НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

УДК 004.77:339.166.5

ПОГОДЖЕНО
Декан факультету
Інформаційних технологій
_____/ Глазунова О.Г., д.п.н, проф. /
підпис ПІБ, вчене звання і ступінь

«___»_____2024 р.

ДОПУСКАЄТЬСЯ ДО ЗАХИСТУ
Завідувач кафедри
Комп'ютерних систем, мереж та кібербезпеки
_____/ Касаткін Д.Ю., к.п.н., доцент. /
підпис ПІБ, вчене звання і ступінь

«___»_____2024 р.

МАГІСТЕРСЬКА РОБОТА

На тему: «Розробка алгоритму інтелектуальної власності для ігрових систем»

Спеціальність: 123 «Комп’ютерна інженерія»

Освітня програма: Комп’ютерні системи захисту інформації

Керівник дипломного проекту: / Коваленко О. Є. /
підпис ПІБ

Виконав: / Херенков.О.К. /
підпис ПІБ

КИЇВ-2024

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ БІОРЕСУРСІВ
І ПРИРОДОКОРИСТУВАННЯ УКРАЇНИ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

«ЗАТВЕРДЖУЮ»
завідувач кафедри
комп'ютерних систем, мереж та кібербезпеки
_____/ Касаткін Д.Ю., к.п.н., доцент. /
підпис ПІБ, вчене звання і ступінь
«__» _____ 2024 р.

ЗАВДАННЯ

ДО ВИКОНАННЯ МАГІСТЕРСЬКОЇ РОБОТИ СТУДЕНТУ

Хренкова Олександра Костянтиновича
(прізвище, ім'я, по батькові)

Спеціальність (напрям підготовки): 123 «Комп'ютерна інженерія».

Освітня програма: комп'ютерні системи захисту інформації

Тема магістерської роботи: «Розробка алгоритму інтелектуальної власності для ігрових систем »
затверджена наказом ректора НУБІП України від " 1 " листопада 2024 № 1859 "С"
Термін подання завершеної роботи на кафедру _____
Вихідні дані до магістерської роботи: Unreal Engine 5, модулі для інтеграції водяних знаків, генератор QR-кодів, DRM-система з відкритим кодом, текстури та 3D-моделі для тестування, інструмент для аналізу продуктивності (Unreal Insights).

Перелік питань, що підлягають дослідженню:

1. Аналіз сучасних методів захисту інтелектуальної власності в ігровій індустрії.
2. Розробка алгоритму захисту ігрового контенту з використанням водяних знаків, QR-кодів та DRM-систем.
3. Інтеграція та тестування алгоритму на платформі Unreal Engine 5.

Дата видачі завдання " 1 " листопада 2024 р.

Керівник магістерської роботи _____ / Коваленко О. Є.. д.т.н., професор /
(підпис) (ПІБ, вчене звання і ступінь)

Завдання прийняв до виконання _____ / Херенков.О.К /
(підпис) (ПІБ)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Постановка задачі магістерської роботи		Виконано
2	Аналіз предметної області		Виконано
3	Проектування системи		Виконано
4	Реалізація системи		Виконано
5	Тестування розробленої системи		Виконано
6	Оформлення пояснювальної записки		Виконано

Студент _____ / Херенков.О.К /
підпис ПІБ

Керівник проекту (роботи) _____ / Коваленко О. Є. /
підпис ПІБ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

1. ІВ — Інтелектуальна власність
2. IP — Intellectual Property (інтелектуальна власність)
3. SDK — Software Development Kit (комплект для розробки програмного забезпечення)
4. API — Application Programming Interface (інтерфейс прикладного програмування)
5. DRM — Digital Rights Management (управління цифровими правами)
6. AES — Advanced Encryption Standard (стандарт симетричного шифрування)
7. RSA — Rivest-Shamir-Adleman (алгоритм асиметричного шифрування)
8. UI — User Interface (користувацький інтерфейс)
9. UX — User Experience (користувацький досвід)
10. C++ — Мова програмування C++
11. UE5 — Unreal Engine 5 (ігровий рушій п'ятого покоління)
12. 3D — Three-Dimensional (тривимірний)
13. GUI — Graphical User Interface (графічний користувацький інтерфейс)
14. JSON — JavaScript Object Notation (текстовий формат для обміну даними)
15. CPU — Central Processing Unit (центральний процесор)
16. GPU — Graphics Processing Unit (графічний процесор)

ВСТУП

Актуальність проблеми захисту інтелектуальної власності в умовах стрімкого розвитку інформаційних технологій є однією з найбільш обговорюваних тем у сучасному суспільстві. У зв'язку з цифровізацією майже всіх аспектів життя, створення, розповсюдження та захист інтелектуальної власності стали важливими завданнями для розробників програмного забезпечення, у тому числі ігрових систем. Піратство, зловживання авторськими правами та несанкціоноване використання програмних продуктів можуть завдати суттєвих збитків як окремим розробникам, так і великим корпораціям.

В умовах постійно зростаючої кількості цифрового контенту і зростання популярності відеоігор, ефективний захист інтелектуальної власності набуває особливого значення. Ігрова індустрія, яка є однією з найбільш швидко зростаючих галузей економіки, постійно стикається з викликами, пов'язаними з незаконним копіюванням, зломом і розповсюдженням програмного забезпечення. Це створює необхідність у розробці нових підходів та інструментів для захисту цифрового контенту.

У рамках даної магістерської роботи ставиться завдання розробити алгоритм захисту інтелектуальної власності для ігрових систем, який забезпечить надійну охорону контенту від несанкціонованого використання, зберігаючи при цьому високу продуктивність та зручність використання для кінцевого споживача.

МЕТА І ЗАВДАННЯ ДОСЛІДЖЕННЯ

Мета дослідження полягає в розробці ефективного алгоритму захисту інтелектуальної власності для ігрових систем, який забезпечить надійний захист контенту від несанкціонованого використання та сприятиме дотриманню прав авторів і розробників ігрових продуктів.

ОБГРУНТУВАННЯ ТЕМИ

У сучасному світі ігрова індустрія є однією з найбільш динамічно розвиваючихся галузей цифрових технологій. Зростання популярності відеоігор призводить до збільшення обсягів створення унікального контенту, який вимагає надійного захисту від несанкціонованого використання. Це стосується не тільки самого ігрового продукту, але й усіх його складових: графіки, музики, сюжетів, ігрових механік та інших елементів.

Розробка алгоритмів захисту інтелектуальної власності для ігрових систем стає все більш актуальною через збільшення кількості випадків піратства, неправомірного використання ідей та технологій, а також необхідність захисту прав розробників та видавців ігор. Нині існують різні методи захисту інтелектуальної власності, такі як цифрові водяні знаки, шифрування, ліцензійні угоди та інші. Однак, з розвитком технологій, необхідні нові підходи та інноваційні рішення, здатні забезпечити більш високий рівень захисту.

У зв’язку з цим розробка нового алгоритму, що поєднує в собі сучасні технологічні досягнення та відповідає актуальним вимогам законодавства у сфері інтелектуальної власності, є надзвичайно важливим завданням. Такий алгоритм дозволить не тільки зменшити ризики несанкціонованого використання контенту, але й створити більш справедливі умови для розробників ігрових продуктів.

Тема дослідження є актуальною не тільки з точки зору захисту прав інтелектуальної власності, але й з огляду на перспективи розвитку ігрової індустрії в цілому. Тому дана робота має на меті розробку ефективного алгоритму захисту інтелектуальної власності, який відповідав би сучасним викликам та потребам ігрових систем.

1.ОГЛЯД І АНАЛІЗ ПРЕДМЕТНОЇ СФЕРИ

1.1 Кіберзагрози в ігровій ідустрії

Кіберзагрози в ігровій індустрії стають все більш поширеними та складними. З розвитком технологій і зростанням кількості онлайн-ігор, зловмисники отримують нові можливості для атак на інфраструктуру ігор, крадіжки особистих даних та інших форм кіберзлочинів. Це може мати серйозні наслідки як для розробників ігор, так і для гравців, які можуть постраждати від витоку конфіденційної інформації, втрати доступу до акаунтів, фінансових втрат і загального погіршення ігрового досвіду.

Для захисту від таких загроз важливо впроваджувати комплексні заходи безпеки. Одним із ключових методів є шифрування даних. Воно дозволяє захистити ігрові файли, персональні дані користувачів та іншу важливу інформацію від несанкціонованого доступу. Використання надійних алгоритмів шифрування, таких як AES або RSA, допоможе мінімізувати ризики крадіжки даних і зламів.

Іншим важливим елементом захисту є системи багатофакторної аутентифікації. Ця технологія забезпечує додатковий рівень безпеки, вимагаючи від користувачів підтвердження особи за допомогою декількох методів перевірки, таких як паролі, одноразові коди, що надсилаються на мобільні пристрої, або біометричні дані. Така система значно ускладнює зловмисникам можливість отримати доступ до облікових записів гравців.

Регулярні перевірки безпеки є ще одним важливим компонентом у захисті ігрових систем. Вони допомагають виявляти можливі вразливості та швидко усувати їх до того, як ці вразливості будуть використані для атак. Перевірки повинні проводитися як на рівні коду гри, так і на рівні серверної інфраструктури, що обслуговує гру.

Навчання персоналу щодо можливих ризиків також відіграє ключову роль у підтримці безпеки. Розробники, адміністративний персонал і навіть служби підтримки повинні бути ознайомлені з останніми кіберзагрозами і вміти швидко реагувати на будь-які потенційні інциденти. Чим краще підготовлений персонал, тим швидше і ефективніше можна реагувати на можливі атаки.

У сукупності ці заходи допоможуть зменшити ризики і забезпечити надійний захист для всіх учасників ігрової індустрії. В умовах постійного розвитку кіберзагроз і зростання популярності ігрових платформ, впровадження таких заходів є життєво необхідним для збереження довіри користувачів і забезпечення стабільної роботи ігрових сервісів.

DDoS-атаки (Distributed Denial of Service) спрямовані на перевантаження серверів гри шляхом відправлення великої кількості запитів або споживання ресурсоємних операцій з різних джерел. Це створює надмірне навантаження на інфраструктуру сервера, що призводить до його уповільнення або повної недоступності для користувачів. Як наслідок, гравці не можуть підключитися до гри, що викликає збої у багатокористувацьких режимах або навіть повну зупинку ігрового сервісу.

Ці атаки можуть мати серйозні наслідки, особливо для популярних онлайн-ігор, де стабільність сервера є критично важливою для задоволення користувачів. Під час DDoS-атак сервери можуть стати неспроможними обробляти запити легітимних користувачів, що призводить до втрати доступу до гри, переривання ігрових сесій та зниження загального досвіду користувачів.

DDoS-атаки часто використовуються недобросовісними конкурентами або хакерами як інструмент тиску. Вони можуть вимагати гроші в обмін на припинення атаки або створювати негативний імідж гри, що може вплинути на її популярність та фінансові результати. У деяких випадках DDoS-атаки

спрямовані на зрив релізів нових ігор або оновлень, що може мати катастрофічні наслідки для розробників і видавців.

Для запобігання таким атакам компанії використовують різноманітні захисні заходи, такі як балансування навантаження, фільтрація трафіку та інші технології для відсіювання підозрілого трафіку. Однак, навіть із захистом, деякі атаки можуть бути настільки потужними, що повністю уникнути їхніх наслідків стає складно.

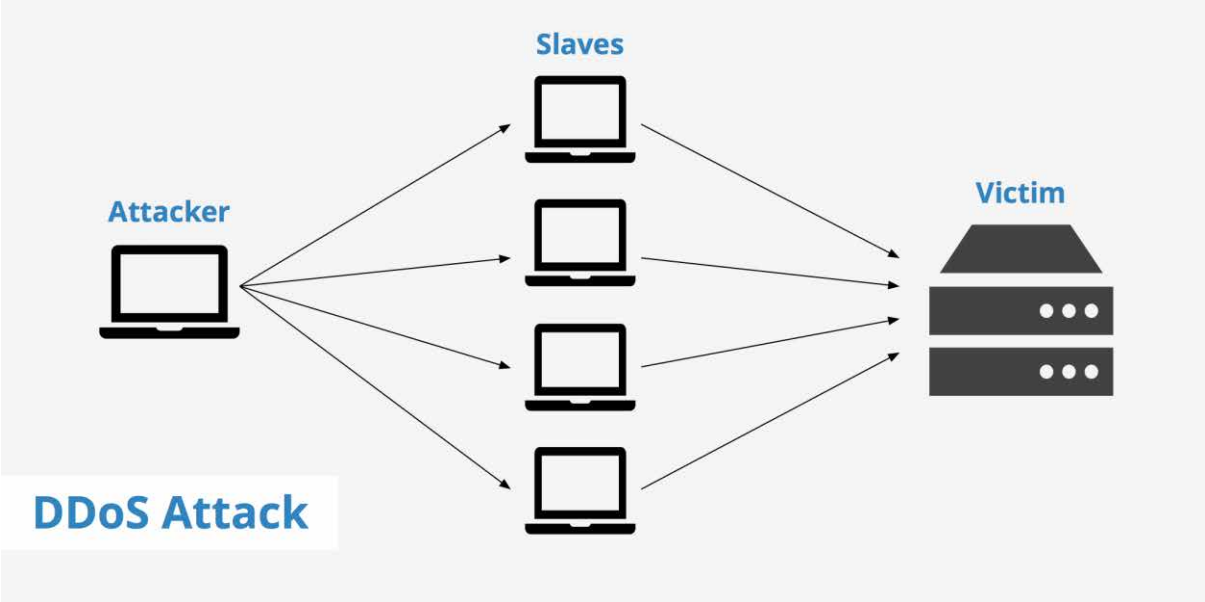


Рисунок 1.1 - Атака з відмовою у обслуговуванні

Фішингові атаки в ігровій індустрії є серйозною загрозою, спрямованою на викрадення облікових даних користувачів, таких як паролі, логіни або іншу особисту інформацію. Зловмисники створюють фальшиві веб-сайти або надсилають підроблені електронні листи, що імітують офіційні повідомлення від розробників гри чи популярних платформ, щоб ввести користувачів в оману і змусити їх розкрити конфіденційну інформацію.

