними шахрайськими схемами.

Складнощі:

1. Проблеми з правозастосуванням, які залишилися після ліквідації КРАІЛ.

2. Високий рівень неформального ринку, особливо через Telegram-казино та недобросовісних операторів.

3. Відсутність судової практики у вирішенні спорів гравець-оператор, що гальмує розвиток правової культури в цій сфері.

Висновок до розділу 1

У першому розділі було здійснено ґрунтовний аналіз ігрових онлайн-платформ, зокрема їх структури, функціоналу, типів ігор, моделей ліцензування та регулювання, а також основних видів шахрайства, що загрожують стабільності функціонування онлайн-казино.

Окрему увагу приділено технічним та організаційним заходам, які забезпечують легальність, безпеку та безперебійну роботу гемблінг-платформ.

Аналіз показав, що системи KYC/AML, модулі антифроду та цифрової ідентифікації стали ключовими бар’єрами на шляху до зловживань і маніпуляцій. Також, розглянуті приклади експлуатації вразливостей програмного забезпечення та використання ботів засвідчили високий рівень ризиків для операторів і споживачів.

Проаналізовано міжнародну практику протидії шахрайству, з акцентом на важливість міждержавної координації, використання глобальних баз даних, стандартів поведінкової аналітики та правових механізмів. Ефективна боротьба з шахрайством вимагає комплексного підходу в поєднанні технологічних рішень, законодавчого регулювання та прозорих процедур.

РОЗДІЛ 2 МУЛЬТИАКАУНТИНГ, ЯК КЛЮЧОВИЙ ІНСТРУМЕНТ СХЕМ ШАХРАЙСТВА

2.1. Мультиакаунтинг, як основа шахрайських схем, специфіка в iGaming

Мультиаккаунтинг - це створення та використання двох та більше облікових записів на одній і тій самій платформі однією фізичною особою з метою обходжень певних обмежень, багаторазової чи повторної участі у бонусних програмах або задля маніпулювання внутрішніми механіками гри. Мультиаккаунтинг у сфері iGaming є не лише окремою загрозою , а й фундаментом для десятків інших схем, таких як бонусне шахрайство, ухилення від блокування облікового запису, повторна участь у розіграшах платформи та координації шахрайської “командної гри”. Такий підхід створює можливість уникнення стандартних фільтрів безпеки платформ і шкодить їм із фінансової та репутаційної сторін [8].

Мотиви використання кількох акаунтів

Існує декілька фундаментальних причин для використання мультиакаунтів з боку недобросовісних користувачів платформ**.**

1. Більшість платформ для заохочення нових гравців використовує акційні пропозиції та бонуси. Мультиаккаунтинг ж дозволяє користувачу отримати повторно усі можливі пропозиції, такі як welcome-бонус, фріспіни, бездепозитні бонуси тощо, за допомогою створення нових акаунтів.

2. З’являється можливість уникати обмежень на ставки чи загальний виграш, які часто обмежують для одного аккаунту, розподіляючи активність між декількома акаунтами.

3. Обходити блокування - після блокування основного аккаунту за підозрілу чи шахрайську активність, користувачі просто створюють новий аккаунт з тими самими намірами.

4. У більшості платформ діє схема, в якій один аккаунт має право на одноразову можливість участі у турнірі, щоб підвищити шанси на виграш, шахраї використовують мультиакаунтинг, бо чим більше акаунтів у турнірній таблиці від одного користувача - тим більший його шанс на перемогу у вибраному турнірі.

5. За допомогою великої кількості акаунті, зловмисники щоденно та щотижнево виносять з платформи одноразові кешбеки,“daily та weekly gifts”, через що платформа несе значні збитки та результативність і вигідність таких програм для операторів не виправдовує себе.

Технічні способи реалізації мультиакаунтингу

Обходження стандартних систем захисту від мультиакаунтингу значно ускладнено через широкий спектр технічних засобів, які шахраї використовують для маскування. Через збільшення доступності цих методів, багатократне обходження механізмів захисту платформ стає набагато простішим і популярнішим [8].

1. Використання VPN (Virtual Private Network) та проксі для зміни IP-адреси, при переключенні між аккаунтами, стало найпопулярнішим методом обходу географічної фільтрації онлайн-платформ, що унеможливлює виявлення дубльованих акаунтів користувачів.

2. Антидетект-браузери, які дозволяють імітувати не лише унікальний пристрій (User-Agent), а й вцілому параметри екрану, мови, часову зону та інші персональні характеристики. (AdsPower Global, Dolphin Antiy, Indigo Browser та інші).

3. Віртуальні машини або емулятори (VirtualBox, VMware, LDPlayer, BlueStacks) для створення “нового” пристрою в очах платформи, що унеможливлює детектування за MAC-адресою, встановленими програмами чи ОС.

4. Підроблені або вкрадені особисті дані, включаючи тимчасові або віртуальні телефонні номери, одноразові платформи для створення та використання в подальшому для шахрайських дій адреси електронної пошти,

купівля чужих документів (часто з даркнету) та загалом випадки підробок особистих даних.

Організація мультиакаунтингу в умовах командної гри

Схема використання мультиакаунтингу серед зловмисної частки користувачів онлайн-платформ зачасту не буває поодинокими, а являє собою систему діяльності організованими групами та деколи цілими шахрайськими угрупуваннями, задля масштабування неправомірних дій і обходження внутрішніх лімітів платформ та безперервності своїх атак [7].

1. Командна структура

Організовані зловмисні угрупування включають у себе різнопрофільних спеціалістів зі своїми зонами відповідальності.

a. Технічні спеціалісти - робота з інфраструктурою (антидетект-браузери, VPN, емулятори).

b. Оператори акаунтів - створення та подальше ведення акаунтів, ігрова активність та активація бонусів.

c. Логісти - підбір платіжних систем, карток, електронних гаманців для виводу коштів з акаунтів.

d. Верифікатори - спеціалізація на проходженні та обходженні системи KYC, використовуючи фейкові чи підроблені документи.

e. Куратори - координація загальної активності та планування і вибір онлайн-казино платформ та ігор.

2. Масштабування за рахунок “ферм” акаунтів

Такі угрупування можуть керувати десятками і сотнями акаунтів, створюючи спеціальзовані “ферми фармінгу” акаунтів (account farming).

Поділ акаунтів відбувається на основі IP-локацій, платіжних інструментів та типів пристроїв. Кожен акаунт має свій технічний слід, який був заздалегідь продуманий сценарієм кураторів угруповань за конкретними параметрами [7].

3. Вивід коштів та відмивання

Безпосередній ключовий етап цих схем зазвичай продуманий до найменших деталей, у вигляді:

a. Використання електронних гаманців (Skrill, Jeton, Binance Pay тощо), які заздалегідь оформлені на фейкові особи.

b. Перекази на акаунти підставних осіб чи за допомогою криптовалютних бірж.

c. Застосування “дроблення” виграшу, для уникнення цілеспрямованої уваги сервісів і служб безпеки та лімітів виводу онлайн-платформ.

Прямі та опосередковані загрози для казино

Наслідки мультиаккаунтів для операторів включають у себе фінансові збитки через зловживання бонусів та промоакцій, особливо у разі великого відсотку мультиаккаунтів на платформі, збої в аналітиці реальної кількості користувачів платформи, порушення умов ліцензування через вимоги точного обліку KYC та зниження довіри до систему з боку чесних користувачів.

Наслідки мультиакаунтингу завдають прямому ризику онлайн-казино платформам і виходять набагато далі ніж приклад простого повторного використання бонусів. Платформа несе системні наслідки функціонуванню, зниження чи знищення репутації, глобальні фінансові втрати та юридичну відповідальність [7].

Прямі збитки:

Через можливість створення мультиакантів та багаторазового отримання бонусних і акційних програм користувачами, платформа спонсорує шахрайську активність і несе безпосередні втрати коштів. Це стає особливо критичним у проявах бездепозитних бонусів та з акційними можливостями виводу без відіграшу. Такі акаунти не приносять прибутку в довгостроковій перспективі але потребують при цьому значних втрат на залучення, обслуговування та обробку. Витрати можуть сягати тисяч та навіть мільйонів доларів щомісячно, в залежності від фінансування бонусних програм зі сторони платформи [7].

Опосередковані загрози:

Довгостроковий деструктивний ефект, через аналітичну дезінформацію ключових бізнес-показників, що створюється на базі аналізу всіх акаунтів платформи, більшу частку яких займають мультиакаунти. Це створює ілюзії

залученості гравців, високу активність та хибні висновки зі сторони операторів, щодо моделі партнерських оплат за показниками (Cost Per Action). Втрати через сплату афіліатам за фейкових користувачів підриває бюджети платформ щомісячно без можливості точної фільтрації [7].

