МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

БАГМЕТ Владислав Сергійович

Методика та засоби запобігання піратства в кіберспорті / Methodology and Means of Preventing Piracy in Esports

спеціальність: 125 – Кібербезпека та захист інформації
освітньо-професійна програма – Кібербезпека

Кваліфікаційна робота

Виконав студент групи КБм -21
В. С. Багмет

Науковий керівник
к.т.н., доцент С.В.Івасьєв

Кваліфікаційну роботу допущено
до захисту:

«____» _____ ___2025 р.

Завідувач кафедри
_____ В.В.Яцків

ТЕРНОПІЛЬ - 2025

Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки
Освітній ступінь «магістр»
спеціальність: 125 - Кібербезпека та захист інформації
освітньо-професійна програма –Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ В.В.Яцків
«____» _____ 2024 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
БАГМЕТ ВЛАДИСЛАВ СЕРГІЙОВИЧ
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
Методика та засоби запобігання піратства в кіберспорті / Methodology and Means of Preventing Piracy in Esports
керівник роботи д.т.н., доцент С.В. Івасьєв
затверджені наказом по університету від 20 грудня 2024 року № 938
2. Строк подання студентом закінченої випускної кваліфікаційної роботи 5 грудня 2025 року.
3. Вихідні дані до кваліфікаційної роботи: завдання на випускну кваліфікаційну роботу студента, наукові статті, технічна література.
4. Основні питання, які потрібно розробити:
– проаналізувати особливості піратства у сфері відеоігор;
– здійснити аналіз еволюції антипіратських технологій;
– оцінити перспективи розвитку систем захисту відеоігор;
– проаналізувати нормативно-правові аспекти протидії піратству у сфері кіберспорту;
– дослідити вразливості сучасних ігрових рушіїв та середовищ виконання;
– проаналізувати проблеми drm-систем і можливості обходу ліцензійних механізмів;
– вивчити вразливості клієнт-серверної архітектури ігрових платформ;
– здійснити детальний аналіз вразливостей популярних ігрових платформ;
– проаналізувати відомі уразливості сучасних ігрових платформ;
– дослідити принципи й особливості експлуатації методу baitandswitch;
розробити методику запобігання піратству в кіберспорті.
5. Перелік графічного матеріалу у роботі:
– Система оплати ігрового ПЗ.
– Модель єдиної системи перевірки.
– Вразливості ігрової платформи steam та схема експлуатації вразливості, що веде до ескалації привілеїв.
– Поведінка Steam сервісу з нормальним запуском та при експлуатації вразливості.
– Методика запобігання піратства у кіберспорті та схема заходів для підвищення кібербезпеки ігрових платформ.

6. Консультанти розділів кваліфікаційної роботи

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

7. Дата видачі завдання 20 грудня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Аналіз предметної області	12.2024 р. – 03.2025 р.	
2	Нормативно правові аспекти у сфері кіберспорту	03.2025 р. – 06.2025 р.	
3	Аналіз вразливостей ігрових платформ	06.2025 р. – 11.2025 р.	

Студент _____ Владислав БАГМЕТ
(підпис)

Керівник роботи _____ к.т.н., доцент Степан ІВАСЬЄВ
(підпис)

АНОТАЦІЯ

Багмет В. С. Методика та засоби запобігання піратства в кіберспорті. – Рукопис.

Дослідження на здобуття освітнього ступеня «магістр» за спеціальністю 125 «Кібербезпека та захист інформації», освітньо-професійна програма «Кібербезпека». – Західноукраїнський національний університет, Тернопіль, 2025.

У роботі виконано проаналізовано особливості піратства у сфері відеоігор, визначено основні чинники його поширення, форми реалізації та економічні наслідки для розвитку індустрії, що дало змогу окреслити ключові загрози ліцензійному програмному забезпеченню та встановити залежність між рівнем піратства і темпами інновацій у геймдев-секторі. Виконано систематизацію відомих CVE, що стосуються платформ на кшталт Steam, визначено домінуючі класи вразливостей (ескалація привілеїв, інжекція, файлові маніпуляції, RCE), що забезпечило формування узагальненого профілю ризиків ігрових екосистем.

Розроблено комплексну методику запобігання піратству у кіберспорті, яка охоплює технічні, організаційні, поведінкові та правові заходи, що забезпечило формування цілісного підходу до захисту кіберспортивних екосистем від порушень авторських прав та експлуатації вразливостей.

Ключові слова: CVE, Steam, RCE, DRM.

ABSTRACT

Bagmet V. S. Methods and means of preventing piracy in cybersport. – Manuscript.

Research for the degree of “Master” in specialty 125 “Cybersecurity and information protection”, educational and professional program “Cybersecurity”. – Western Ukrainian National University, Ternopil, 2025.