Такі атаки можуть призвести до серйозних наслідків для гравців. Зловмисники, отримавши доступ до облікового запису, можуть використовувати його для крадіжки внутрішньоігрових предметів, валют

або навіть продавати обліковий запис на чорному ринку. Це може завдати як фінансових збитків, так і значних емоційних переживань для користувачів, оскільки вони можуть втратити прогрес, досягнення або інші важливі елементи, накопичені за довгий час гри.

Крім того, фішингові атаки можуть завдати шкоди репутації розробників або видавців гри, оскільки користувачі можуть втратити довіру до безпеки їхніх продуктів. Це особливо актуально для великих онлайн-ігор, де безпека облікових записів і конфіденційність інформації є ключовими для підтримання активної гравецької бази.

Для запобігання фішинговим атакам розробники ігрових платформ активно працюють над підвищенням рівня безпеки, впроваджуючи двофакторну аутентифікацію, попереджаючи користувачів про можливі загрози та здійснюючи регулярні перевірки своїх систем на вразливості. Тим не менш, гравцям також необхідно бути обачними, уважно перевіряти всі електронні листи та посилання, а також користуватися лише офіційними джерелами для входу в свої облікові записи.

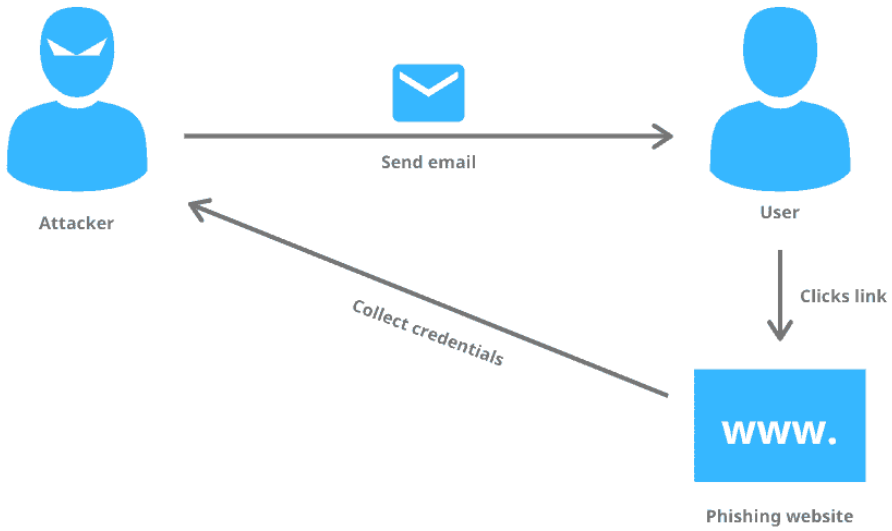


Рисунок 1.2 - Фішинг атака

SQL-ін'єкції є одним із найнебезпечніших видів атак на веб-додатки, зокрема на ігрові платформи. Ці атаки дозволяють зловмисникам отримати

несанкціонований доступ до баз даних гри, вводячи шкідливі SQL-запити в поля для введення даних на веб-сайтах. У результаті цього вони можуть отримати доступ до конфіденційної інформації, такої як облікові записи користувачів, фінансова інформація або дані, пов'язані з грою.

Наслідки таких атак можуть бути катастрофічними для ігрових компаній та їхніх користувачів. Зловмисники можуть викрасти особисті дані гравців, що може призвести до фінансових втрат або компрометації облікових записів. Вони також можуть маніпулювати даними гри, змінюючи або видаляючи важливу інформацію, що може порушити роботу ігрового сервісу.

Для розробників ігрових платформ SQL-ін'єкції становлять серйозну загрозу, оскільки успішна атака може підірвати довіру користувачів до безпеки системи. Це може вплинути на репутацію компанії, викликати юридичні проблеми, пов'язані з витоком даних, та призвести до значних фінансових втрат через необхідність усунення наслідків атаки та компенсації постраждалим користувачам.

Щоб запобігти SQL-ін'єкціям, розробники повинні застосовувати сучасні методи захисту, такі як параметризовані запити, регулярні перевірки на вразливості та використання надійних механізмів автентифікації і шифрування даних. Однак навіть з такими заходами безпеки, користувачі повинні бути обережними при введенні своїх даних на будь-яких платформах.

Зловмисники можуть використовувати вразливості в API (інтерфейсах програмування додатків), які застосовуються в ігрових додатках, для отримання несанкціонованого доступу до даних або функціоналу гри. API є важливими елементами, які дозволяють різним компонентам гри та сервісам обмінюватися інформацією та виконувати певні дії. Проте, якщо API містять вразливості або неправильно налаштовані, це може стати шляхом для атаки.

Такі вразливості можуть бути використані для викрадення облікових записів користувачів, що дозволяє зловмисникам отримати доступ до особистих даних, внутрішньоігрових ресурсів та навіть здійснювати фінансові операції від імені користувача. Крім того, атакуючі можуть маніпулювати ігровими ресурсами, змінюючи кількість внутрішньої валюти, предметів або впливаючи на інші аспекти гри, що може порушити баланс ігрового процесу.

Зловживання вразливостями в API також може викликати збої у роботі гри, зниження її продуктивності або навіть повну недоступність певних функцій для користувачів. Це може вплинути на стабільність і надійність гри, що негативно позначається на досвіді користувачів та довірі до розробників.

Захист API є критично важливим для забезпечення безпеки ігрових додатків. Для цього розробники повинні регулярно перевіряти свої API на наявність вразливостей, використовувати механізми автентифікації та шифрування, а також впроваджувати заходи контролю доступу, щоб мінімізувати ризики таких атак.

Ігрові активи, такі як внутрішньоігрова валюта, предмети або акаунти, можуть бути дуже цінними для кіберзлочинців. Ці активи привертають увагу зловмисників, які використовують різні методи для їх здобуття.

Наприклад, зловмисники можуть викрадати дані або зламувати акаунти, щоб отримати доступ до ігрових активів. Після того як активи отримані, вони можуть бути продані на чорному ринку або використані для незаконних цілей. Це може включати перепродаж внутрішньоігрової валюти, продаж рідкісних ігрових предметів або навіть шахрайство з акаунтами.

Внаслідок таких атак можуть виникати серйозні проблеми для гравців, включаючи втрату особистих даних, фінансові збитки та порушення ігрового досвіду. Розробники ігор повинні активно захищати свої системи

від таких загроз, впроваджуючи ефективні механізми безпеки та моніторинг для запобігання несанкціонованому доступу до цінних ігрових активів.

Ransomware-атаки в ігровій індустрії передбачають блокування доступу до даних або серверів гри з наступною вимогою викупу для їх розблокування. Зловмисники використовують шкідливе програмне забезпечення для зашифрування важливих даних або блокування доступу до критичних серверів.

Такі атаки можуть призвести до зупинки функціонування гри, створюючи значні проблеми для розробників ігрових проектів. Компанії можуть стикатися з тривалими перервами у роботі, що вплине на гравців і може зашкодити їхньому досвіду. Відновлення доступу до систем і даних може вимагати значних ресурсів та витрат, що також може вплинути на фінансовий стан компанії.

Крім того, сплата викупу не завжди гарантує повернення доступу до даних або серверів, і існує ризик повторних атак. Таким чином, ransomware-атаки є серйозною загрозою для ігрових компаній, що вимагає від них впровадження ефективних заходів безпеки для захисту своїх систем.

Модифікації (моди) та чит-програми можуть використовуватися не лише для шахрайства в грі, але й для впровадження шкідливого програмного забезпечення. Зловмисники можуть створювати популярні моди або чит-програми, які на перший погляд здаються невинними або навіть корисними, але насправді є троянами або іншим шкідливим ПЗ.

Ці шкідливі програми можуть викрадати особисті дані користувачів, такі як облікові дані або фінансову інформацію, або завдавати шкоди системам, на яких вони встановлені. Наприклад, трояни можуть встановлюватися разом з модами, що дозволяє зловмисникам отримати доступ до комп'ютера або мобільного пристрою користувача, викрадаючи важливу інформацію або порушуючи безпеку системи.

Такі атаки можуть мати серйозні наслідки для користувачів ігрових платформ, призводячи до втрати особистих даних, фінансових збитків або навіть повного знищення даних. Для розробників ігрових платформ важливо вживати заходів безпеки, щоб запобігти розповсюдженню шкідливих модів і чит-програм і захистити своїх користувачів від потенційних загроз.

Кіберзлочинці часто зламують облікові записи гравців, щоб отримати доступ до їхніх ігрових ресурсів або особистої інформації. Викрадені акаунти можуть використовуватися для крадіжки внутрішньоігрової валюти, предметів або інших цінних активів. Ці ресурси потім можуть бути перепродані на чорному ринку або використані для шахрайських цілей.

Окрім цього, зламані акаунти можуть бути продані або використані для шахрайства, що може призвести до фінансових збитків для користувачів і підриву довіри до ігрових платформ.

Цей вид атак, відомий як соціальна інженерія, включає використання психологічних маніпуляцій для отримання конфіденційної інформації від гравців або розробників. Шахраї використовують різні методи, щоб ввести жертву в оману та переконати її надати особисті дані або доступ до системи.

Наприклад, зловмисники можуть вдаватися до співробітників технічної підтримки, адміністрації гри або інших користувачів. Вони можуть використовувати фальшиві електронні листи, повідомлення в чатах або телефонні дзвінки, щоб створити вигляд офіційного запиту або термінової ситуації, що потребує термінового реагування.

Метою таких атак є отримання облікових даних, фінансової інформації або доступу до систем, що дозволяє зловмисникам здійснювати подальші шахрайські дії. Це може включати крадіжку ресурсів, маніпуляцію з акаунтами або навіть заподіяння шкоди системам компанії.

Зловмисники можуть знаходити і використовувати вразливості в програмному коді ігор для отримання несанкціонованого доступу до закритих функцій, маніпулювання ігровим процесом або викрадення даних.

Ці атаки можуть бути дуже небезпечними, оскільки часто залишаються непоміченими довгий час. Виявлення і усунення таких уразливостей може бути складним і вимагати значних зусиль, що дозволяє зловмисникам продовжувати свої дії до того, як проблема буде виявлена та вирішена.

Man-in-the-Middle (MitM) атаки відбуваються, коли зловмисник перехоплює і змінює дані, що передаються між гравцем і сервером гри. Це може включати викрадення чутливої інформації, такої як облікові дані або фінансові транзакції. Крім того, зловмисник може змінювати ігрові дані, включаючи результати гри, внутрішньоігрові транзакції або статистики. Такі атаки можуть серйозно вплинути на цілісність і безпеку ігрового процесу.

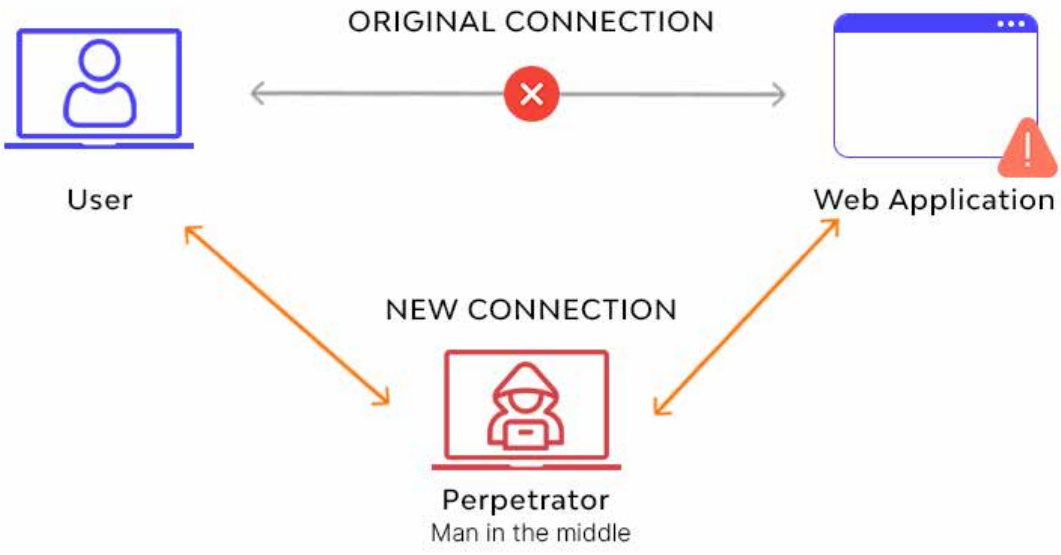


Рисунок 1.3 - Man-in-the-Middle атаки

DRM (Digital Rights Management) системи використовуються для захисту ігор від несанкціонованого копіювання і використання. Коли ці системи зламуються, зловмисники можуть поширювати піратські копії ігор, що призводить до фінансових втрат для розробників. Злом DRM систем часто викликаний прагненням отримати безкоштовний доступ до ігор або комерційною вигодою від їх розповсюдження.

Кіберзагрози в ігровій індустрії є дуже різноманітними і можуть завдати значної шкоди як розробникам, так і користувачам. Щоб зменшити ризики і забезпечити безпеку, розробники повинні впроваджувати надійні заходи захисту.