Репутаційні наслідки:

У разі витоку використовування шахрайських схем, платформи ризикують втратити репутацію серед афіліатів, баєрів, гравців і насамперед державних регуляторів. У публічному просторі це буде мати колосальні наслідки у вигляді масовості публічних статей та звинуваченню, що унеможливлює спростування навіть при наявності внутрішніх заходів безпеки.

2.2. Шахрайські схеми, засновані на мультиакаунтингу

Мультиакаунтиг - основа реалізацій складних схем зловмисників в сфері онлайн-гемблінгу, ця проблема виходить за межі простої реєстрації декількох акаунтів і створює потужний інструмент заробітку для користувачів та угруповань з неправомірними намірами [7].

Бонусне шахрайство: розширена стратегія “Bonus Hunt”

Зловживання бонусними пропозиціями:

Бонусні програми - це фундаментальний інструмент утримання, заохочення та залучення користувачів на онлайн-казино платформах. Ці програми включають у себе вітальні пакети як для нових так і для існуючих гравців, бездепозитні бонуси, фріспіни, відсутність вейджеру, промоакції, кешбек системи, програми лояльності та акційні пропозиції. Саме через це вони і стають найпопулярнішою мішенню для шахраїв, які використовують різні схеми для отримання неправомірної вигоди.

Сутність зловживання бонусами:

Зловживання бонусами - це свідоме використання акційних та бонусних механік платформи у спосіб, що суперечить їх першочерговому призначенню системою але формально зачасту не порушує правил платформи. Користувачі

створюють або підлаштовують свою поведінку під технічні недосконалості бонусної системи платформи аби отримати неправомірний виграш із мінімальним ризиком втрати аккаунту.

Основні типи бонусних схем:

1. Зловживання вітальним бонусом (Welcome bonus/pack)

Мета - отримати багаторазовий або кількаразовий доступ до бонусу нових користувачів платформи, новий аккаунт = новий бонус.

Ризик для казино - втрата великої кількості бюджету на неісну.чих нових клієнтів.

2. Бонус-Хантинг (Bonus Hunt) з відкладеним запуском бонусів

Гравець активує бонус у слоті, де можна “накопичити” функцію, виходить із гри до її запуску, а потім повертається й грає послідовно в кількох слотах із заготовленими попередньо бонусами.

Ризик для казино - часткове або повне уникнення відіграшу у користувача (відсутність вейджеру).

Практичний приклад шахрайства та комбіновані бонусні атаки:

1. Бонус-хантинг у слоті Solar Queen

У цьому слоті реалізовано механіку накопичувального бонусу. Користувач грає до моменту активації бонусного раунду, після чого виходить із гри не запускаючи останній бонусний раунд. Такі дії дозволяють гравцю:

a. заморозити кілька активних бонусів у різних типових слотах;

b. повернутися пізніше й отримати множинний виграш;

c. використати бонуси після активації депозитного або бездепозитного бонусу;

d. використати для множника бонусний рахунок і повернутись на останній раунд вже використовуючи реальний баланс і отримати виграш на реальній баланс замість бонусного.

Завдяки цьому частина виграшу нараховується вже під час активного бонусу, але до моменту запуску вейджеру, який створює вікно для його часткового виводу або уникнення відіграшу.

2. Відігравання через системну діру гри Aviator

Гравці використовували Aviator, де за умовчанням у більшості казино-платформ діяв автозбір виграшу на коефіцієнті 1,25. Таким чином після запуску бонусу встановлювався автозабір, що допомагало шахраям систематично забирати виграші на мікро коефіцієнтах без великого ризику та відкручувати вейджер стабільно і без втрат. На деяких платформах залишали частину балансу, як реальну, доступну для виводу.

Це довготривала стратегія, яка імітувала повністю чесну гру, але фактично була заснована на механічному, обчисленному підході використовуючи системну дірку.

Свого часу саме цей спосіб завдав масивних втрат у великій кількості онлайн платформ, тому внутрішню механіку гри Aviator було перероблено.

3. Вивід виграшу через незбережені бонуси

Окремі провайдери (наприклад слот Book of Ra) не зберігають стан та статус бонусів після виходу гравцем з гри. Тобто, коли гравець активує бонус, після чого виходить з гри, до його безпосереднього запуску, система не відновлює бонус при повторному вході у гру і виграш нараховується на реальний баланс, оскільки вейджер втрачається.

Ця поведінка використовується систематично у багатьох аккаунтах, що дозволяє отримати виграш без потреби у відіграші перед виводом.

Схеми маніпуляцій балансом та обхід лімітів

1. Виведення часткового виграшу до активації вейджеру

У деяких системах виграш користувача поділяється на бонусний та реальний баланс, якщо виграш системою автоматично не блокується для відіграшу, користувач може вивести його достроково.

Ризик для казино - Фінансові втрати.

2. Зміна слотів для уникнення умов бонусної програми

Платформи зачасту прописують вимоги щодо ставок або конкретних слотів для відіграшу, зловмисники ж грають на так званій “сірій зоні” - це слоти, які технічно не заборонені але мають високий коефіцієнт виграшу.

3. Експлуатація симуляції рулетки

У неліцензійних або технічно не досконалих програмно казино-платформах , що використовують симулятори рулетки існують можливості:

a. Гравець може одночасно зробити ставку як на червоне так і на чорне.

b. Має можливість достроково вийти із гри, не дочекавшись результатів зроблених ставок.

c. У результаті гроші за зроблені ставки можуть бути повернені, але в окремих випадках лише одна частина ставки , а інша не фіксується, що дозволяє уникнути програшу.

Такі дії технічно не фіксуються системою казино за обертання і можуть повторюваться, за допомогою мультиаккаунтингу, одночасно на безлічі облікових записах.

4. Обхід системи в слоті Turbo Mines

В іграх на кшталт Turbo Mines від TurboGames, користувачу відкриваються деякі можливості для обходу системи:

a. Повністю злити реальний баланс у слоті, в якому потенційно складно вибрати для імітації реальної гри.

b. Після чого активувати бонус.

c. Знову зайти у гру, використовуючи бонусний рахунок, та залишити один слот до бонусного виграшу і тільки після цього переключитися на реальний баланс.

d. Добрати виграш на реалний баланс, тим самим мінімізуючи ризик будь яких втрат.

У результаті цього, частина виграшу зараховується “поза системою бонусів”, що дозволяє подальше виведення гравцем коштів без відіграшу.

5. Маніпуляції з балансом та ставками

Окрім популярного зловживання бонусними програмами, однією з поширених форм онлайн шахрайства на платформах онлайн-казино є маніпуляція з балансом та системою внутрішніх ставок. Цей тип дозволяє

користувачам отримати несправедливу перевагу у вигляді обходу системи контролю грошових втрат і виграшів або ж при виводу коштів, при цьому не виконуючи вимог та умов гри.

Такі маніпуляції діляться на декілька категорій:

a. Змішування бонусного та реального балансів

У деяких ігрових онлайн-платформах, які використовують чи працюють на застарілих платвормах з кастомними біліг-системами, існує технічна вразливість, коли система некоректно розділяє бонусні та реальні кошти.

Коли гравець отримує виграш під час бонусної гри, замість того, щоб відіграти вейджер, він переходить у слот без бонусної підтримки (наприклад Turbo Mines). Кошти з бонусного виграшу перетворюються на “реальні”, через те що слот не має механіки відслідковування джерела балансу користувача. Тому після кількох дій гравець успішно виводить свій виграш, обминаючи вимогу відіграшу та отримує замість бонусних - реальні гроші на свій рахунок.

b. Залишкові ставки для обходу блокування

У деяких слотах гравець може залишити незавершену ставку або активну гру (наприклад рулетку чи слот у якому йде відіграш за допомогою фріспінів). Робиться ставка (наприклад на червоне та чорне одночасно) та до завершення раунду гравець достроково виходить із гри.

У залежності від реалізацій механіки, баланс може бути:

- Автоматично повернутий, що надає змогу уникнути програшу;
- Частково заморожений, залишається у сірій зоні;
- Не зафіксований і використовується повторно.

Такі дії вводять в оману механізми контролю ставок та дозволяють гравцю маніпулювати своєю активністю.

c. Вплив на порядок відіграшу (вейджер)

Частина платформ досі не реалізує автоматичний запуск відіграшу з момента виграшу, а активує його лише після зміни слота, завершення бонусної гри чи після оновлення сесії. Цим користуються шахраї виграючи в іграх з активним бонусом, не завершуючи сесію або змінюючи слот без підтримки

бонусів у ньому, після чого виводять кошти “реального” балансу, поки вейджер не активовано.

Маскування через зміну ідентифікаторів та “переносна поведінка”

Масова реалізація мультиакаунтів підвищується завдяки технічному маскуванню, що у сукупності дозволяє успішно приховати пов'язані між собою акаунти від внутрішніх систем безпеки платформ. Існуючі методи боротьби з мультиаккаунтами дуже обмежені та зачасту малоефективні:

1. IP-фільтрація неефективна при використанні користувачем VPN сервісів.

1. Cookies або localStorage легко видаляються вручну користувачем.

2. Пристроєва ідентифікація (device ID) може бути підроблена та скинута.

3. Мобільна аутентифікація (SMS або email) також не гарантує унікальності через можливе використання віртуальних номерів або тимчасової пошти.

Масовий вивід коштів з використанням різних платіжних систем

Завершальний та найбільш критичний етап шахрайських схем на базі мультиакаунтингу, який реалізується після активації бонусів, відіграшу виграшів або ж умов платформи. Для успішного виводу застосовується широкий спектр платіжних інструментів, підібраних під кожен аккаунт.

Ключовий спосіб - це дроблення виграшу між численними акаунтами або гаманцями. Створюється можливість уникати лімітів виводу на платформі, знижувати ризики виявлення підозрілих транзакцій, мінімізувати втрати у випадку блокування конкретних, окремих акаунтів та механічна плутанина аналітики KYC/AML систем, за рахунок розосередження коштів.

Технічними прийомами виводу стає - використання різних електронних платіжних систем з фіктивними чи тимчасовими даними, активне використання віртуальних карток і анонімних крипто гаманців. Також, досвічені шахраї можуть імітувати природну ігрову поведінку гравців, розділяючи великі виграші на дрібні ставки з метою обходу алгоритмів виявлення, використовуючи

однакову суму ставок по колу, чергуючи слоти, щоб система не ідентифікувала монотонну гру і акаунт у подальшому не привертав уваши служб безпеки.

Така модель стає високорівневою шахрайською схемою для відмивання коштів, яка значно ускладнює можливість виявлення та притягнення до відповідальності.

2.3. Обмеження існуючих методів виявлення мультиакаунтів

Не дивлячись на наявність широкого спектру технічних засобів боротьби з мультиакаунтами, більшість представленних традиційних методів мають суттєві обмеження, що дозволяє їх безперешкодно обходити. Успішне виявлення та подальше ліквідування дублюючих акаунтів потребує комплексного поєднання кількох джерел даних, але і це не може гарантувати 100% результат.

IP-адреса та геолокація, як критерій виявлення

Використання IP-адреси та фізичного розташування є класичним інструментом у виявленні паралельної активності в одній мережі але широка доступність VPN унеможливлює точне визначення місця користувача, можливість легко змінювати IP-адресу призводить до недостовірної прив’язки місцезнаходження користувача.

Використання відбитку пристрою, cookies та localStorage

Цифровий відбиток, який часто використовують у системах і включає у себе дані про роздільну здатність екрану, мову, версію браузера та ОС, встановлені шрифти, плагіни та час не мають ваги проти антидетект-браузерів з їх можливістю змінювати або рандомізувати ці параметри, Cookies та LocalStorage, що легко очищаються або блокуються та віртуальних машин з можливістю створення нового унікального “відбитку”.

Поведінкова аналітика (behavioral analysis)

Поведінкова аналітика базується на моніторингу дій користувача і є перспективною але:

1. Не працює проти сценаріїв із копійованими поведінковими шаблонами або скриптовими емулюваннями.

2. Не працює проти навчанної групи операторів, які симулюють “природну поведінку”.

3. Не працює у великих масштабах, через складність обчислювальних ресурсів і можливість помилкових спрацювань.

Модерація акаунтів вручну

Ручна перевірка залишається найнадійнішим але у той самий час і найдорожчим способом боротьби з мультиакаунтами. Хоч ручна модерація допомагає більш ефективно виявити типові шахрайства за допомогою логів, схожих ігор, аналізу історії платежів та прив’язаних даних але вимагає натомість великого штату персоналу модераторів.

Створюється проблема неможливості масштабувати цей спосіб під платформи з тисячами нових користувачів щодня і може спричинити конфлікти з реальними гравцями, через помилкові блокування [8].

2.4. Цифрова верифікація за допомогою сервісу “Дія”

Після аналізу масштабного поширення мультиакаунтингу та шахрайських схем, побудованих на цьому в онлайн-гемблінгу, можно зробити висновок, що традиційні методи перевірки особи не мають колишньої ефективності.

Перспективним рішенням стає введення цифрової верифікації особи через державні інструменти, зокрема український застосунок “ДІЯ”, який має перспективу зменшити чи повністю позбавити онлайн-платформи обсягів шахрайств побудованих на мультиакаунтах, та забезпечити прозорість KYC-процесів.

Необхідність переходу до нових інструментів ідентифікації

Як вже було зазначено та доведено, класичні методи ідентифікації користувачів більше не гарантують унікальності акаунту. Через що система KYC, яка не має державного бекенду, стає легкою мішенню для шахраїв і

виникає потреба у використанні державних реєстрів для перевірки особи, автоматизованого підтвердження віку та ІПН та неможливості повторного використання одних і тих самих документів на різні акаунти з подальшим їх блокуванням на платформі.

Можливості та переваги сервісу

Застосунок “ДІЯ” дає змогу платформам отримати швидкий доступ до:

1. Перевірки особистості за допомогою Державного реєстру фізичних осіб без можливості підробки документів.
2. Підтвердження віку для запобігання неповнолітніх гравців на платформі.
3. Унікальності користувача, один акаунт = один ІПН/Паспорт.
4. Безпеки персональних даних, через здійснення обміну за допомогою захищених каналів з логуванням.
5. Простоти у використанні гравцем, підтвердження у декілька кліків без завантажень документів та сканів.

Технічні аспекти інтеграції

Реалізація інтеграції вимагає:

1. Створення REST API або Webhook-механізму, який ініціює запит на верифікацію.
2. Генерації callback URL для прийому результату перевірки.
3. Дешифрування отриманих даних та їх валідації (перевірка ІПН, віку, ПІБ).
4. Внесення обмежень на реєстрацію чи блокування при повторному використанні даних.
5. Логування процесу та журналу відмов.

Обмеження та виклики

Не дивлячись на перспективність рішення, цифрова верифікація гравців має певні обмеження:

1. Сервіс “Дія” функціонує виключно для громадян України, тому унеможливлює варіант покриття іноземних гравців.

2. API “Дії” потребує стабільного доступу та резервних механізмів, що може призводити до технічних перебоїв.

3. Невеликі платформи можуть не мати ресурсів на доопрацювання, через великі витрати на інтеграцію.

4. На жаль, поки що не існує нормативного обов’язку використовувати “Дію” як єдине джерело ідентифікації гравців.

Перспективи поширення в iGaming-галузі

Платформи, які першими впровадять цифрову верифікацію користувачів на своїх платформах за допомогою сервісу “ДІЯ”, зможуть підвищити рівень довіри з боку державних регуляторів та гравців, зменшать внутрішні витрати на модерацію акаунтів, захистять себе від можливих санкцій через порушення KYC/AML вимог та отримають конкурентну перевагу завдяки прозорості та безпеці.

З огляду на перспективу законодавчого закріплення цифрової ідентифікації в азартному сегменті, використання сервісу “ДІЯ” може стати стандартом галузі легального онлайн-гемблінгу в Україні.

Висновок до розділу 2

У другому розділі було детально розглянуто мультиакаунтинг, як ключовий інструмент реалізації шахрайських схем на онлайн-платформах. Проаналізовано мотиви зловмисників, технічні способи маскування активності, командну організацію шахрайських угруповань та масштабовані моделі маніпулювання балансами, бонусами і платіжними системами. Показано, що мультиакаунтинг є не просто порушенням політики платформи, а складною системною загрозою, яка завдає прямі фінансові збитки, спотворює аналітику, підриває довіру гравців і створює ризики для регуляторної відповідності.

Особливу увагу приділено аналізу конкретних шахрайських практик: бонусне полювання, симуляція ігрової активності, змішування балансів, використання технічних лазівок у слотах та обхід лімітів виводу коштів. Також

досліджено слабкі сторони традиційних механізмів виявлення мультиакаунтів, зокрема обмеження IP-аналізу, cookies, поведінкової аналітики та ручної модерації.