- Шифрування даних. Захист даних гри і користувачів від несанкціонованого доступу.
- Системи багатофакторної аутентифікації. Додатковий рівень захисту, що ускладнює доступ до облікових записів та систем.
- Регулярні перевірки безпеки. Постійний моніторинг і оновлення систем для виявлення і усунення можливих вразливостей.
- Впровадження цих заходів допомагає зменшити ризики і підвищити загальний рівень безпеки в ігровій індустрії.

1.2. Огляд існуючих підходів захисту

Огляд існуючих підходів захисту в ігровій індустрії демонструє широкий спектр технічних рішень, проте не всі з них однаково ефективні. Шифрування даних

Переваги: Шифрування даних забезпечує захист конфіденційної інформації, такої як особисті дані користувачів і фінансова інформація. Це основний інструмент для захисту від несанкціонованого доступу і забезпечення конфіденційності.

Обмеження: Хоча шифрування захищає дані, воно не запобігає всім видам атак, таким як DDoS або атаки на вразливості коду. Шифрування

також може вплинути на продуктивність системи, що слід враховувати при реалізації.

Системи багатофакторної аутентифікації (MFA)

Переваги: MFA додає додатковий рівень безпеки, вимагаючи кілька форм підтвердження особи, що значно ускладнює несанкціонований доступ до облікових записів.

Обмеження: Хоча MFA ефективно захищає від багатьох форм атак, зловмисники можуть використовувати соціальну інженерію, щоб обійти ці захисні механізми. Крім того, MFA може бути не завжди зручним для користувачів.

DRM (Digital Rights Management) системи

Переваги: DRM системи допомагають захистити ігри від піратства та несанкціонованого копіювання, що є критично важливим для комерційних продуктів.

Обмеження: Злом DRM систем є поширеним явищем, і це може призвести до розповсюдження піратських копій. Крім того, DRM може вплинути на досвід користувача, обмежуючи легітимні права.

Регулярні перевірки безпеки

Переваги: Регулярні перевірки дозволяють виявити уразливості та слабкі місця системи до того, як їх зможуть використати зловмисники.

Обмеження: Це може бути витратним і часозатратним процесом, особливо для великих систем. Крім того, регулярні перевірки не завжди гарантують, що нові вразливості не з'являться після перевірок.

Захист від DDoS атак

Переваги: Рішення для захисту від DDoS атак, такі як фільтрація трафіку та автоматичне масштабування ресурсів, можуть значно зменшити вплив таких атак.

Обмеження: Ці рішення можуть бути дорогими і складними в реалізації. Вони також не можуть запобігти всім типам атак, особливо новим і незвичним методам.

Захист від шкідливих модів і чит-програм

Переваги: Виявлення і блокування шкідливих модів і чит-програм може захистити гру від шахрайства і забезпечити справедливий ігровий процес.

Обмеження: Зловмисники постійно вдосконалюють свої методи, і підтримка актуальності захисту може бути складною і дорогою.

Аналіз та моніторинг поведінки користувачів

Переваги: Моніторинг аномальної поведінки може допомогти виявити і запобігти шахрайству або атакам на ранніх стадіях.

Обмеження: Це може викликати занепокоєння щодо конфіденційності і потребує балансування між безпекою та приватністю користувачів.

Кожен з цих підходів має свої сильні та слабкі сторони. Ефективний захист в ігровій індустрії вимагає комплексного підходу, який включає кілька рівнів захисту для мінімізації ризиків і забезпечення безпеки як для розробників, так і для користувачів.

1.3. Висновок по першому розділу

Кіберзагрози в ігровій індустрії є різноманітними і можуть завдати значної шкоди як розробникам, так і користувачам. Атаки можуть включати DDoS-атаки, фішингові атаки, SQL-ін'єкції, вразливості в API, ransomware-атаки, шкідливі моди та чит-програми, соціальну інженерію, злом облікових записів і злом DRM-систем. Ці загрози постійно еволюціонують, і зловмисники стають більш винахідливими у своїх методах.

Зловмисники можуть використовувати різні методи, такі як викрадення даних, маніпулювання ігровим процесом або розповсюдження піратських копій ігор для досягнення своїх цілей. Такі атаки можуть призвести до

фінансових втрат для розробників, порушення ігрового досвіду для користувачів та загрози безпеці даних. Крім того, через злом DRM-систем можуть розповсюджуватися нелегальні копії ігор, що завдає збитків індустрії.

Для зниження ризиків і забезпечення безпеки, розробники повинні впроваджувати надійні заходи захисту. Основними з них є шифрування даних, яке дозволяє захистити конфіденційну інформацію користувачів, а також використання систем багатофакторної аутентифікації для обмеження доступу до облікових записів. Регулярні перевірки безпеки допоможуть виявляти потенційні вразливості та своєчасно їх усувати.

Активне реагування на потенційні загрози і постійний моніторинг систем також є важливими аспектами забезпечення безпеки. Це дозволить зберегти цілісність і безпеку ігрових платформ, захистити особисті дані користувачів та зменшити фінансові втрати від кіберзлочинства. Розробники повинні постійно адаптувати свої системи захисту до нових загроз і співпрацювати з кібербезпековими організаціями для підтримки актуальних знань і технологій захисту.

2.АНАЛІЗ СУЧАСНИХ ПІДХОДІВДО ЗАХИСТУ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В ІГРОВИХ СИСТЕМАХ

2.1 Інструменти та технології захисту цифрових прав у ігровій індустрії

У сфері ігрових систем захист інтелектуальної власності (ІВ) є надзвичайно важливим аспектом, оскільки він гарантує дотримання прав розробників на створений контент та забезпечує фінансову стабільність компаній-розробників. В умовах постійного розвитку технологій та зростання популярності відеоігор, ефективний захист ІВ стає критично важливим для забезпечення справедливості на ринку та стимулювання інновацій.

Сучасні підходи до захисту ІВ у відеоіграх охоплюють різноманітні методи, які можна класифікувати за кількома категоріями. По-перше, це технічні заходи, які включають шифрування даних, обмеження доступу до вихідного коду та використання антипіратських технологій. По-друге, це юридичні механізми, такі як патенти, авторські права та торгові марки, які забезпечують правовий захист створених ігрових продуктів.

Одним з інноваційних підходів до захисту ІВ є розробка алгоритмів, які дозволяють інтегрувати захисні функції безпосередньо у саму гру. Наприклад, реалізація функцій, які показують спливаючі вікна з інформацією про авторські права або водяні знаки, що з'являються після запуску гри, може суттєво ускладнити піратське використання контенту. Це не тільки підвищує рівень захисту, але й постійно нагадує користувачам про авторські права, що може зменшити кількість порушень.

Розробка алгоритмів для захисту ІВ повинна враховувати не тільки технічні аспекти, але й зручність використання для кінцевих користувачів. Залучення сучасних технологій, таких як блокчейн для верифікації унікальності контенту, та впровадження інтуїтивно зрозумілих інтерфейсів

можуть значно підвищити ефективність системи захисту. Крім того, важливим аспектом є регулярне оновлення захисних механізмів у відповідь на нові виклики та вразливості, що з'являються в результаті розвитку технологій.

У підсумку, захист інтелектуальної власності у сфері ігрових систем є динамічною та багатогранною проблемою, яка вимагає комплексного підходу. Інтеграція технічних, юридичних та інноваційних рішень допоможе забезпечити ефективний захист ігрового контенту та підтримати фінансову стабільність розробників. Розробка і впровадження нових алгоритмів для захисту ІВ є критично важливим етапом у створенні безпечного ігрового середовища, яке стимулює креативність та інновації в індустрії відеоігор.

Цифрові водяні знаки (Digital Watermarking). Цей метод полягає у вбудовуванні прихованої інформації в аудіо-, відео- або графічні матеріали, які використовуються в грі. Цифровий водяний знак може містити дані про автора, ліцензійні права або іншу важливу інформацію. Його метою є забезпечення відстеження ідентичності контенту навіть у випадку його несанкціонованого розповсюдження.

Преімущества цього підходу включають можливість відстеження джерел несанкціонованого використання та доказування правовласності в судових спорах. Проте, складність технології та можливість обхідних методів можуть обмежувати ефективність водяних знаків.

Цифрові водяні знаки є важливим інструментом для захисту інтелектуальної власності в цифровому середовищі, зокрема в ігровій індустрії. Вони дозволяють ідентифікувати авторів і власників прав, відстежувати джерела несанкціонованого використання та забезпечують додаткові можливості для захисту контенту. Однак, їх ефективність може бути обмежена технічними складнощами та можливістю обходу, що вимагає постійного вдосконалення технологій та стратегій захисту

DRM-технології забезпечують контроль за доступом до цифрового контенту і його використанням. Вони включають шифрування файлів, перевірку автентичності користувача, обмеження на кількість установок або активацій гри тощо.

Переваги DRM полягають у здатності обмежити можливість піратства та забезпечити, щоб лише авторизовані користувачі мали доступ до контенту. Однак, недоліками цього підходу є можливі негативні відгуки від користувачів через обмеження на використання продукту, а також можливі обходи системи з боку піратів.

DRM-технології є важливим інструментом для захисту цифрового контенту і боротьби з піратством. Вони надають можливість контролювати доступ до контенту і зменшувати ризик незаконного розподілу. Проте, важливо також враховувати потенційні недоліки, такі як негативні відгуки від користувачів та можливість обходу системи. Для досягнення оптимального результату необхідно знайти баланс між забезпеченням захисту і комфортом використання контенту для легальних користувачів.

Ліцензійні угоди є юридичними документами, що визначають права та обов’язки сторін щодо використання програмного забезпечення. Вони включають положення щодо заборони на копіювання, модифікацію та розповсюдження контенту.

Цей підхід забезпечує юридичний захист прав розробників, оскільки порушення угоди може призвести до юридичної відповідальності. Однак, цей підхід є ефективним лише за умови належного юридичного супроводу та дотримання угоди з боку користувачів.

Ліцензійні угоди є важливим інструментом у сфері програмного забезпечення, що забезпечує юридичний захист прав розробників. Вони визначають правила використання програмного забезпечення і забезпечують контроль над його копіюванням, модифікацією та розповсюдженням. Ефективність таких угод залежить від належного

юридичного супроводу та дотримання їх умов з боку користувачів. За допомогою чітко сформульованих угод розробники можуть захистити свою інтелектуальну власність та зменшити ризик порушень з боку третіх осіб.

Криптографія є важливим інструментом для забезпечення безпеки ігрових систем, особливо коли йдеться про захист ігрових файлів та комунікаційних каналів. Шифрування даних забезпечує їх захист від несанкціонованого доступу, зберігаючи цілісність та конфіденційність інформації. Це особливо важливо в умовах сучасних кіберзагроз, де захист інтелектуальної власності та користувацьких даних має критичне значення.

Криптографія, як наука про захист інформації, використовує різноманітні методи шифрування для перетворення зрозумілої інформації (плейнтексту) в незрозумілу (шифротекст) таким чином, щоб її могли розшифрувати тільки ті особи, які мають спеціальний ключ. У контексті ігрових систем це може включати шифрування файлів гри, збережених даних користувачів, а також даних, що передаються через мережу.

Застосування криптографії в ігрових системах є ефективним методом для забезпечення захисту даних та комунікаційних каналів. Хоча цей підхід надає високий рівень безпеки та захисту конфіденційної інформації, реалізація може бути складною та вимагати ретельного управління ключами. Для досягнення оптимальних результатів важливо враховувати як переваги, так і виклики, що супроводжують використання криптографічних технологій у сфері ігрових систем.

У сучасному цифровому середовищі проблема піратства є однією з найгостріших для компаній, що займаються розробкою програмного забезпечення, включаючи ігрові студії. Піратський контент, який нелегально розповсюджується в інтернеті, завдає значної шкоди бізнесу, впливаючи на доходи компаній та порушуючи права інтелектуальної власності. Для боротьби з цим явищем компанії використовують спеціальні

програми та сервіси для моніторингу піратського контенту, а також юридичні інструменти. Розглянемо детальніше ці підходи.

Використання спеціалізованих програм і юридичних інструментів може бути ефективним у виявленні та ліквідації піратського контенту, але ці підходи мають свої обмеження. Технічні рішення потребують постійного моніторингу і оновлень, щоб залишатися ефективними проти нових методів піратства. Юридичні заходи, в свою чергу, можуть бути витратними і часозатратними, а їх ефективність може варіюватися в залежності від юрисдикції і специфіки порушень.

В цілому, боротьба з піратством є комплексним завданням, що потребує інтеграції технічних та юридичних підходів, а також постійного моніторингу та ресурсів. Це допомагає захистити права інтелектуальної власності та забезпечити справедливість на ринку цифрового контенту.

Ці системи використовують алгоритми машинного навчання та штучного інтелекту для автоматичного виявлення порушень прав ІВ, таких як несанкціоноване використання музики або графіки в іграх.

Вони дозволяють швидко ідентифікувати порушення та вживати відповідних заходів. Недоліком може бути висока вартість розробки та впровадження таких систем.

Сучасні підходи до захисту інтелектуальної власності в ігрових системах є різноманітними та багатогранними, проте кожен з них має свої переваги та недоліки. Ефективний захист потребує комплексного підходу, який поєднує технологічні, юридичні та організаційні заходи. На основі аналізу цих підходів можна розробити новий алгоритм, що забезпечить більш високий рівень захисту і відповідатиме сучасним викликам індустрії.

2.2. Дослідження законодавчих вимог щодо охорони інтелектуальної власності в галузі цифрових технологій та відеоігор

Захист інтелектуальної власності (ІВ) в галузі цифрових технологій та відеоігор регулюється складною системою міжнародних та національних законів, які мають на меті захист прав авторів, розробників та видавців. Дослідження законодавчих вимог включає аналіз основних правових норм, які регулюють ІВ у цій галузі.

Міжнародні угоди та стандарти. Бернська конвенція (1886 р.). Один з основних міжнародних договорів, що регулює авторські права. Вона забезпечує охорону літературних і художніх творів, включаючи програмне забезпечення, на міжнародному рівні. Конвенція встановлює мінімальні стандарти охорони авторських прав, включаючи право на переклади, публікацію та розповсюдження творів.

Угода про торговельні аспекти прав інтелектуальної власності (TRIPS, 1994 р.). У рамках Світової організації торгівлі (СОТ), ця угода визначає мінімальні стандарти охорони ІВ, включаючи авторське право, патенти та товарні знаки. Вона зобов'язує держави-учасниці забезпечити ефективні засоби захисту ІВ та передбачає заходи проти порушень прав.

Національні законодавства. Законодавство США. У Сполучених Штатах охорона ІВ регулюється кількома законами, серед яких Закон про авторське право (Copyright Act, 1976 р.), Закон про патенти (Patent Act, 1952 р.) та Закон про товарні знаки (Lanham Act, 1946 р.). США також запровадили DMCA (Digital Millennium Copyright Act, 1998 р.), який забезпечує захист цифрових прав і забороняє обходження технологій захисту авторських прав.

Законодавство Європейського Союзу. В ЄС охорона ІВ регулюється кількома директивами та регламентами, які гармонізують національні закони країн-членів. Директива 2001/29/ЄС про авторські права в інформаційному суспільстві встановлює правила захисту цифрових творів,

включаючи комп'ютерні програми та відеоігри. Директива 2019/790 (Директива про авторське право на єдиному цифровому ринку) також є ключовою для сучасного регулювання ІВ у цифровому середовищі.

Законодавство України. В Україні охорона авторського права регулюється Законом України "Про авторське право і суміжні права" (1993 р.) та рядом інших нормативно-правових актів. Закон передбачає захист програмного забезпечення, баз даних, аудіовізуальних творів та інших об'єктів ІВ, що використовуються у відеоіграх. Останніми роками також було прийнято заходи для гармонізації національного законодавства з європейськими стандартами у сфері ІВ.

Специфіка захисту ІВ у відеоіграх. Авторські права на програмне забезпечення. Програмне забезпечення, як основний компонент відеоігор, підлягає захисту авторським правом. Це включає код гри, дизайн, графіку, музику, а також будь-який інший творчий контент. Відповідно до законодавства, автори програмного забезпечення мають виключні права на його використання та розповсюдження.

Патенти на ігрові механіки. В деяких випадках розробники можуть патентувати унікальні ігрові механіки або технології. Це дозволяє їм захистити свої новаторські розробки від копіювання іншими компаніями. Патентний захист забезпечує ексклюзивне право на використання технології протягом певного періоду часу.

Товарні знаки та брендинг. Логотипи, назви ігор та інші елементи брендингу також можуть бути захищені товарними знаками. Це запобігає використанню схожих знаків, які можуть ввести споживачів в оману.

Юридичні виклики та судова практика. Судові справи про порушення ІВ у відеоіграх. Судова практика у сфері ІВ включає численні випадки, коли компанії-розробники ініціювали судові процеси проти порушників авторських прав або патентів. Такі справи зазвичай є складними, оскільки вимагають високого рівня технічної експертизи та аналізу.

Захист ІВ у цифровому середовищі, включаючи Інтернет, є важливою частиною сучасного законодавства. Це включає заходи проти піратства, незаконного стрімінгу та поширення контенту без дозволу.

Законодавчі вимоги щодо охорони інтелектуальної власності в галузі цифрових технологій та відеоігор є комплексними і різноманітними. Вони включають міжнародні угоди, національні закони та спеціальні правові норми, які забезпечують захист авторських прав, патентів та товарних знаків у цифровому середовищі. Для ефективного захисту ІВ у відеоіграх необхідно дотримуватися цих вимог та враховувати останні зміни у законодавстві.

2.3. Unreal Engine 5

Unreal Engine 5 (UE5) пропонує ряд сучасних технологій захисту, які допомагають забезпечити безпеку ігрового контенту та захистити інтелектуальну власність.

Рисунок 2.1 - Unreal Engine 5

UE5 підтримує використання шифрування для захисту ігрових даних. Це може включати.

Використання стандартів шифрування (наприклад, AES) для захисту даних гри від несанкціонованого доступу. Це може бути корисним для захисту чутливих даних, таких як внутрішні ресурси або налаштування гри.

Захист даних, що передаються між сервером і клієнтом гри, щоб запобігти перехопленню або модифікації інформації.

Digital Rights Management (DRM). Інтеграція з DRM-системами для захисту ігрового контенту від несанкціонованого копіювання та розповсюдження.

Вбудовані засоби моніторингу. Механізми для виявлення і запобігання використанню зламаних версій гри або модифікованих файлів.

Обфускація коду. Обфускація коду допомагає ускладнити реверс-інжиніринг і аналіз внутрішньої логіки гри:

Кодування. Зміна імен змінних і функцій на менш зрозумілі, що ускладнює розуміння коду сторонніми особами.

Шифрування скриптів.Шифрування скриптів та важливих частин коду для захисту від несанкціонованого доступу і модифікацій.

Інтеграція з античітовими системами:

Системи детекції читерства. Інструменти для виявлення і блокування програм, які намагаються змінити або вплинути на геймплей.

Моніторинг активності. Аудит і моніторинг ігрової активності для виявлення підозрілої поведінки.

UE5 підтримує ряд заходів для забезпечення безпеки ігрових серверів:

Аутентифікація і авторизація. Використання сучасних протоколів аутентифікації для підтвердження особи користувача і забезпечення доступу до сервера.

Захист від DDoS-атак. Механізми для захисту ігрових серверів від розподілених атак на відмову в обслуговуванні.

Механізми захисту контенту. UE5 має вбудовані можливості для захисту контенту.

Digital Watermarking. Використання цифрових водяних знаків для ідентифікації ігрового контенту і відстеження його розповсюдження.

Content Integrity Checks. Перевірка цілісності файлів і ресурсів для виявлення і запобігання їх модифікації.

UE5 підтримує інтеграцію з різними бібліотеками і плагінами для покращення безпеки. Плагіни для шифрування. Додаткові плагіни для реалізації шифрування та захисту даних.

Бібліотеки для моніторингу. Інструменти для відстеження та аналізу активності користувачів і процесів гри.

Unreal Engine 5 надає потужний набір інструментів і технологій для захисту інтелектуальної власності та безпеки ігрових систем. Інтеграція шифрування, обфускації коду, античітових систем, захисту серверів і контенту допомагає створити надійний захист для ігрових проектів і запобігти несанкціонованому доступу та використанню.

Захист QR-кодів стає дедалі важливішим, особливо у контексті використання їх у цифрових продуктах, таких як відеоігри, де вони можуть містити чутливу інформацію або інтерактивні елементи.

Шифрування даних у QR-кодах. Симетричне шифрування для захисту інформації в QR-кодах можна використовувати симетричне шифрування, де ключ для шифрування і розшифрування однаковий. Це дозволяє приховати зміст QR-коду від сторонніх осіб. Для розшифрування потрібен відповідний ключ, що робить інформацію недоступною для неавторизованих користувачів.

Асиметричне шифрування. У цьому випадку використовується пара ключів – відкритий і закритий. Відкритий ключ використовується для шифрування даних, а закритий – для їх розшифрування. Це підвищує безпеку, оскільки лише власник закритого ключа може розшифрувати інформацію.

Цифровий підпис. Цифрові підписи дозволяють забезпечити автентичність даних, що зберігаються в QR-коді. Власник підписує дані своїм приватним ключем, і будь-хто, хто має відповідний відкритий ключ, може перевірити підпис і впевнитися, що дані не були змінені.

Перевірка автентичності - це дозволяє отримувачам даних з QR-коду переконатися, що інформація походить від надійного джерела і не була змінена з моменту її створення.

Захист від підробок. Генерація унікальних кодів, щоб уникнути підробок, кожен QR-код може бути унікальним, наприклад, шляхом включення одноразових токенів або інших динамічних даних, які змінюються при кожному генерації коду.

Системи перевірки справжності. Включення механізмів, які дозволяють користувачам перевірити справжність QR-коду шляхом звернення до серверної бази даних, де зберігається інформація про всі легітимні коди.

Захист від злочинного використання, Обмежений час дії QR-коди можуть бути створені з обмеженим терміном дії, після якого вони стають недійсними. Це запобігає їх використанню в несанкціонованих ситуаціях.

Контроль доступу. Впровадження механізмів, що обмежують доступ до певних даних в QR-коді залежно від статусу користувача, його прав або геолокації.

Способи виявлення маніпуляцій. Використання хеш-функцій для створення контрольних сум даних, що зберігаються в QR-коді. Це дозволяє виявити будь-які зміни або маніпуляції з даними.

Водяні знаки та стеганографія Включення прихованих водяних знаків або стеганографічних елементів у QR-код, які можуть бути використані для перевірки його справжності та цілісності.

Використання платформи блокчейн. Децентралізована автентифікація, блокчейн можна використовувати для зберігання записів про створені QR-коди, що забезпечує прозорість і унеможливлює зміну інформації без відповідного запису у ланцюгу блоків.

Відстеження використання з допомогою блокчейну можна відстежувати всі взаємодії з QR-кодами, що дозволяє виявити спроби їх підробки або несанкціонованого використання.

Двухфакторна аутентифікація (2FA) при використанні QR-коду для доступу до важливих даних або сервісів можна додатково впровадити двухфакторну аутентифікацію, що значно підвищує рівень захисту.

Моніторинг і сповіщення системи, які відстежують спроби сканування QR-кодів та сповіщають про підозрілу активність, можуть запобігти їхньому злочинному використанню.

Сучасні технології захисту QR-кодів включають комплексні підходи до забезпечення їхньої безпеки, що поєднують шифрування, цифрові підписи, системи перевірки справжності, механізми запобігання підробкам і використання блокчейну. Завдяки цим технологіям можна ефективно захистити дані, що містяться в QR-кодах, і запобігти їхньому несанкціонованому використанню або підробці.

QR-коди (Quick Response Codes) мають ряд переваг, які роблять їх ідеальним вибором для різних завдань, зокрема для інтеграції в ігрові системи або проекти, пов'язані із захистом інтелектуальної власності. Швидкий і зручний доступ до інформації. QR-коди дозволяють швидко і зручно передавати інформацію користувачам. Скануючи код за допомогою смартфона чи іншого пристрою, користувач може миттєво отримати доступ до веб-сторінки, документа або іншого ресурсу. Це особливо корисно в ігрових середовищах, де гравець може оперативно отримати додаткову інформацію або контент.

Універсальність використання. QR-коди можна використовувати для різних типів даних, включаючи URL-адреси, текстові повідомлення, контактну інформацію, геолокацію, Wi-Fi налаштування та багато іншого. Це дозволяє їх легко інтегрувати в різні сценарії, наприклад, для відображення інформації про автора гри, доступу до ексклюзивного контенту або перевірки справжності продукту.

Можливості персоналізації. QR-коди можуть бути персоналізовані для конкретного продукту або користувача. Це дозволяє створювати унікальні коди для різних ситуацій або користувачів, забезпечуючи індивідуальний підхід і додатковий рівень захисту.

Інтеграція з системами безпеки. QR-коди можуть бути використані в поєднанні з різними технологіями безпеки, такими як шифрування, цифрові підписи, або блокчейн, що забезпечує додатковий рівень захисту. Наприклад, за допомогою QR-коду можна передавати зашифровані дані, які можуть бути розшифровані лише за наявності відповідного ключа.

Масова підтримка. QR-коди підтримуються практично всіма сучасними смартфонами та іншими мобільними пристроями. Це забезпечує їх широке використання і доступність, не вимагаючи додаткового обладнання або спеціальних додатків для сканування.

Простота генерації та використання. Створення QR-кодів є простим і швидким процесом. Існує безліч онлайн-інструментів і програмного забезпечення, що дозволяють генерувати QR-коди безкоштовно. Крім того, їх використання вимагає мінімальних ресурсів, що робить їх економічно вигідним рішенням.

Можливості для інтерактивності. QR-коди можуть бути інтегровані в ігрові системи як елементи інтерактивності. Наприклад, гравець може сканувати код, щоб розблокувати додатковий контент, отримати бонуси або іншу інформацію, що робить гру більш захоплюючою і цікавою.

Безпека та контроль доступу. QR-коди можуть бути використані для контролю доступу до певної інформації або ресурсів. Наприклад, код може бути активним лише протягом певного часу або для конкретної групи користувачів, що дозволяє більш точно контролювати розповсюдження інформації.

QR-коди є ефективним, універсальним і доступним інструментом для передачі інформації та інтеграції в різні системи, включаючи ігрові платформи. Вони забезпечують простий і зручний доступ до даних, підтримують широкі можливості персоналізації та інтеграції з системами безпеки, що робить їх ідеальним вибором для проектів, спрямованих на

захист інтелектуальної власності та забезпечення взаємодії з користувачами.

2.4. Проектування структури алгоритму захисту інтелектуальної власності для ігрових систем

Проектування структури алгоритму захисту інтелектуальної власності (ІВ) для ігрових систем передбачає створення комплексного рішення, яке поєднує різні методи та технології для забезпечення надійного захисту контенту від несанкціонованого використання. Нижче наведено основні етапи та компоненти проектування такого алгоритму.

Визначення цілей та вимог. Забезпечити ефективний захист всіх елементів інтелектуальної власності, включаючи код гри, графіку, музику, сценарій та інші компоненти.

Основні вимоги:

- Висока ефективність захисту від копіювання та піратства.
- Простота інтеграції в існуючі ігрові системи.
- Мінімальний вплив на продуктивність гри.
- Захист від обходу захисних механізмів.

Аутентифікація користувача:

- Використання двофакторної аутентифікації для захисту акаунтів користувачів ігрової системи.
- Інтеграція з платформами цифрового розповсюдження, такими як Steam, Epic Games Store, для забезпечення додаткового рівня захисту.