Розглянута та запропонована цифрова верифікація гравців через сервіс “Дія”, як потенційне рішення проблеми, що відкриває нові можливості для впровадження надійної ідентифікації користувачів та перспективи поширення в рамках українського ринку.

РОЗДІЛ 3
РОЗРОБКА ІНТЕГРАЦІЇ З «ДІЄЮ» ДЛЯ БОРОТЬБИ З МУЛЬТИАКАУНТИНГОМ ТА ОЦІНКА ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ МЕТОДИКИ

3.1. Архітектура та технічна реалізація інтеграції

Інтеграція із сервісом цифрової ідентифікації громадян «Дія» дозволяє забезпечити унікальність кожного акаунта на платформі онлайн-казино та ефективно боротися з мультиакаунтингом на етапі реєстрації.

Основна мета - перевірка достовірності особистих даних користувача за допомогою державного реєстру, а також унеможливлення повторної реєстрації одного користувача під іншими обліковими записами.

Процес ініціюється на стороні користувача — він запускає процедуру ідентифікації (Step 1). Фронтенд передає запит на верифікацію до бекенду (Step 2), який, у свою чергу, генерує унікальну сесію для авторизації через «Дію» (Step 3). Дія створює тимчасове посилання на підтвердження особи (Step 4), що повертається до фронтенду (Step 5).

На цьому етапі користувач відкриває мобільний застосунок «Дія» для проходження верифікації користувача. А саме він підлягає процесу біометричної перевірки (розпізнавання обличчя), погоджується на передачу даних або відхиляє запит (Step 6).

Якщо погоджено — відбувається шифрування особистих документів (Step 7), генерація посилання на ці дані (Step 8) і передача на бекенд системи казино через callback (Step 9).

На сервері документи розшифровуються і передаються у верифікаційний модуль для подальшої перевірки (Step 10). Загальна архітектура показана на схемі наведеній на рисунку 3.1:

Рисунок 3.1 – Структурна схема архітектури обміну даних між елементами

Step 1: Ініціація верифікації користувачем

На рисунку 3.2 показано процес ініціації користувачем на сайті First для подальшого проходження верифікації, шляхом надання доступу до внутрішнього паспорту через сервіс «ДІЯ».

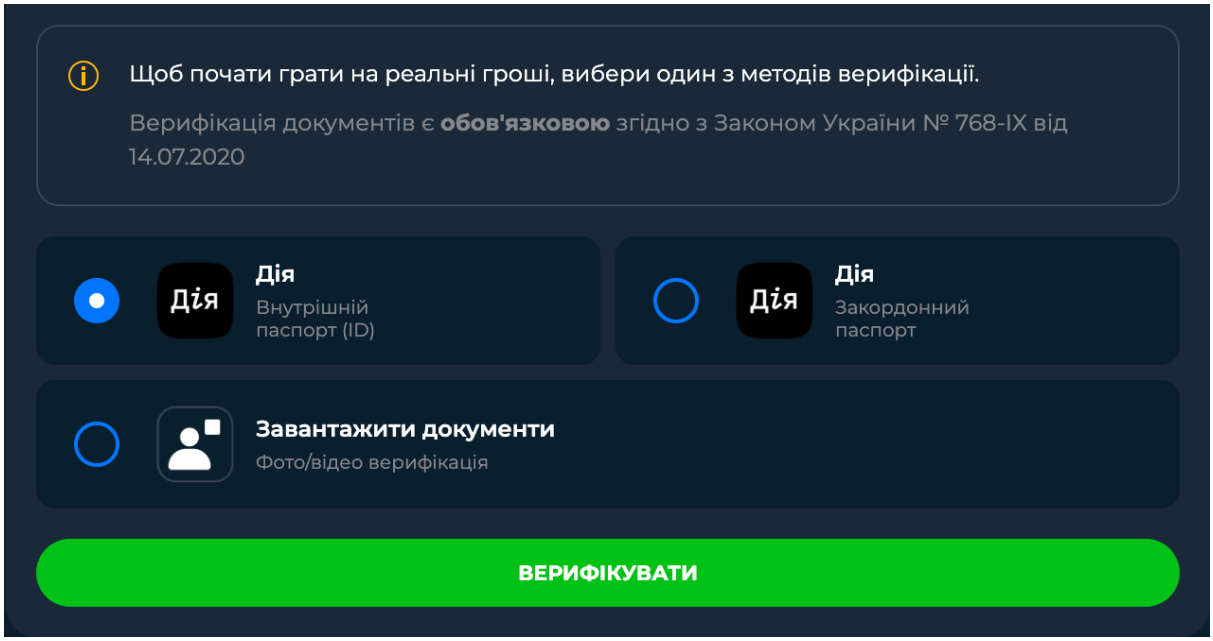

Рисунок 3.2 – Перехід до процесу перевірки особи.

Step 2: Запит на створення верифікації

```
router.get('/identification/diia', async (req, res) => {
    if(!config.diia  !config.diia.is_active  !config.apiDomain) {
        return res.json({ status: false })
    }
```

Перевірка активності конфігурації та доступності API «Дії».

Step 3: Backend створює request_id та отримує посилання

```
const request_id = await diia_lib.createIdentification(req.user);
    if (!request_id) {
      return res.status(500).json({
        status: false,
        errors: {
          diia: 'cannot_create_link'
        }
      })
    }

const redirect_url = await diia_lib.getIdentificationUrl(request_id);
    return res.json({
      status: true,
      type: 'qr',
      data: {
        url: redirect_url,
      }
    })
```

Створення запиту на верифікацію в «Дії» та передача користувачу посилання.

Step 4: DIIA формує посилання на підтвердження

Реалізовано опосередковано: у getIdentificationUrl(request_id) — логіка на стороні бібліотеки diia_lib.

Step 5: Користувач переходить за посиланням, відкриває «Дію»

На рисунках 3.3 – 3.7 показано процес проходження верифікації та надання документів з боку користувача.

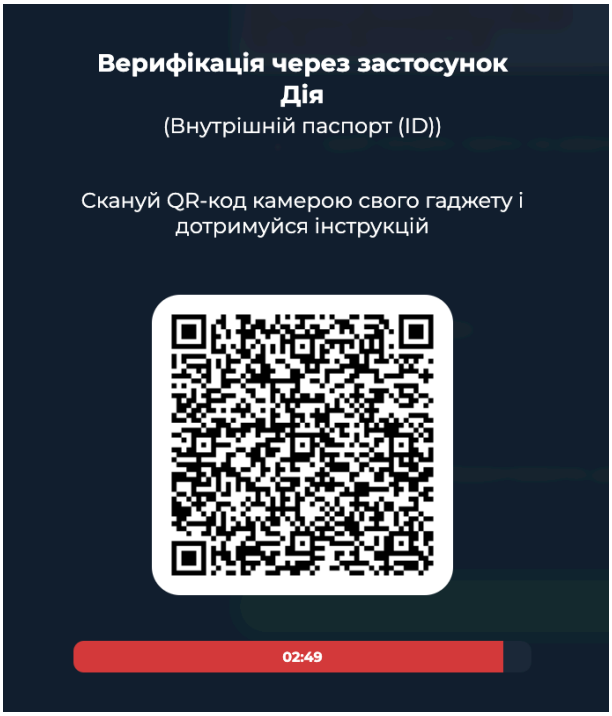

Рисунок 3.3 – Початок процесу перевірки особи.

Step 6: DIIA здійснює FaceID та підписує документи

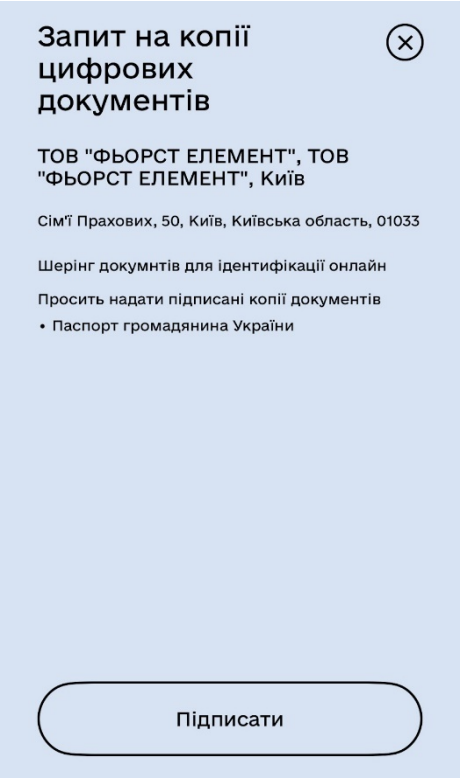

Рисунок 3.4 – Запит на копії цифрових документів всередині застосунку “Дія”.