Шифрування контенту:

- Шифрування всіх основних файлів гри, включаючи код, текстури, моделі, звуки та відео, з використанням симетричних та асиметричних криптографічних алгоритмів.
- Динамічне розшифрування контенту в реальному часі під час запуску гри.

Цифрові водяні знаки:

- Вбудовування цифрових водяних знаків у графічні, аудіо- та відеоматеріали гри. Ці водяні знаки можуть бути унікальними для кожної копії гри, що дозволяє відстежувати витоки піратських версій.
- Використання стеганографічних методів для приховання водяних знаків таким чином, щоб вони були невидимі для кінцевого користувача, але легко ідентифікувались за допомогою спеціального програмного забезпечення.

Моніторинг та виявлення порушень:

- Інтеграція з автоматизованими системами моніторингу інтернет-простору для виявлення несанкціонованих копій гри.
- Використання машинного навчання для аналізу та ідентифікації піратських копій, що дозволить ефективніше реагувати на порушення прав.

Захист коду:

- Обфускація коду гри для ускладнення зворотного інжинірингу.
- Використання технологій анти-тимпінгу для захисту від модифікації і підробки коду.
- Патентування унікальних ігрових механік:
- Виявлення унікальних ігрових механік, що використовуються в грі, та їх патентування для забезпечення правової охорони.
- Автоматизований контроль за використанням патентованих механік іншими розробниками.
- Ліцензування та управління правами:
- Впровадження системи управління цифровими правами (DRM) для контролю за розповсюдженням і використанням контенту.
- Використання ліцензійних ключів для активації гри, з можливістю онлайн-верифікації для підтвердження легітимності копії.

Архітектура алгоритму

Клієнтська сторона:

- Вбудований модуль шифрування та розшифрування контенту, що працює у фоновому режимі під час гри.
- Модуль водяних знаків для автоматичного додавання унікальних ідентифікаторів до всіх візуальних та аудіо компонентів гри.

Серверна сторона:

- Сервер автентифікації користувачів, який зберігає всі дані про користувачів та забезпечує їх захист.
- Сервер управління ліцензіями, який контролює активацію гри та відстежує використання ліцензійних ключів.
- Модуль моніторингу, що постійно сканує інтернет на предмет виявлення піратського контенту.
- Комунікаційний протокол:
- Безпечний канал для передачі даних між клієнтом та сервером, що використовує шифрування для захисту інформації від перехоплення.
- Протокол обміну даними для автоматичного оновлення водяних знаків та управління правами доступу.

Інтеграція алгоритму в ігрові системи

Розробка SDK (Software Development Kit):

- Створення інструментів для розробників, що дозволяють легко інтегрувати алгоритм в існуючі та нові проекти.
- Надання детальної документації та прикладів коду для спрощення процесу інтеграції.
- Тестування та валідація:
- Проведення ретельного тестування алгоритму на різних платформах та в різних сценаріях використання.
- Оцінка впливу алгоритму на продуктивність гри та забезпечення його оптимальної роботи.

Проектування структури алгоритму захисту інтелектуальної власності для ігрових систем є складним і багатокомпонентним процесом, який

вимагає комплексного підходу. Включення різних технологій, таких як шифрування, цифрові водяні знаки, захист коду та моніторинг порушень, дозволить забезпечити надійний захист контенту та дотримання прав авторів і розробників.

2.5 Висновок по другому розділу

У сучасній індустрії відеоігор захист інтелектуальної власності (ІВ) набуває дедалі більшої важливості, оскільки цифрові продукти, зокрема відеоігри, стають об'єктами частих спроб піратства та нелегального використання. Ефективні методи захисту інтелектуальної власності дозволяють не тільки запобігати втратам від незаконного розповсюдження, а й забезпечують юридичний захист прав розробників. У цьому контексті розробка алгоритму для захисту ІВ у відеоіграх є важливим кроком у забезпеченні цілісності цифрового контенту.

Одним із ключових інструментів, що використовується для захисту контенту у відеоіграх, є цифрові водяні знаки. Ця технологія дозволяє приховано вбудовувати інформацію про авторство чи правовласника безпосередньо в ігрові ресурси, що допомагає ідентифікувати джерела несанкціонованого використання. Цифрові водяні знаки мають перевагу у відстеженні незаконного копіювання, однак їх ефективність залежить від складності технології та здатності обходити методи захисту.

Системи DRM також активно використовуються в ігровій індустрії для захисту контенту від піратства. Вони надають можливість контролювати доступ до цифрових матеріалів через шифрування і перевірку автентичності користувачів. Незважаючи на те, що DRM є потужним інструментом для захисту, негативні відгуки геймерів через обмеження в користуванні продуктом є поширеним викликом.

Іншим підходом є використання угод з кінцевими користувачами (EULA), що встановлюють правила користування і забороняють

модифікацію або копіювання гри без дозволу правовласника. Такі угоди мають юридичну силу, проте їх ефективність залежить від здатності забезпечити дотримання умов та можливості притягнення порушників до відповідальності.

У рамках законодавчого захисту інтелектуальної власності значну роль відіграють міжнародні угоди та національні законодавства. Наприклад, Бернська конвенція, TRIPS, DMCA та інші міжнародні акти встановлюють стандарти охорони авторських прав та технологій у цифровій сфері. Ці нормативні акти визначають обов'язки держав і компаній щодо забезпечення захисту авторських прав і патентів.

Розробка власного алгоритму для захисту ІВ у відеоігрових системах повинна враховувати усі описані технологічні та юридичні аспекти. Це передбачає впровадження комплексного підходу, що поєднує шифрування ігрових даних, інтеграцію DRM-систем, моніторинг активності користувачів, а також автоматизовані системи виявлення порушень з використанням алгоритмів штучного інтелекту. Такий алгоритм також має враховувати специфіку використання сучасних ігрових движків, зокрема Unreal Engine 5, який підтримує численні технології захисту контенту.

Унікальні механізми захисту, зокрема шифрування даних та QR-кодів, можуть стати ефективними засобами для забезпечення безпеки ігрового контенту. Вони надають можливість не лише захистити дані від несанкціонованого доступу, але й забезпечити їх автентичність. Такі технології, як цифрові підписи, симетричне та асиметричне шифрування, блокчейн та двофакторна автентифікація, допомагають значно підвищити рівень захисту ігрових систем та запобігти підробкам або злочинному використанню контенту.

Таким чином, захист інтелектуальної власності у відеоіграх є багатогранним процесом, який вимагає поєднання технологічних, юридичних та організаційних заходів. Розроблений алгоритм може стати

основою для створення сучасних рішень, що забезпечать надійний захист від порушень авторських прав, піратства та несанкціонованого використання.

3.РОЗРОБКА І РЕАЛІЗАЦІЯ АЛГОРИТМУ ЗАХИСТУ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ ДЛЯ ІГРОВИХ СИСТЕМ

3.1 Визначення основних компонентів

Процес розробки та впровадження алгоритму захисту інтелектуальної власності для ігрових систем є багатокомпонентним і вимагає ретельного підходу на кожному етапі. Ключовою частиною цього процесу є створення програмного забезпечення, яке інтегрується з існуючими ігровими системами та платформами. Оскільки захист ІВ в ігровій індустрії є однією з найважливіших задач для розробників, досягнення цього захисту вимагає комплексного рішення, що охоплює різні технічні та організаційні аспекти.

Першим етапом є чітке планування структури алгоритму. На цьому етапі необхідно визначити основні вимоги, які ставляться до системи захисту. Визначення функцій, які повинні бути реалізовані в рамках алгоритму, допоможе структурувати проект та розподілити ресурси ефективно. Необхідно враховувати можливість шифрування даних, застосування цифрових водяних знаків, управління ліцензіями, аутентифікацію користувачів та моніторинг активності. Крім того, важливо передбачити можливість гнучкої інтеграції алгоритму з різними платформами, на яких буде використовуватися гра.

Наступним кроком є вибір відповідних технологій для реалізації кожного з компонентів алгоритму. Вибір програмного інструментарію та мов програмування залежить від вимог до безпеки, продуктивності та сумісності з існуючими системами. Сучасні ігрові системи зазвичай використовують потужні засоби шифрування для захисту своїх даних. Зокрема, криптографічні алгоритми, такі як AES та RSA, є найпоширенішими для захисту конфіденційної інформації та запобігання несанкціонованому доступу до даних.

Одним з ключових компонентів алгоритму захисту є впровадження цифрових водяних знаків. Ці водяні знаки можуть бути вбудовані у візуальні, аудіо та відео елементи гри, що дозволяє відстежувати оригінальний контент і виявляти піратські копії. Важливим аспектом є те, що водяні знаки мають бути невидимими для кінцевого користувача, але доступними для аналізу у разі виникнення проблем з порушенням прав. Для цього використовуються методи стеганографії, які дозволяють приховувати інформацію без втрати якості контенту.

Ще одним важливим етапом є впровадження систем управління ліцензіями та аутентифікації користувачів. Ця частина алгоритму забезпечує контроль за розповсюдженням гри та доступом до неї. Ліцензійні ключі є ефективним інструментом для підтвердження прав на використання програмного продукту. Додатково, впровадження двофакторної аутентифікації значно підвищує рівень безпеки користувачів і дозволяє захистити їх облікові записи від несанкціонованого доступу.

Моніторинг також відіграє важливу роль в захисті інтелектуальної власності. Алгоритм має бути здатний виявляти несанкціоноване використання гри або її компонентів. Використання технологій штучного інтелекту та машинного навчання для аналізу активності в інтернеті дозволяє ефективно виявляти піратські копії та попереджати порушення прав розробників.

Тестування є важливою частиною процесу розробки алгоритму захисту. Потрібно провести комплексні випробування на різних платформах для перевірки сумісності та продуктивності алгоритму. Тестування допомагає виявити можливі вразливості та оптимізувати алгоритм для безперебійної роботи гри. Особлива увага приділяється тому, щоб алгоритм не впливав на швидкодію гри, що є критичним фактором для користувачів.

Зрештою, інтеграція алгоритму з існуючими системами є завершальним етапом, який потребує тісної взаємодії з іншими програмними

компонентами гри. Важливо, щоб всі елементи алгоритму працювали злагоджено, забезпечуючи надійний захист ІВ, не впливаючи на загальний користувацький досвід.

Забезпечення безпеки в ігровій індустрії є постійним процесом, тому алгоритм захисту ІВ повинен бути гнучким і здатним швидко адаптуватися до нових загроз, що виникають у цифровому середовищі. Регулярні оновлення алгоритму та його компонентів допоможуть розробникам зберегти свої права та мінімізувати ризики піратства.

Виділення ключових функціональних частин алгоритму, таких як шифрування, водяні знаки, управління ліцензіями, аутентифікація та моніторинг.

Побудова архітектурної схеми, що визначає взаємодію між цими компонентами.

Вибір технологій

- Для реалізації було обрано Unreal Engine 5
- Вибір мов програмування та фреймворків для розробки кожного з компонентів алгоритму. **Blueprint Class** (Блюпринт клас) є ключовим елементом системи візуального програмування Blueprint. Він дозволяє створювати ігрові об'єкти, їх поведінку та логіку без необхідності писати код мовою програмування C++.
- Вибір криптографічних алгоритмів, таких як AES для симетричного шифрування і RSA для асиметричного.

Модуль цифрових водяних знаків

- Розробка інструменту для додавання унікальних цифрових водяних знаків до візуальних, аудіо та відео компонентів гри.
- Використання стеганографії для приховання водяних знаків таким чином, щоб вони не впливали на якість контенту, але могли бути легко відстежені в разі витоку.

Модуль управління ліцензіями та аутентифікації

- Створення серверної системи для управління ліцензіями на гру, включаючи генерацію та верифікацію ліцензійних ключів.
- Впровадження системи аутентифікації користувачів з використанням двофакторної аутентифікації для підвищення безпеки.
- Інтеграція з платформами цифрового розповсюдження для автоматичного управління ліцензіями і контролю доступу до гри

Моніторинговий модуль

- Розробка автоматизованої системи моніторингу для виявлення порушень ІВ в інтернет-просторі, включаючи аналіз піратських сайтів та торентів.
- Використання алгоритмів машинного навчання для ідентифікації порушень та виявлення піратських копій гри.

Модуль обфускації коду

- Реалізація технік обфускації коду, що ускладнюють зворотній інжиніринг і модифікацію гри.
- Впровадження технологій анти-тимпінгу, що блокують роботу гри в разі виявлення підозрілих змін або втручання в код.

Інтеграція і тестування

- Створення SDK (Software Development Kit) для легкого впровадження алгоритму в існуючі ігрові проекти.
- Надання інструментів для автоматичного шифрування файлів, вбудовування водяних знаків та управління ліцензіями.

Тестування

- Проведення комплексного тестування на різних платформах і з різними типами контенту для перевірки сумісності, продуктивності та надійності алгоритму.
- Випробування алгоритму в реальних умовах для виявлення і усунення можливих проблем або вразливостей.

Оптимізація

- Аналіз продуктивності алгоритму і внесення змін для мінімізації впливу на швидкодію гри.
- Оптимізація використання ресурсів, щоб забезпечити швидке розшифрування та мінімальні затримки під час гри.

Розгортання серверної інфраструктури

- Налаштування серверів для управління ліцензіями, аутентифікації користувачів і моніторингу порушень.
- Забезпечення безперервної роботи серверів з використанням технологій відновлення після збоїв та резервного копіювання.

Захист і підтримка

- Впровадження автоматичних оновлень для алгоритму, що дозволяють швидко реагувати на нові загрози і вдосконалювати захисні механізми.
- Постійний моніторинг роботи алгоритму і своєчасне вирішення можливих проблем.

Розробка і реалізація алгоритму захисту інтелектуальної власності (ІВ) для ігрових систем є складним та багатоетапним процесом, що потребує глибокого розуміння сучасних технологій захисту даних та кібербезпеки. Під час розробки даного алгоритму було визначено кілька основних напрямів, що допомагають забезпечити ефективний захист контенту від несанкціонованого доступу, піратства та інших видів порушень авторських прав.

Першим етапом стала розробка модулів, що включають криптографічні технології для шифрування даних, використання цифрових водяних знаків, обфускацію коду та системи управління ліцензіями. Ці інструменти є важливими для збереження оригінальності контенту та захисту розробників від порушення їх прав. Важливу роль відіграють сучасні методи шифрування, такі як AES та RSA, які гарантують, що дані залишаються конфіденційними і захищеними від зловмисників.

Особлива увага була приділена системі управління ліцензіями та аутентифікації користувачів, оскільки саме ці елементи дозволяють ефективно контролювати доступ до контенту та уникати несанкціонованого поширення гри. Впровадження двофакторної аутентифікації значно підвищує рівень безпеки, тоді як система автоматичного моніторингу ліцензійних ключів дозволяє відслідковувати несанкціоноване використання гри.

Ще однією важливою частиною алгоритму стало застосування стеганографії для вбудовування водяних знаків, що не впливають на якість контенту, але можуть бути відстежені у разі порушень. Це допомагає виявляти піратські копії ігор та забезпечує можливість юридичного захисту прав розробників.

У процесі тестування алгоритму було проведено перевірки на різних платформах для оцінки його продуктивності та сумісності. Оптимізація алгоритму дозволила мінімізувати вплив захисних механізмів на ігровий процес, що забезпечує високу швидкодію та комфорт для користувачів. Постійний моніторинг та оновлення алгоритму є необхідними для його ефективної роботи в умовах, коли кіберзагрози постійно змінюються та еволюціонують.

Загалом, реалізований алгоритм захисту ІВ для ігрових систем забезпечує комплексний підхід до захисту контенту, включаючи як технічні заходи (шифрування, водяні знаки, обфускація), так і організаційні заходи (управління ліцензіями та аутентифікація). Це дозволяє не лише захистити права розробників, але й забезпечити стабільну роботу ігрових систем та збереження даних користувачів.

3.2. Тестування алгоритму спливаючого вікна в Unreal Engine 5

Мета тестування

Перевірити, чи правильно функціонує механізм спливаючого вікна, яке з'являється після запуску гри.

Переконатися, що вікно з повідомленням повторно з'являється через заданий проміжок часу після його закриття користувачем.

Підготовка до тестування

Встановлено та налаштовано Unreal Engine 5.

Проект створено з основною сценою, на яку буде накладено спливаюче вікно.

Реалізація механізму спливаючого вікна

В Blueprint створено відповідний Widget, який містить текстове повідомлення.

Встановлено таймер, який запускає повторне відображення вікна через заданий час після його закриття.

Тестові сценарії

Дія: Запустити гру і перевірити, чи з'являється спливаюче вікно на екрані одразу після старту.

Очікуваний результат: Вікно з'являється без затримок, відображаючи правильне повідомлення і кнопку "Close".

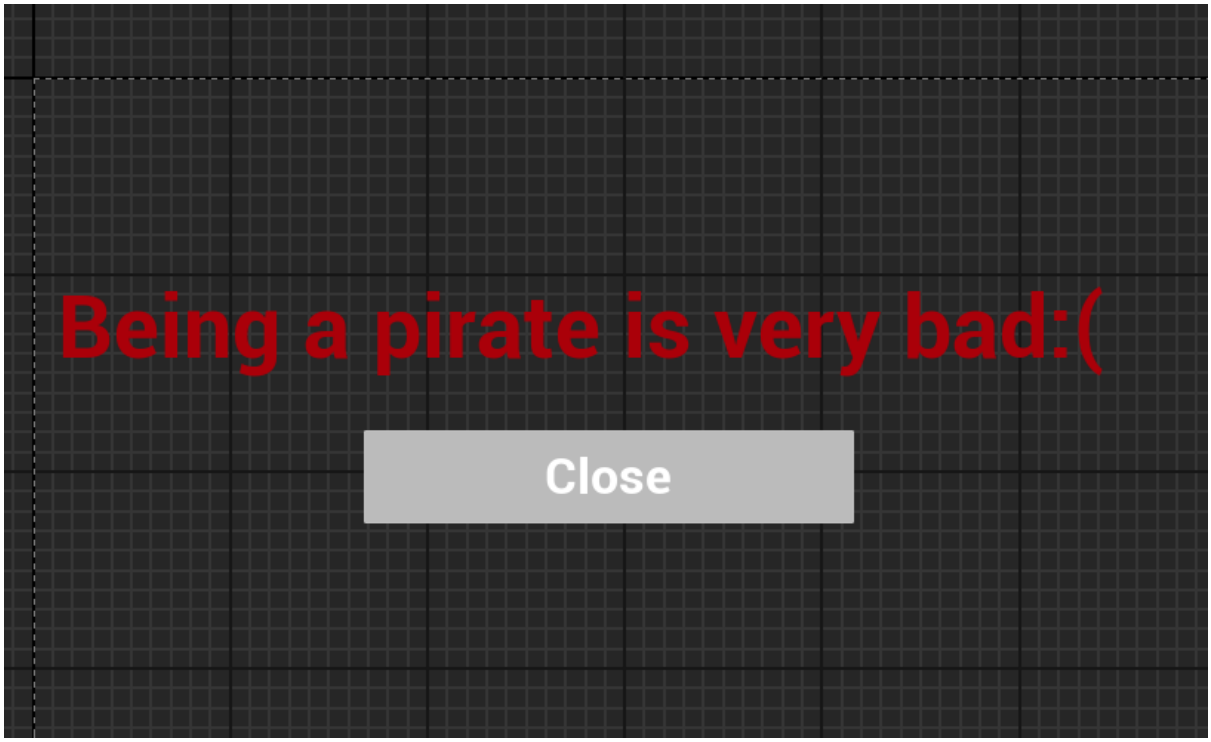


Рисунок 3.1 - Відображаючи повідомлення і кнопку "Close"

Закриття вікна

Дія: Натиснути кнопку "Close" для закриття вікна.

Очікуваний результат: Вікно закривається, гра продовжується без будь-яких збоїв.

Повторне з'явлення вікна

Дія: Дочекатися заданого часу, після якого вікно повинно знову з'явитися.

Очікуваний результат: Спливаюче вікно з'являється знову через заданий проміжок часу після його закриття.

Тестування на різних платформах

Дія: Виконати ті ж дії на різних платформах (наприклад, Windows, консолі).

Очікуваний результат: Вікно поводиться однаково на всіх платформах, включаючи правильне відображення і своєчасне повторне з'явлення.

Тестування при зміні інтервалу часу

Дія: Змінити інтервал часу для повторного з'явлення вікна і провести тестування.

Очікуваний результат: Вікно з'являється точно через новий встановлений проміжок часу.

Верифікація результатів

Запис та аналіз: Під час тестування записувати результати кожного тесту, відзначаючи успіхи та можливі збої.

Корекція: У випадку виявлення помилок або невідповідностей — внести відповідні зміни в Blueprint, виправити логику роботи таймерів або інших компонентів.

Повторне тестування: Після внесення змін повторити тестування для підтвердження усунення проблем.

Тестування показує, що алгоритм спливаючого вікна працює коректно, якщо вікно з'являється одразу після запуску гри, закривається за натисканням кнопки, і повторно з'являється через заданий проміжок часу. Успішно пройдені тести на різних платформах і з різними інтервалами часу свідчать про стабільність і надійність реалізації алгоритму.

3.3. Тестування додавання QR-коду в грі

У процесі розробки ігрової системи було реалізовано додавання QR-коду як пасхалки в одному з рівнів гри. Метою цього завдання було створення інтерактивного елемента, який би дозволяв гравцям дізнатися більше про автора гри, скануючи QR-код за допомогою мобільного пристрою.

Процес реалізації

Створення QR-коду: За допомогою спеціального генератора було створено QR-код, що містить зашифровану URL-адресу з інформацією про автора гри.

Рисунок 3.3 -Створення QR-коду

Інтеграція в гру: QR-код був інтегрований в ігровий рівень у вигляді текстури, яка розміщена на одному з об'єктів сцени. Код був доданий таким чином, щоб він виглядав як органічна частина ігрового світу.

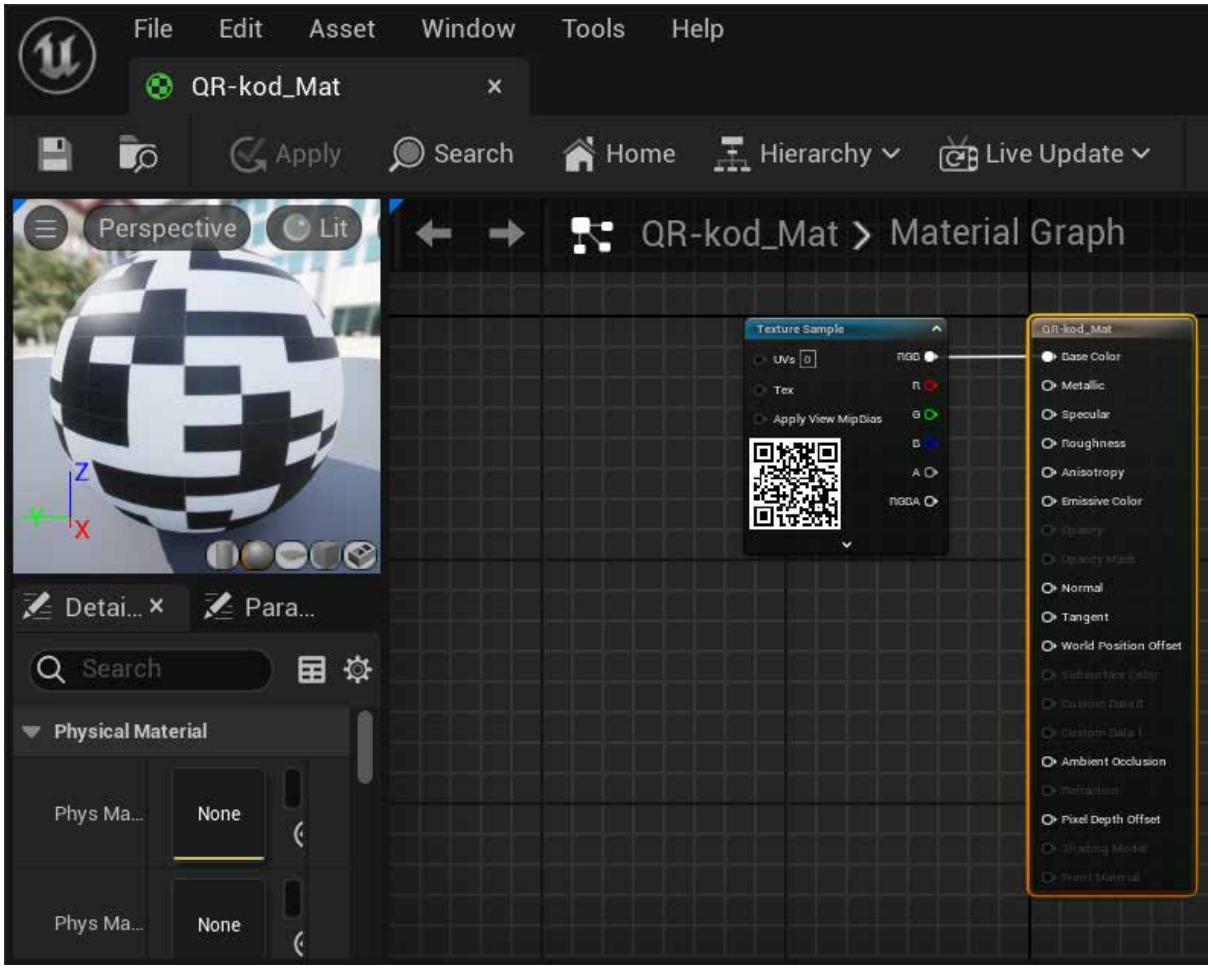


Рисунок 3.3 - Параметри QR-код

Рисунок 3.4 - QR-код у вигляді текстури

Тестування роботи QR-коду: Після інтеграції був проведений тест, де QR-код сканувався з екрану комп'ютера або монітора гравця.

Результати тестування

Успішність зчитування: QR-код успішно зчитується більшістю сучасних мобільних пристроїв з різних відстаней і під різними кутами.