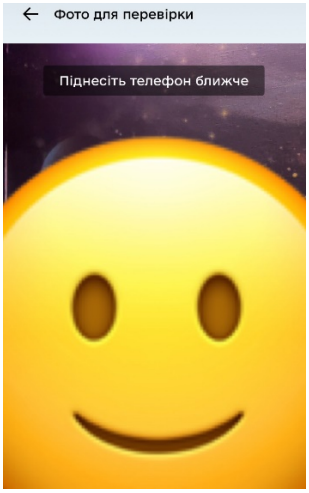

Рисунок 3.5 – Верифікація користувача за допомогою *FaceID*.

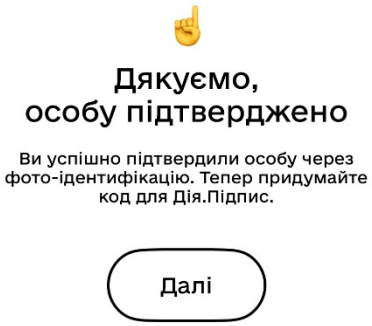

Рисунок 3.6 – Успішне підтвердження особи.

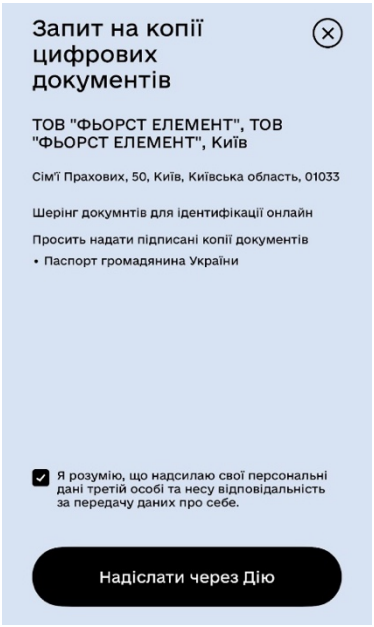

Рисунок 3.7 – Надання документів ідентифікації користувача платформі.

Step 7: Backend отримує зашифровані файли

```
router.post('/process', upload.any(), async (req, res) => {
  if(!req.files.length) {
    console.error('DIIA | Files doest passed')
    return res.json({ status: false })
  }

  req.file = req.files[0]
```

Файли надходять у вигляді req.files, завдяки multer.

Step 8: Backend надсилає файли на розшифрування

```
const [fileDecrypt, jsonDecrypt] = await Promise.all([
```

```
diia_lib.documentDecrypt(
    req.file.buffer,
    request_id,
    path.join(folder, `${code}-decrypted.pdf`)
  ),
  diia_lib.documentDecrypt(
    req.body.encodeData,
    request_id,
    path.join(folder, `${code}-decrypted.json`)
  )
 ])
```

Передача PDF/JSON на розшифрування через diia_lib.documentDecrypt.

Step 9: Backend зчитує, парсить та перевіряє JSON

```
const decryptedEncodedData = fs.readFileSync(path.join(folder, `${code}-decrypted.json`));
  const parsedJSON = JSON.parse(decryptedEncodedData.toString());
  const dockJSON = parsedJSON.data[uploaded_filename][0];
```

На рисунку 3.8 показано, як після успішного проходження перевірок аккаунт верифікується.

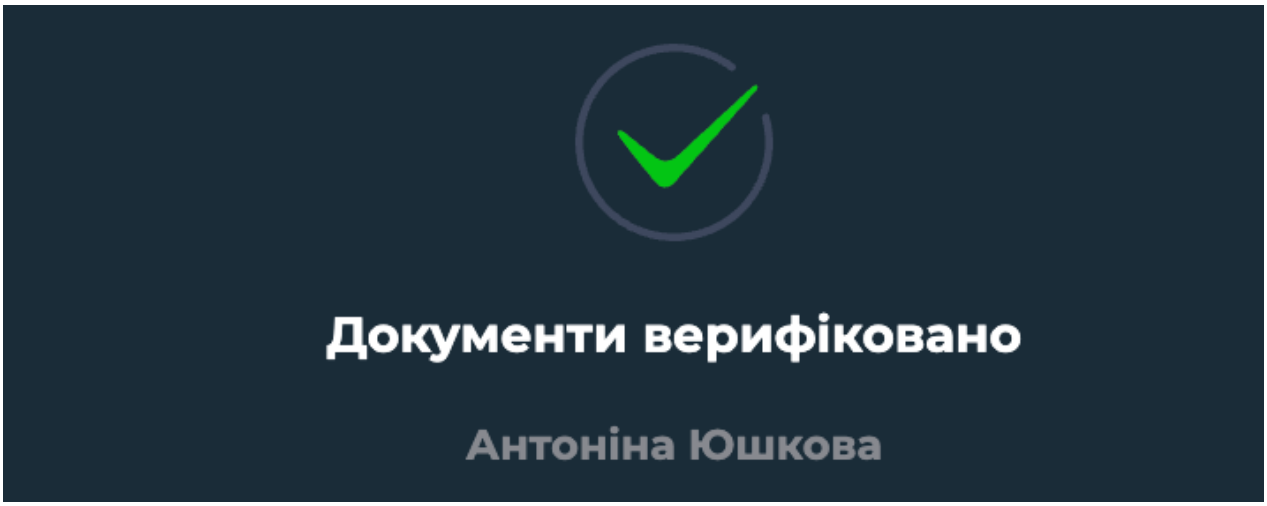

Рисунок 3.8 – Успішна верифікація акаунта користувача на платформі.

3.2. Обробка, збереження та логування отриманих даних

Після підтвердження в Дії система отримує зашифровані документи через callback (етапи 9–10). Приклад одного вигляду наповнення JSON-документу:

{
"taxpayerNumber": "43758634875",
"residenceUA": "УКРАЇНА ЧЕРНІГІВСЬКА ОБЛАСТЬ ПРИЛУЦЬКИЙ РАЙОН С. РУДІВКА ВУЛ. ВИШНЕВА БУД. 6.\nДата реєстрації: 02.02.2010",
"docNumber": "003453474y7",
"genderUA": "Ж",
"nationalityUA": "Україна",
"lastNameUA": "Олійник",
"firstNameUA": "Олена",
"middleNameUA": "Василівна",
"birthday": "01.02.1985",
"birthPlaceUA": "м. Харків",
"issueDate": "19.12.2017",
"expirationDate": "19.12.2027",
"recordNumber": "3534534534-2453454",
"department": "3123",
"genderEN": "F",
"id": "19950801-03985-2017-12-19",
"lastNameEN": "Olena",
"firstNameEN": "Oliynyk",
"fileName": "internal-passport-4a5624e4-b414-4013-986a-60a71116ae5b-12.05.2025, 17:28:55-1.pdf.p7s.p7e"
}

Схожі JSON з реальними даними користувачів використовується у внутрішніх перевірках системи казино після розшифрування.

3.3. Загальна логіка системи та схема прийняття рішень

Після отримання та розшифрування персональних документів через сервіс «Дія». Після того, як ви успішно отримаєте та розшифруєте свої персональні документи за допомогою сервісу «Дія», система автоматично розпочне комплексний процес перевірки. Цей етап є критично важливим для забезпечення безпеки та цілісності вашого акаунта користувача.

Система «Дія» проводить серію логічних перевірок, що охоплюють різні аспекти отриманих даних. Це включає, але не обмежується:

Перевіркою достовірності: Система звіряє отримані дані з наявними державними реєстрами, щоб переконатися в їхній актуальності та відповідності офіційним записам.

Аналізом цілісності даних: Проводиться перевірка на наявність будь-яких пошкоджень або модифікацій у переданих документах.

Виявленням аномалій: Застосовуються алгоритми для виявлення підозрілої активності або невідповідностей, які можуть вказувати на спроби шахрайства або несанкціонованого доступу.

Перевіркою відповідності вимогам: Система перевіряє, чи відповідають отримані документи встановленим стандартам та вимогам, необхідним для подальшої роботи з акаунтом.

На основі результатів цих перевірок система «Дія» визначає подальшу долю вашого акаунта.

Це може включати:

- Повне підтвердження та активацію;
- Запит на додаткову інформацію;
- Тимчасове блокування або призупинення;
- Відмова в активації.

Цей автоматизований процес гарантує, що лише верифіковані та автентичні дані використовуються для роботи з вашим акаунтом у «Дії», забезпечуючи високий рівень безпеки та надійності сервісу.

Механізм прийняття рішень реалізований у вигляді послідовних умовних операторів (if), кожен з яких відповідає за окремий критерій відсіювання. Загальна схема прийняття рішень показана на рисунку 3.9 нижче:

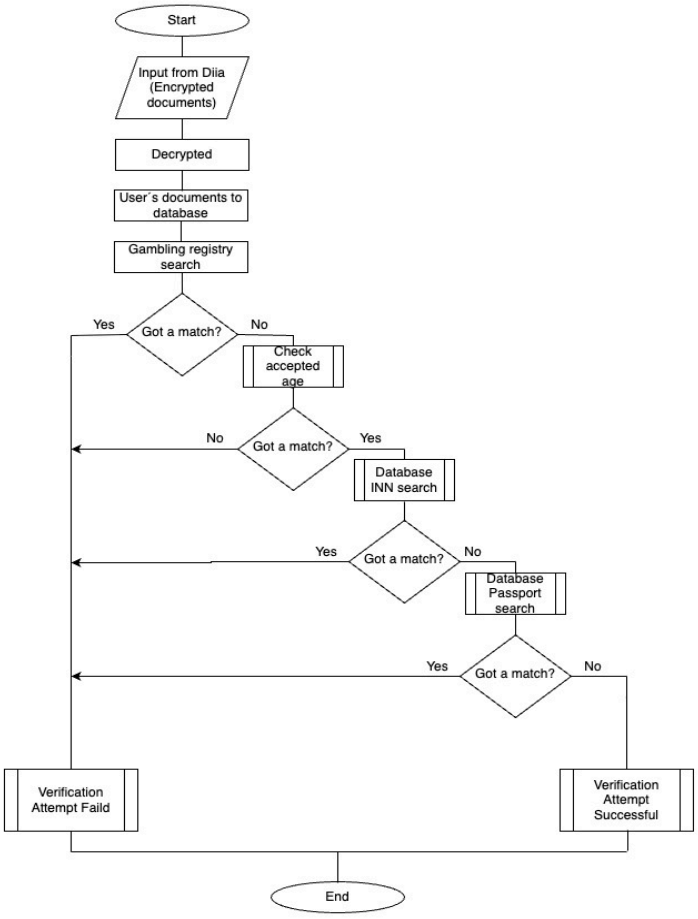

Рисунок 3.9 – Схема перевірки та фільтрації користувачів.

Step 10: Верифікація та фільтрація користувача

1. Перевірка вікових обмежень

Якщо дата народження користувача підтверджує, що йому менше 21 року, акаунт автоматично блокується.

```
if(moment(dockJSON.birthday, 'DD.MM.YYYY').isAfter(ago21years)) {
  user_update.is_active = 0
  user_update.is_blocked = 1
  user_update.disable_comment = 'Вікові обмеження'
}
```

2. Перевірка на лудоманію

Якщо користувач наявний у державному або внутрішньому реєстрі осіб, що мають обмеження до участі в азартних іграх (лудоманія), система одразу блокує акаунт.

Ця перевірка виконується через зовнішній сервіс checkLudoman().

```
const is_ludoman = await user_check_service.checkLudoman(request.user_id)

if(is_ludoman) {
  user_update.is_active = 0
  user_update.is_blocked = 1
  user_update.disable_comment = 'Лудоман'
}
```

3. Перевірка на мультиакаунтинг

Функція documentsMultiaccountsCheck() перевіряє, чи не існує вже акаунтів з таким самим ІПН або номером документа. У разі виявлення — користувача одразу блокують із відповідною поміткою.

```
const is_no_duplicate = await verification.documentsMultiaccountsCheck(request.user_id)

if(is_no_duplicate) {
  user_update.is_active = 0
  user_update.is_blocked = 1
  user_update.disable_comment = 'Мультиакаунт'
}
```

3.4. Дослідження ефективності інтеграції запропонованого рішення

Після впровадження інтеграції з цифровим сервісом «Дія» у квітні 2025 року, платформа онлайн-казино First зафіксувала помітне покращення ключових бізнес-метрик. Порівняльний аналіз періоду січень - травень демонструє суттєву зміну в якості трафіку та монетизації користувачів.

Зокрема, середній чек на одного користувача зріс із 280 грн у січні–лютому до 390 грн у травні. Аналогічну позитивну динаміку показав і ARPU (середній дохід на користувача), який збільшився з 260 - 280 грн на початку року до 390 грн у травні. Це вказує на покращення точності цільової аудиторії та підвищення її платоспроможності після впровадження перевірки особи через «Дію». Також, спостерігається стійке зниження відсотку мультиакаунтів — із 14% у січні до лише 3% у травні після вводу верифікації. Це є прямим підтвердженням ефективності технічного блокування повторних реєстрацій на основі ІПН, паспортних даних і перевірки віку. Ще одним позитивним результатом стало збільшення частки повторних депозитів: з 16 - 18% у перших місяцях року до 35% у травні. Цей показник свідчить про підвищену довіру користувачів до платформи та їхню готовність продовжувати гру після першої взаємодії.

	Reg, #	Reg -> FD	FD, #	Mults,%	ARPU, UAH	Verif & no bet, %
01.06.2025						
01.05.2025	38 243	19%	7 144	3%	905	1,36%
01.04.2025	29 478	19%	5 459	4%	953	1,85%
01.03.2025	30 724	24%	7 520	13%	749	10,24%
01.02.2025	35 733	25%	9 065	15%	981	11,74%
01.01.2025	52 194	24%	12 629	15%	816	10,75%

Рисунок 3.10 Статистики платформи онлайн-казино First до та після інтеграції цифрової ідентифікації.

3.5. Поведінковий аналіз та відгуки користувачів

Користувачі, які проходять верифікацію через «Дію», демонструють вищий рівень залучення.

Після блокування мультиакаунтів, зменшення “порожніх” акаунтів і скорочення кількості анонімних гравців покращилися ключові поведінкові показники - зросли середній дохід на користувача (ARPU), конверсія в депозит та якість першого поповнення.

Разом із тим, впровадження верифікації викликало неоднозначну реакцію з боку частини аудиторії. У квітні 2025 року, одразу після запуску перевірки через «Дію», кількість нових реєстрацій знизилася приблизно на 4%.

Це пояснюється тим, що частина користувачів не мала досвіду роботи з електронними документами або уникала процедури через небажання ділитися персональними даними.

Але вже в травні реєстрації зросли, що не лише компенсувало попереднє падіння, але й перевищило середньомісячний показник з початку року. Це свідчить про те, що користувачі швидко адаптувалися до нової системи, а бар'єр у вигляді цифрової верифікації перестав бути суттєвим.

Зменшення кількості скарг до служби підтримки, стабілізація темпів реєстрацій і позитивна динаміка в ARPU підтверджують, що більшість користувачів сприймає інтеграцію, як частину сучасного, легального та безпечного процесу взаємодії з платформою.

Отримані результати підтверджують ефективність запровадження верифікації через «Дію» для боротьби з мультиакаунтингом і підвищенням якості користувацької бази. Інтеграція не лише підвищила безпеку та прозорість продукту, а й заклала фундамент для довготривалого підвищення ефективності, відповідності регулюванню та зменшення залежності від ручної модерації.

Висновки до розділу 3

У третьому розділі в результаті розробки та впровадження інтеграції з державним сервісом цифрової ідентифікації громадян «Дія» було реалізовано повноцінне технічне рішення для перевірки користувачів на платформі онлайн-казино. Система дозволяє ефективно блокувати мультиакаунтинг завдяки перевірці ІПН, паспортних даних та віку гравця ще на етапі реєстрації. Передача та обробка даних відбувається у повністю автоматизованому режимі через API

«Дії», без участі модераторів, що знижує ризик помилок та прискорює процес верифікації.

Подальший аналіз результатів інтеграції на реальному прикладі онлайн-казино First показав, що запропонована методика не лише технічно працездатна, а й приносить відчутну користь бізнесу. Було зафіксовано покращення ключових метрик: зменшення кількості шахрайських акаунтів, підвищення середнього чека, ARPU та зростання довіри з боку аудиторії. Користувачі адаптувались до нової процедури верифікації, що підтверджує доцільність і потенціал масштабування цього підходу для всієї сфери iGaming та суміжних онлайн-сервісів з високими ризиками шахрайства.