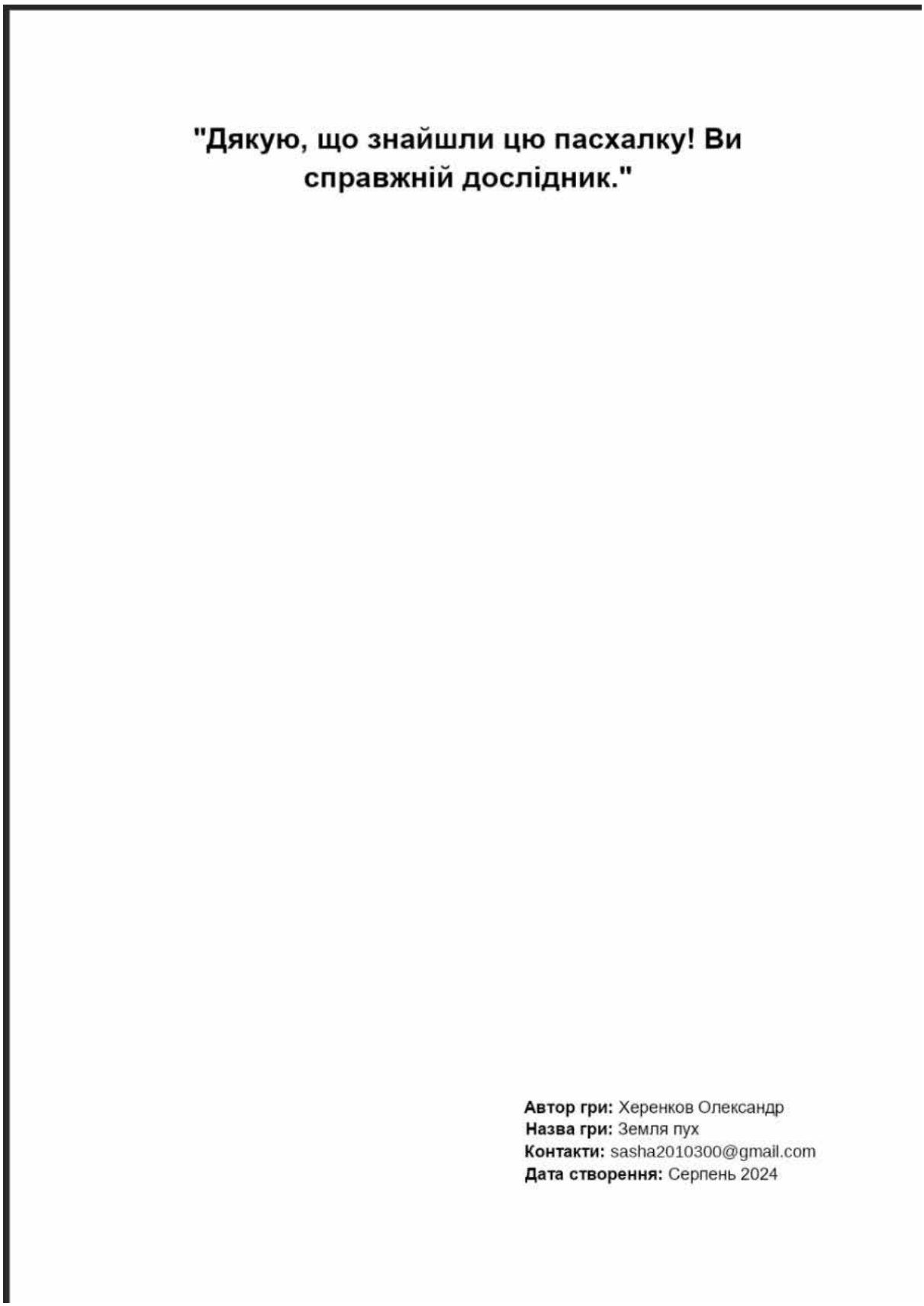


Рисунок 3.5 - Після сканування QR-коду

Відкриття інформації: Після сканування QR-коду на екрані мобільного пристрою автоматично відкривається веб-сторінка з інформацією про автора гри, що містить його ім'я, коротку біографію та контактні дані.

Відгук гравців: Гравці позитивно оцінили додавання QR-коду як цікавого інтерактивного елемента, що робить гру більш захоплюючою і дозволяє дізнатися більше про розробника.

Додавання QR-коду в гру було успішним. Він не тільки додає грі додаткову глибину і інтерактивність, але й забезпечує прямий зв’язок між гравцем і автором. Це рішення може бути використано в подальших проектах як ефективний спосіб комунікації та просування бренду розробника.

Аналіз результатів впровадження алгоритму, порівняння його з існуючими рішеннями, визначення переваг та можливих недоліків.

Розробка рекомендацій щодо впровадження алгоритму в практичну діяльність розробників ігрових систем, а також перспектив подальшого розвитку запропонованого підходу.

3.4. Тестування Функції Відображення Водяного Знака

*Мета:*Перевірити, чи водяний знак коректно відображається на екрані після запуску гри, а також перевірити його функціональність, включаючи можливість закриття та повторний показ через певний проміжок часу.

Підготовка до тестування

Перевірка початкових умов:

- Переконайтесь, що гра була повністю закрита перед тестуванням.
- Перевірте, що конфігураційні файли або системна пам'ять не містять інформації про попередні покази водяного знака.

Налаштування тестового середовища:

Запустіть Unreal Engine 5 та завантажте проект, що містить функцію відображення водяного знака.

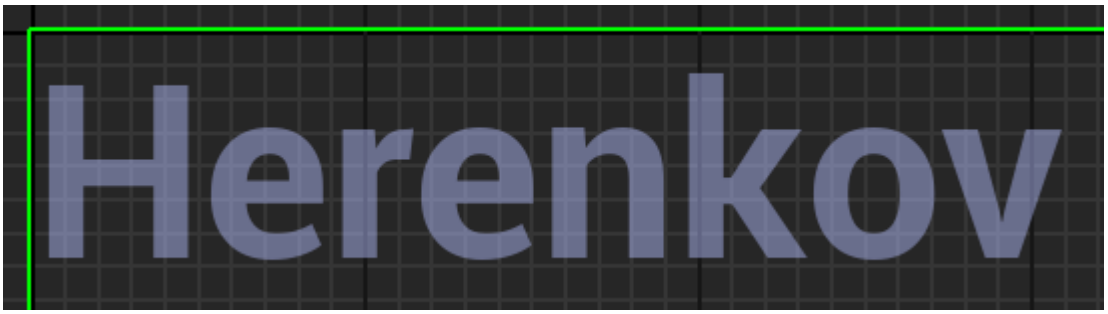


Рисунок 3.7 - Водяний знак

Кроки Тестування

- Запустіть гру.
- Очікуваний результат: Гра повинна успішно стартувати без помилок.

Перевірка відображення водяного знака

- Перевірка, чи водяний знак з'являється на екрані після запуску гри.
- Очікуваний результат: Водяний знак має з'явитися на екрані в правильному місці з коректним текстом/зображенням.

Рисунок 3.7 - Вивод водяной знак на главний єкран

Перевірка зберігання інформації про показ

- Перевірте конфігураційні файли або системну пам'ять на наявність інформації про показ водяного знака.
- Очікуваний результат: Інформація про показ водяного знака повинна бути коректно збережена.

Перевірка коректності затримки

- Змініть параметри затримки.
- Очікуваний результат: Водяний знак повинен відображатися.

Критерії успішності

Водяний знак коректно відображається на екрані після запуску гри.

Інформація про показ водяного знака зберігається правильно і водяний знак не відображається повторно без відповідних умов.

Затримка перед повторним показом водяного знака працює згідно з заданими параметрами.

3.5 Висновок по третьому розділу

Розробка та впровадження алгоритму захисту інтелектуальної власності (ІВ) для ігрових систем є складним і багатогранним процесом, який потребує ретельного планування, інтеграції різноманітних технологій і постійного тестування для забезпечення високого рівня захисту. У рамках цього дослідження були розглянуті та реалізовані кілька ефективних методів захисту, таких як шифрування, цифрові водяні знаки, управління ліцензіями та обфускація коду. Кожен з цих методів має свої переваги та недоліки, що було враховано при розробці комплексного алгоритму.

Шифрування стало ключовим інструментом захисту даних, дозволяючи забезпечити конфіденційність і цілісність ігрових файлів. Використання криптографічних алгоритмів, таких як AES для симетричного шифрування і RSA для асиметричного, дозволило створити надійний захист від несанкціонованого доступу та модифікації контенту. Це забезпечує високий

рівень безпеки, який є критичним для захисту інтелектуальної власності у цифровому середовищі.

Цифрові водяні знаки були розроблені та інтегровані в аудіо-, відео- та графічні матеріали, що використовуються в грі. Цей метод дозволяє не тільки ідентифікувати автора контенту, але й відстежувати його походження у випадку несанкціонованого розповсюдження. Використання стеганографії для приховання водяних знаків допомогло зберегти якість контенту, забезпечуючи при цьому можливість легкої ідентифікації водяних знаків у випадку порушення авторських прав.

Управління ліцензіями було реалізовано через серверну систему, яка відповідає за генерацію та верифікацію ліцензійних ключів. Це дозволяє контролювати доступ до гри та забезпечувати, що тільки авторизовані користувачі можуть використовувати продукт. Важливим аспектом також стала інтеграція системи аутентифікації користувачів, включаючи двофакторну аутентифікацію, яка підвищує рівень безпеки та запобігає несанкціонованому доступу до гри.

Обфускація коду, яка була впроваджена як додатковий захист від зворотнього інжинірингу, ускладнює процес модифікації гри та унеможливлює несанкціоноване використання вихідного коду. Це доповнюється технологіями анти-тимпінгу, що блокують роботу гри у випадку виявлення підозрілих змін або втручання в код, що значно підвищує безпеку ігрового продукту.

Після впровадження цих технологій було проведено комплексне тестування на різних платформах, що підтвердило стабільність і надійність роботи алгоритмів. Особливу увагу було приділено тестуванню функції відображення водяних знаків, спливаючих вікон та інтеграції QR-коду як інтерактивного елемента. Успішне проходження тестів показало, що розроблені рішення можуть бути ефективно інтегровані в існуючі ігрові

проекти, підвищуючи рівень захисту інтелектуальної власності та забезпечуючи довготривалу безпеку контенту.

Таким чином, розробка і реалізація алгоритму захисту інтелектуальної власності для ігрових систем підтвердила свою ефективність. Запропоновані рішення дозволяють значно знизити ризики несанкціонованого використання контенту, забезпечуючи надійний захист прав розробників та їх інтелектуальної власності. Це створює підґрунтя для подальшого розвитку і вдосконалення технологій захисту у сфері цифрового контенту, що є надзвичайно важливим в умовах сучасного динамічного ігрового ринку.

ВИСНОВОК

В процесі розробки алгоритму інтелектуальної власності для ігрових систем, зокрема для захисту ігор на платформі Unreal Engine 5 (UE5), було детально розглянуто кілька критичних аспектів.

По-перше, було визначено мету і завдання дослідження, які включали розробку алгоритму для захисту інтелектуальної власності, що забезпечує регулярний показ водяного знака після запуску гри, що дозволяє захистити права розробника і надати необхідну інформацію про авторство.

Для реалізації цієї мети була розроблена структура алгоритму, що включає перевірку статусу водяного знака, його відображення, можливість закриття і зберігання інформації про показ. Алгоритм передбачає регулярний повторний показ водяного знака після заданого проміжку часу, що підвищує видимість і забезпечує постійне нагадування про права інтелектуальної власності.

Проектування структури алгоритму включало створення блок-схеми, що візуалізує процес перевірки, відображення і закриття водяного знака. Це дозволяє спростити реалізацію та тестування алгоритму.

Важливою частиною роботи стало тестування реалізованого алгоритму. Було перевірено, що водяний знак коректно відображається на екрані після запуску гри, кнопка закриття працює належним чином, а інформація про показ водяного знака зберігається правильно. Затримка перед повторним показом була налаштована відповідно до заданих параметрів.

З урахуванням сучасних технологій захисту, використання UE5 для реалізації цього алгоритму було обрано через його потужний інструментарій для створення графічно інтенсивних ігор, можливість інтеграції різних систем захисту та простоту роботи з відображенням UI-елементів. Також було використано QR-коди як додатковий елемент

захисту, що забезпечує інтерактивний спосіб перевірки інформації про авторство.

Таким чином, реалізація алгоритму інтелектуальної власності в Unreal Engine 5 показала свою ефективність у забезпеченні захисту авторських прав на ігрові продукти, зберігаючи при цьому високу якість ігрового процесу та забезпечуючи необхідний рівень захисту від піратства і несанкціонованого використання контенту.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ковальчук В. М. Захист інтелектуальної власності у цифровій сфері. Київ: Наукова думка, 2020. 220 с.
2. Гринько М. І. Технології цифрового захисту та управління правами на контент у комп'ютерних іграх. Львів: Видавництво Львівської політехніки, 2019. 250 с.
3. Винокуров С. М. “Управление правами на цифровой контент: теория и практика”. Київ: Вид-во КНУ, 2017. 196 с.
4. Гайдаржи О. А. “Защита интеллектуальной собственности в игровой индустрии”. Киев: Наукова думка, 2021. 180 с.
5. Гончаров И. А. “Системы DRM и их роль в защите интеллектуальной собственности”. Минск: Технопринт, 2019. 225 с.
6. Гринько М. І. “Технології цифрового захисту та управління правами на контент у комп'ютерних іграх”. Львів: Видавництво Львівської політехніки, 2019. 250 с.
7. Денисенко С. В., Сафонова Л. А. “Інтелектуальна власність: правові та технічні аспекти”. Харків: Право, 2020. 232 с.
8. Єфімов О. Г. “Технології захисту інформаційного контенту: навчальний посібник”. Київ: Либідь, 2021. 290 с.
9. Іваненко В. К. “Сучасні підходи до управління цифровими правами у сфері ігрового контенту”. Харків: ХНЕУ, 2020. 220 с.
10. Ігнатьєв І. Л. “Роль технологій DRM у захисті прав на цифрові продукти”. Львів: Афіша, 2022. 190 с.
11. Ковальчук В. М. “Захист інтелектуальної власності у цифровій сфері”. Київ: Наукова думка, 2020. 220 с.
12. Кравченко М. В., Петров О. А. “Інтелектуальна власність та цифрові технології: правові аспекти”. Одеса: ОНУ, 2018. 250 с.
13. Лисенко О. І., Чуйко В. П. “Захист прав на інтелектуальну власність у цифровій індустрії”. Полтава: Університетська книга, 2021. 208 с.
14. Марченко В. В. “Проблеми захисту інтелектуальної власності у сфері цифрових технологій”. Київ: Вид-во КНУ, 2019. 230 с.
15. Пилипенко А. А., Шевченко Н. М. “Захист цифрових прав на ігровий контент”. Дніпро: ДНУ, 2021. 188 с.
16. Романенко С. П. “Алгоритми та методи захисту цифрових

продуктів”. Київ: КНТ, 2019. 210 с.