ВИСНОВКИ

На сьогоднішній день проблема шахрайства в онлайн-гемблінгу, зокрема мультиакаунтингу, є надзвичайно актуальною для операторів грального бізнесу. У першому розділі було проаналізовано суть явища мультиакаунтингу, його найпоширеніші форми, такі як бонусне шахрайство, обхід лімітів, техніки маскування, а також методи виявлення подібних порушень. Було виявлено, що традиційні інструменти боротьби з мультиакаунтингом, зокрема IP-ідентифікація чи device fingerprinting, мають обмежену ефективність.

У другому розділі розглянуто існуючі методи виявлення мультиакаунтів та проаналізовано їхні обмеження. Було зроблено висновок, що для вирішення цієї проблеми потрібен новий підхід, заснований на офіційній цифровій ідентифікації користувачів, який унеможливлює повторні реєстрації однією особою.

У третьому розділі було запропоновано та реалізовано інтеграцію з державним сервісом цифрової ідентифікації «Дія». Було створено архітектуру взаємодії, реалізовано бекенд-модуль на Node.js, описано обробку зашифрованих документів, логіку перевірки даних користувача, автоматичну блокування акаунтів у випадку порушень та збереження результатів верифікації. Таким чином, розроблене рішення дозволяє ефективно виявляти та блокувати мультиакаунти ще на етапі реєстрації.

У четвертому розділі було здійснено аналіз впровадження інтеграції на прикладі реального продукту — онлайн-казино First. Було проаналізовано статистику до і після запуску, виявлено покращення ключових показників та зменшення кількості шахрайських акаунтів. Також проаналізовано реакцію користувачів, що підтвердило адаптацію аудиторії до нової системи.

Таким чином, усі поставлені у першому розділі завдання були виконані, а мета дипломної роботи — створення ефективного інструменту боротьби з мультиакаунтингом шляхом цифрової верифікації — була досягнута.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. The Complete Idiot’s Guide to Online Gambling. Alpha Books. URL: https://www.amazon.com/Complete-Idiots-Guide-Online-Gambling/dp/0789722070

2. Online Crime and Internet Gambling. McMullan, J. L. Journal of Gambling Issues, July 2010. URL: https://www.researchgate.net/publication/228385400_Online_crime_and_Internet_gambling

3. Постанова КМУ від 21 березня 2025 р. № 314 "Про центральний орган виконавчої влади, що реалізує державну політику у сфері організації та проведення азартних ігор та лотерейній сфері" URL: https://zakon.rada.gov.ua/laws/show/314-2025-%D0%BF#Text

4. Комісія з регулювання азартних ігор та лотерей. Інформаційне повідомлення від 29.05.2024 «Щодо необхідності верифікації користувачів гральних закладів» URL: https://www.gc.gov.ua/ua/Informatsiini-povidomlennia/35968.html

5. Постанова Кабінету Міністрів України від 12 квітня 2025 р. № 314 «Про внесення змін до деяких постанов Кабінету Міністрів України». URL: https://zakon.rada.gov.ua/laws/show/314-2025-%D0%BF#Text

6. Online Gambling Market Growth Forecast. Asia Gaming Brief, March 2023. URL: https://agbrief.com/news/australia/08/03/2023/online-gambling-market-to-grow-by-150-5-billion-until-2027-report/

7. How To Mitigate Multi-Accounting on Gambling Platforms, 2024 LexisNexis Risk Solutions. URL: https://risk.lexisnexis.com/insights-resources/article/multi-accounting-fraud

8. Kadar T. How to Prevent iGaming Fraud: Its Types, Consequences & Methods, April 2025 URL: https://seon.io/resources/igaming-fraud-prevention/

9. Messenger I. Casino Security and Surveillance. Protecting Assets, Ensuring Safety, and Preventing Fraud., October 2024 URL:

https://www.angusrobertson.com.au/books/casino-security-and-surveillance-ian-messenger/p/9781998376032

10. iGaming Fraud & Compliance Day 2024 https://sumsub.com/igaming-web/

11. Banks J. Online Gambling and Crime Causes, Controls and Controversies, 2014 URL: https://www.routledge.com/Online-Gambling-and-Crime-Causes-Controls-and-Controversies/Banks/p/book/9780367600525?srsltid=AfmBOopqwKPVME-LgxCO0DncEe46Jps_89KdUeisYpQ7Dir9zFg__4PW

12. USA — LockPoker Case (2013–2015). PokerNews. URL: https://www.pokernews.com/news/2025/01/lock-poker-former-ceo-on-the-hook-for-2-2-million-47774.htm

13. Sweden — Bonus Abuse and Unlicensed Sites (2021). iGaming Business. URL: https://igamingbusiness.com/sustainable-gambling/swedes-list-bonuses-as-main-reason-for-using-unlicensed-sites/

14. UK — Use of Poker Bots on GGPoker (2020). TwoPlusTwo Forum. URL: https://forumserver.twoplustwo.com/29/news-views-gossip/detecting-bots-uncovering-insights-ggpoker-data-analysis-1836315/index7.html

15. Philippines — Live Casino Fraud Case (2019). Bloomberg. URL: https://www.bloomberg.com/news/features/2025-01-13/mystery-of-alice-guo-and-how-pogos-unleashed-transnational-crime-in-philippines

16. Australia — Sportsbet and AML Investigation (2022). Reuters. URL: https://www.reuters.com/technology/sportsbet-pledges-comply-with-australias-anti-money-laundering-laws-2024-05-30/

17. Постанова Кабінету Міністрів України від 25 березня 2025 року № 336 «Про ліквідацію Комісії з регулювання азартних ігор та лотерей» з 1 квітня 2025 року URL: https://zakon.rada.gov.ua/laws/show/336-2025-%D0%BF#Text

18. Закон України №768-IX «Про державне регулювання діяльності щодо організації та проведення азартних ігор» URL: https://zakon.rada.gov.ua/laws/show/768-20#Text

19. Постанова Кабінету Міністрів України від 11 листопада 2020 р. № 1341 «Про затвердження Ліцензійних умов провадження діяльності з організації та проведення азартних ігор у мережі Інтернет». URL: https://zakon.rada.gov.ua/laws/show/1341-2020-%D0%BF#n864

20. Griffiths M. Gambling and Gaming Addictions in Adolescence, Mark Griffiths July 2002 URL: https://www.wiley.com/en-us/Gambling+and+Gaming+Addictions+in+Adolescence-p-9781854333483