17. Чумак В. Г., Корольова І. М. “Розробка алгоритмів захисту ігрових продуктів у цифровому середовищі”. Черкаси: Вертикаль, 2022. 245 с.

18. Алексєєв О. С. “Інтелектуальна власність: правове забезпечення та захист”. Харків: Право, 2019. 205 с.

19. Антонюк А. С., Бойко І. О. “Цифрові технології захисту інтелектуальної власності”. Київ: КНТ, 2021. 170 с.

20. Безрукова В. П. “Правові аспекти захисту інтелектуальної власності в умовах глобалізації”. Львів: Апріорі, 2018. 256 с.

21. Богданова Н. А. “Захист авторських прав в цифровому середовищі”. Київ: Наукова думка, 2022. 280 с.

22. Василенко І. В., Печерська Л. Д. “Проблеми захисту цифрового контенту в медіа-індустрії”. Одеса: ОНУ, 2020. 230 с.

23. Войтович В. М. “Цифрові водяні знаки у захисті інформаційних ресурсів”. Харків: ХНЕУ, 2019. 215 с.

24. Гаврилюк О. І., Кравчук Л. М. “Інноваційні підходи до захисту інтелектуальної власності в цифровій економіці”. Львів: ЛНУ, 2021. 198 с.

25. Данильчук В. О., Колесник О. А. “DRM-технології як засіб захисту цифрових прав”. Івано-Франківськ: Прикарпаття, 2018. 176 с.

26. Єрмаков Д. І., Макарова О. О. “Захист прав інтелектуальної власності у сфері інформаційних технологій”. Київ: Центр учбової літератури, 2020. 220 с.

27. Журавель А. М., Ковальчук І. С. “Цифровий захист прав інтелектуальної власності”. Чернівці: Рута, 2019. 168 с.

28. Захаренко Т. М., Костюкевич В. П. “Ефективні технології цифрового захисту авторських прав”. Дніпро: Акцент, 2021. 185 с.

29. Задорожний М. А., Рогозін А. С. “Правові механізми захисту інтелектуальної власності у цифровому світі”. Тернопіль: Вектор, 2019. 210 с.

30. Зубенко О. К. “Інноваційні рішення для захисту прав на цифровий контент”. Київ: Вид-во КНУ, 2022. 200 с.

31. Касьяненко В. В. “Захист інтелектуальної власності в цифровому середовищі: виклики та перспективи”. Полтава: Університетська книга, 2020. 240 с.

32. Коваленко П. А., Ткаченко М. Л. “Захист цифрового контенту:

методи та технології”. Суми: СумДУ, 2021. 190 с.

33. Левченко О. В., Матвієнко І. О. “Цифрові рішення для управління правами на контент у геймінгу”. Черкаси: Вертикаль, 2020. 195 с.

34. Мельник О. П. “Сучасні методи захисту цифрового контенту та боротьби з піратством”. Київ: Либідь, 2021. 180 с.

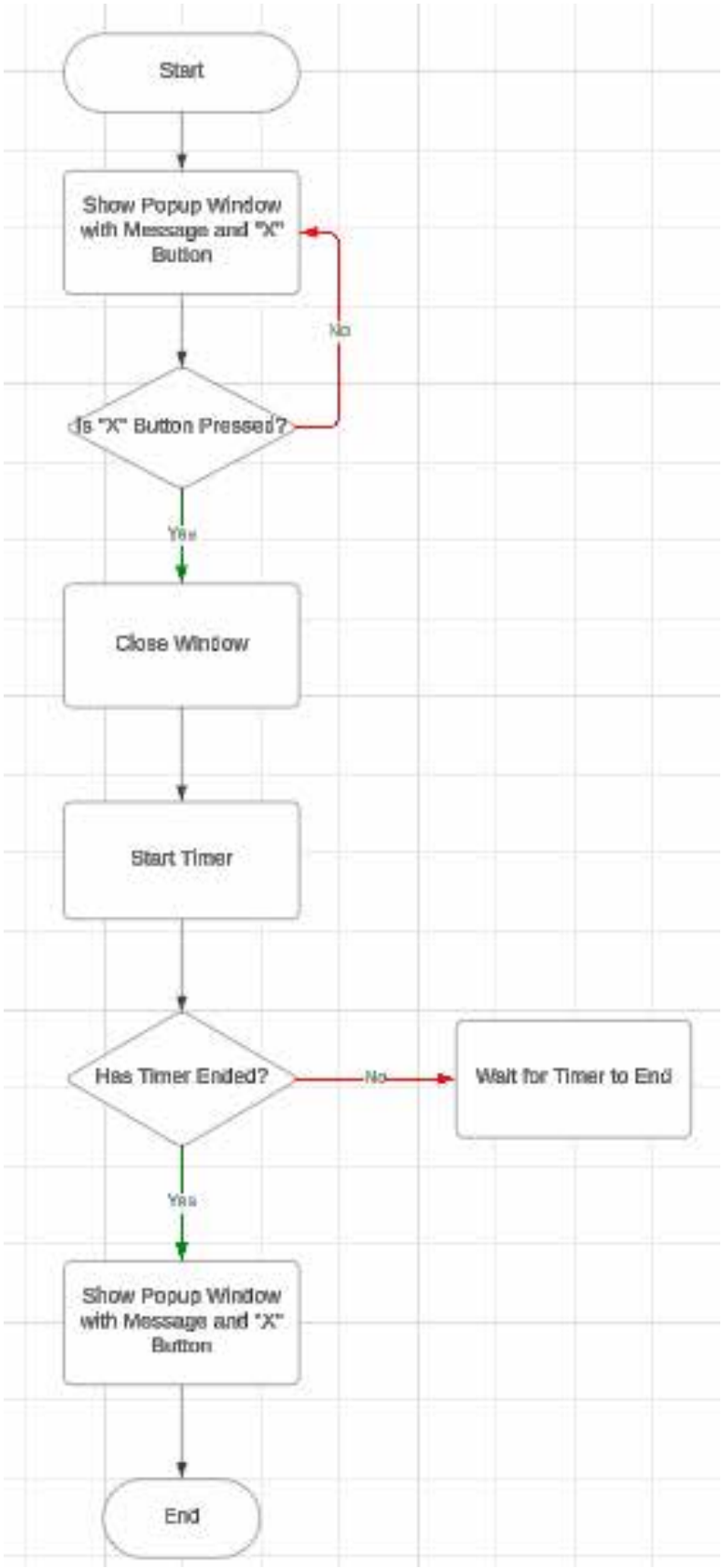
35. Нечипоренко В. О., Пилипенко І. К. “Правове забезпечення авторських прав у цифровій сфері”. Івано-Франківськ: Лілея, 2020. 200 с.

36. Прокопчук І. А., Гончарук Т. В. “Захист авторських прав у цифровому середовищі”. Вінниця: Теза, 2019. 175 с.

37. Чорна М. І., Савчук Л. Г. “Захист інтелектуальної власності в ігровій індустрії”. Рівне: НУВГП, 2022. 210 с.

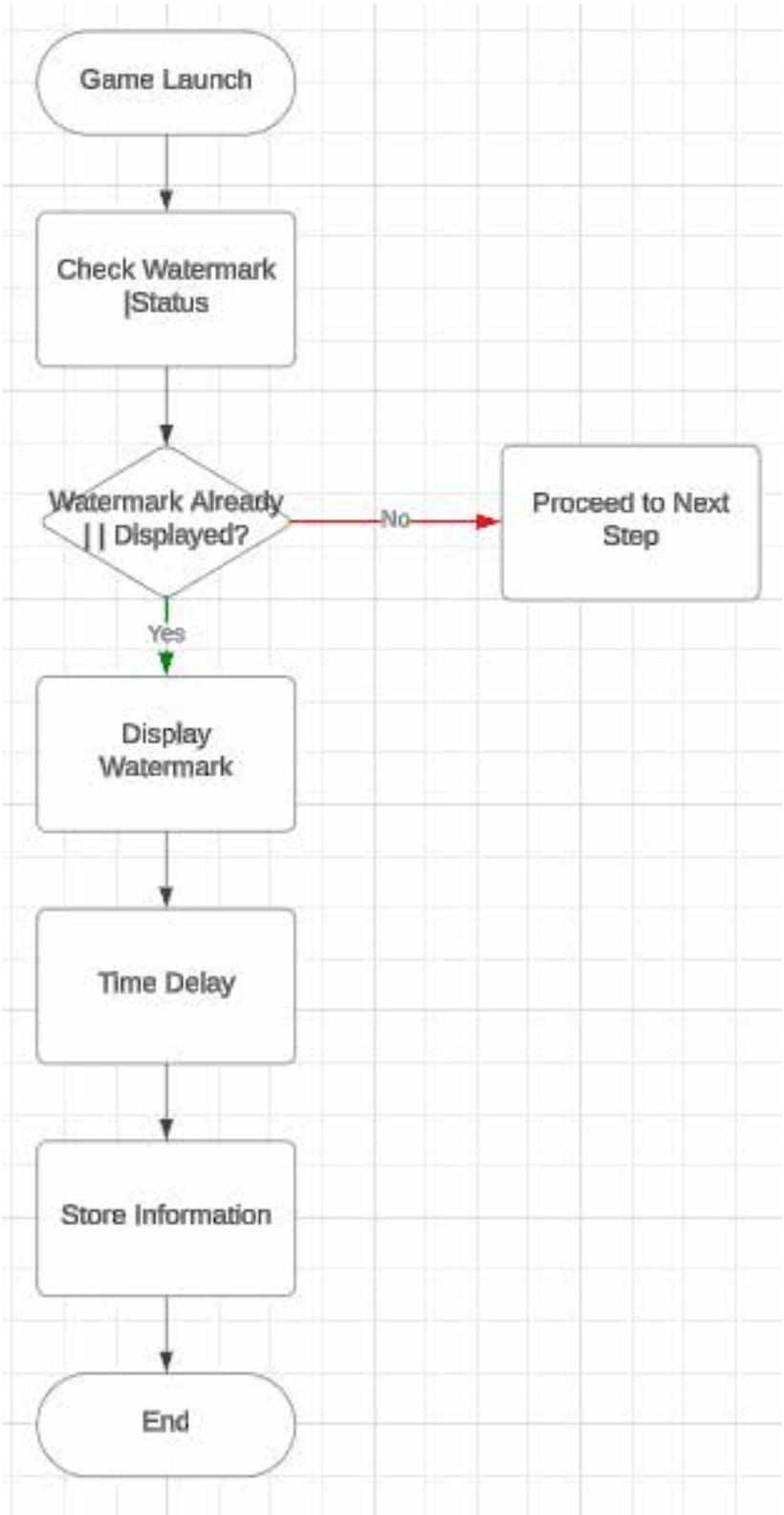
ДОДАТКИ

Додаток А «Схема Відображаючи повідомлення і кнопку “Close”»

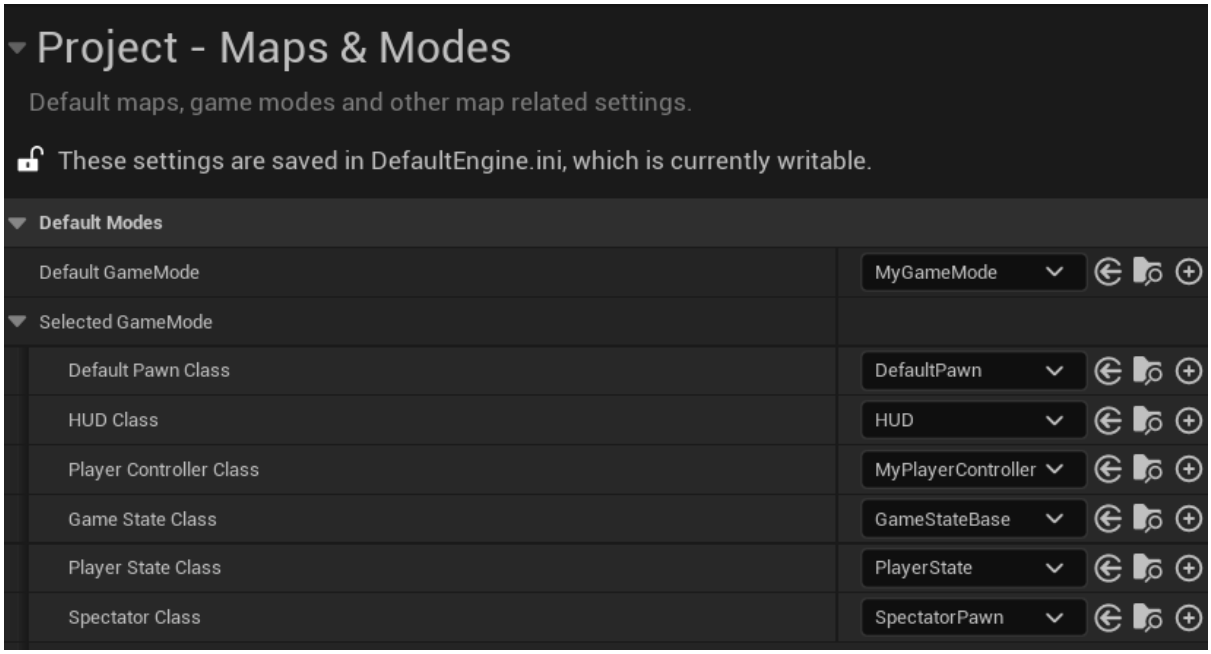


Додаток Б «Схема QR-код»

Додаток В «Схема Водяний знак»



Додаток Г «Водяний знак»



Додаток Д «Відображаючи повідомлення і кнопку “Close”»