ДОДАТОК А
ЛІСТІНГ ПРОГРАМНОЇ ІНТЕГРАЦІЇ З СЕРВІСОМ “ДІЯ”

```
//отримання посилання для ідентифікації
router.get('/identification/diia', async (req, res) => {
  if(!config.diia  !config.diia.is_active  !config.apiDomain) {
     return res.json({ status: false })
  }

  try {
    //створення ідентифікаційного запиту
    //отримуємо унікальний ідентифікатор запиту від “Дія”
    const request_id = await diia_lib.createIdentification(req.user);

    if (!request_id) {
      return res.status(500).json({
        status: false,
        errors: {
          diia: 'cannot_create_link'
        }
      })
    }

    //створюємо посилання для перенаправлення користувача для ідентифікації
    const redirect_url = await diia_lib.getIdentificationUrl(request_id);

    //повертаємо посилання для перенаправлення користувачеві
    return res.json({
      status: true,
```

```
      type: 'qr',
      data: {
        url: redirect_url,
      }
    })
  } catch ( err ) {
    return res.status(500).json({
      status: false,
      errors: {
        global: 'server_error'
      }
    })
  }
})Обробка колбеку

//...dependencies

const multer = require('multer');
const upload = multer({ dist: config.files_folder + '/temp' });

const moment = require('moment-timezone')
moment.tz.setDefault('Europe/Kiev')

var router = express.Router();

const SEX = {
  M: 'm',
  F: 'f'
}
```

```
//запрос на отримання
//upload.any() -- middleware для отримання файлов із запиту (multer lib)
router.post('/process', upload.any(), async (req, res) => {
  const badReqException = { status: true };

  if(!req.files.length) {
    console.error('DIIA | Files doest passed')
    return res.json({ status: false })
  }

  req.file = req.files[0]

  //Перевірка типу документа (паспорт або внутрішній паспорт)
  if(!['foreign-passport', 'internal-passport'].includes(req.file.fieldname)) {
    console.error('DIIA | File type doesnt allowed: ', req.file.fieldname)
    return res.json({ status: false })
  }

  //отримуємо ідентифікатор запиту, який створила “Дія”(щоб зв'язати запит з користувачем)
  const request_id = req.headers['x-document-request-trace-id'];

  if(!request_id) {
    console.error(`DIIA | ${moment().format('YYYY-MM-DD HH:mm:ss')} | Request ID is empty`)
    return res.json({ status: false })
  }

  //шукаєм запит в “Дія” в базі даних, щоб зрозуміти, що даний запит дійсно існує і ще не був опрацьован
```

```
        const request = await mongodb().collection('diia_requests').findOne({
requestId: request_id, status: 'new' });

        if(!request) {
          console.error(`DIIA | ${moment().format('YYYY-MM-DD HH:mm:ss')} |
Request ${request_id} not found`)
          return res.json({ status: false })
        }

        //надсилаємо відповідь, що ми отримали файли
        res.json({ "success": true })

        let code = crypto.randomBytes(10).toString('hex');

        try {
          const folder = config.files_folder + '/temp/' + code[0] + '/' + code[1];
          await execSync('mkdir -p ' + folder);

          //відправляємо файли на сервер дешифрування, де лежить декриптор з
ключами дешифрування, які ми отримали при складанні контракту з “Дія”
          const [fileDecrypt, jsonDecrypt] = await Promise.all([
            diia_lib.documentDecrypt(
              req.file.buffer,
              request_id,
              path.join(folder, `${code}-decrypted.pdf`)
            ),
            diia_lib.documentDecrypt(
              req.body.encodeData,
              request_id,
              path.join(folder, `${code}-decrypted.json`)
```

```
      )
    ])

    //перевіряєм, що файли були успішно розшифровані
    if (!fileDecrypt.status || !jsonDecrypt.status) {
      console.error(`DIIA | ${moment().format('YYYY-MM-DD HH:mm:ss')} |
${request_id} | Decrypt error`)
      return res.json({ status: false })
    }

    //читаємо розшифровані файли
    const decryptedDoc = fs.readFileSync(path.join(folder, `${code}-
decrypted.pdf`))
    const decryptedEncodedData = fs.readFileSync(path.join(folder, `${code}-
decrypted.json`));

    //перевіряємо, чи файли успішно прочитано
    if (!decryptedDoc || !decryptedEncodedData){
      console.error(`DIIA | ${moment().format('YYYY-MM-DD HH:mm:ss')} |
${request_id} | Unable read decrypted file`)
      return res.json({ status: false })
    }

    const parsedJSON = JSON.parse(decryptedEncodedData.toString());

    //перевіряємо, чи файли успішно прочитано
    if (
      !parsedJSON ||
      !parsedJSON.data ||
      !parsedJSON.data[uploaded_filename].length ||
```

```
        !parsedJSON.data[uploaded_filename][0]
      ) {
        console.error(`DIIA | ${moment().format('YYYY-MM-DD HH:mm:ss')} |
${request_id} | Cant read parsed file`)
        return res.json({ status: false })
      }

      const dockJSON = parsedJSON.data[uploaded_filename][0];

      //якщо налаштований s3 то відправляємо файли на s3 (s3 - сховище
файлів)
      if (config.document_storage && config.document_storage === 's3') {
        const folder = '/' + code[0] + '/' + code[1];

        let s3_start = new Date().getTime() / 1000
        await awsS3.uploadFile({ data: decryptedDoc },
config.aws.document_bucket_name, code, folder);
        let s3_end = new Date().getTime() / 1000
        logger_lib.log('INFO', 'DIIA (S3)', `Ecexution time: ${s3_end - s3_start}`)
      }let pr_start = new Date().getTime() / 1000

      const dateNow = moment().format('YYYY-MM-DD HH:mm:ss');

      const fileMime = tools.getMimeType(decryptedDoc);
      const fileSize = decryptedDoc.byteLength;

      //добавляємо документ у базу даних
      const to_db_arr = [
        {
          user_id: request.user_id,
```

```
    type: 'passport',
    code,
    name: req.file.fieldname,
    filesize: fileSize,
    mime: fileMime,
    admin_id: 0,
    created_date: dateNow,
    status: 'verified',
  }
];

const values = to_db_arr.map(el => [
  el.user_id,
  el.type,
  el.code,
  el.name,
  el.filesize,
  el.mime,
  el.admin_id,
  el.created_date,
  el.status
]);

let promises = []

promises.push(
  mongodb().collection('user_documents').insertOne(values)
)

const ago21years = moment().subtract(21, 'years').startOf('day');
```

```
//переносимо дані з “Дія” у базу даних
const user_update = {
  updated_date: dateNow,
  name: [dockJSON.firstNameUA, dockJSON.lastNameUA].join(' '),
  firstname: dockJSON.firstNameUA,
  lastname: dockJSON.lastNameUA,
  middlename: dockJSON.middleNameUA,
  sex: SEX[dockJSON.genderEN],
  birthday: moment(dockJSON.birthday, 'DD.MM.YYYY').format('YYYY-
MM-DD'),
  passport: dockJSON.docNumber,
  inn: dockJSON.taxpayerNumber,
  residence_country: dockJSON.nationalityUA,
}

//якщо користувачу менше за 21 рік , то блокуємо його акаунт
if(moment(dockJSON.birthday, 'DD.MM.YYYY').isAfter(ago21years)) {
  user_update.is_active = 0
  user_update.is_blocked = 1
  user_update.disable_comment = Вікові обмеження
}

//оновлюємо користувача у базі даних
promises.push(
  mongodb().collection('users').updateOne(
    { user_id: request.user_id },
    { $set: user_update }
  )
)
```

```
  //логіруємо документ у базі даних
  await mongodb().collection('diia_documents').insertOne({
    user_id: request.user_id,
    dock_data: JSON.stringify(dockJSON),
    created_date: moment().format('YYYY-MM-DD HH:mm:ss')
   })

  //відмічаємо, що запит на верифікацію був виконан
  await  mongodb().collection('diia_requests').updateOne(
    { requestId: request.requestId, status: 'new' },
    {
     $set: {
       status: 'done',
       verification_date: dateNow,
       updated_date: dateNow
     }
    }
   )

  await Promise.all(promises)

  //перевіряємо чи є користувач лудоманом
const is_ludoman = await user_check_service.checkLudoman(request.user_id)

  //якщо так, то блокуємо його аккаунт
  if(is_ludoman) {
   user_update.is_active = 0
   user_update.is_blocked = 1
   user_update.disable_comment = 'Лудоман'
```

```
            await mongodb().collection('users').updateOne(
              { user_id: request.user_id },
              { $set: user_update }
            )
          }

          //перевіряємо користувача на мультиакаунти
          const is_no_duplicate = await
verification.documentsMultiaccountsCheck(request.user_id)

          //якщо є, то блокуємо його аккаунт
          if(is_no_duplicate) {
            user_update.is_active = 0
            user_update.is_blocked = 1
            user_update.disable_comment = 'Мультиакаунт'

            await mongodb().collection('users').updateOne(
              { user_id: request.user_id },
              { $set: user_update }
            )
          }
        } catch (e) {
          console.error('!========= DIIA ERROR: ', e.message);
          return res.json({ status: false })
        }
      });

      module.exports = router;
```

ДОДАТОК Б

ПРИКЛАД СТРУКТУРИ ПЕРСОНАЛЬНИХ ДАНИХ ПІСЛЯ ДЕШИФРУВАННЯ ФАЙЛІВ ВІД СЕРВІСУ «ДІЯ»

{
"taxpayerNumber": "43758634875",
"residenceUA": "УКРАЇНА ЧЕРНІГІВСЬКА ОБЛАСТЬ ПРИЛУЦЬКИЙ РАЙОН С. РУДІВКА ВУЛ. ВИШНЕВА БУД. 6.\nДата реєстрації: 02.02.2010",
"docNumber": "003453474y7",
"genderUA": "Ж",
"nationalityUA": "Україна",
"lastNameUA": "Олійник",
"firstNameUA": "Олена",
"middleNameUA": "Василівна",
"birthday": "01.02.1985",
"birthPlaceUA": "м. Харків",
"issueDate": "19.12.2017",
"expirationDate": "19.12.2027",
"recordNumber": "3534534534-2453454",
"department": "3123",
"genderEN": "F",
"id": "19950801-03985-2017-12-19",
"lastNameEN": "Olena",
"firstNameEN": "Oliynyk",
"fileName": "internal-passport-4a5624e4-b414-4013-986a-60a71116ae5b-12.05.2025, 17:28:55-1.pdf.p7s.p7e"
}