The paper analyzes the features of piracy in the field of video games, identifies the main factors of its spread, forms of implementation and economic consequences for the development of the industry, which made it possible to outline the key threats to licensed software and establish the relationship between the level of piracy and the pace of innovation in the game development sector. Known CVEs related to platforms such as Steam were systematized, and dominant vulnerability classes (privilege escalation, injection, file manipulation, RCE) were identified, which provided a generalized risk profile for gaming ecosystems.

A comprehensive methodology for preventing piracy in eSports was developed, which includes technical, organizational, behavioral, and legal measures, which provided a holistic approach to protecting eSports ecosystems from copyright infringement and vulnerability exploitation.

Keywords: CVE, Steam, RCE, DRM.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ACL (Access Control List) – список контролю доступу, механізм визначення прав користувачів до об’єктів файлової системи.

API (Application Programming Interface) – інтерфейс прикладного програмування, набір засобів взаємодії програмних компонентів.

CVE (Common Vulnerabilities and Exposures) – загальний перелік вразливостей та експозицій, міжнародний реєстр відомих дефектів безпеки.

CVSS (Common Vulnerability Scoring System) – система стандартизованого оцінювання ступеня критичності вразливостей.

DRM (Digital Rights Management) – технології керування цифровими правами, спрямовані на запобігання несанкціонованому копіюванню.

DLL (Dynamic Link Library) – бібліотека динамічного завантаження у Windows.

DoS/DDoS (Denial of Service / Distributed Denial of Service) – відмова в обслуговуванні / розподілена відмова в обслуговуванні.

EoP (Elevation of Privilege) – ескалація привілеїв, отримання користувачем або процесом вищого рівня доступу.

ESL (Esports League) – кіберспортивна ліга.

FPS (First-Person Shooter) – жанр ігор від першої особи.

GPU (Graphics Processing Unit) – графічний процесор.

HKLM (HKEY_LOCAL_MACHINE) – системна гілка реєстру Windows.

IAM (Identity and Access Management) – управління ідентичністю та доступом.

LPE (Local Privilege Escalation) – локальна ескалація привілеїв.

MMO (Massively Multiplayer Online) – масова багатокористувацька онлайн-гра.

ВСТУП

Проблематика піратства у кіберспорті є надзвичайно актуальною в умовах стрімкого розвитку цифрової економіки та глобалізації ігрової індустрії. Кіберспорт перетворився на повноцінну галузь із мільярдними оборотами, що поєднує технології, бізнес і масову культуру. Зростання кількості користувачів, розширення платформ цифрової дистрибуції та інтенсивна комерціалізація змагань створюють сприятливе середовище для виникнення і поширення піратських практик. Незаконне копіювання ігор, маніпуляції з ліцензіями, обхід DRM-захисту та несанкціоноване втручання у турнірне програмне забезпечення безпосередньо впливають на фінансову стабільність компаній-розробників і організаторів кіберспортивних подій. Крім економічних аспектів, піратство у кіберспорті становить значну загрозу для інформаційної безпеки. Поширення модифікованих клієнтів, зламаних ігрових акаунтів та нелегальних серверів призводить до витоку персональних даних, втрати цифрових активів гравців і можливості здійснення кібератак через компрометоване програмне забезпечення. З технічного погляду, кіберспорт оперує складними клієнт-серверними архітектурами, уразливість яких може бути використана як канал для поширення шкідливого коду або несанкціонованого контролю над обчислювальними ресурсами користувачів.

Мета і завдання дослідження. Метою дослідження є обґрунтування, розроблення та систематизація методів і засобів запобігання піратству в кіберспорті шляхом аналізу технічних, організаційних та правових механізмів захисту ігрових платформ.

Досягнення визначеної мети передбачає вирішення таких завдань:

- проаналізувати особливості піратства у сфері відеоігор;
- здійснити аналіз еволюції антипіратських технологій;
- оцінити перспективи розвитку систем захисту відеоігор;
- проаналізувати нормативно-правові аспекти протидії;
- дослідити вразливості сучасних ігрових рушіїв та середовищ виконання;
- проаналізувати проблеми drm-систем і можливості обходу ліцензійних

механізмів;

– вивчити вразливості клієнт-серверної архітектури ігрових платформ;

– здійснити детальний аналіз вразливостей популярних ігрових платформ та відомих вразливостей;

– дослідити принципи й особливості експлуатації методу baitandswitch;

– розробити методику запобігання піратству в кіберспорті;

Об’єкт дослідження – процес функціонування кіберспортивних систем і платформ.

Предмет дослідження – сукупність методів, технологій, механізмів та практик, спрямованих на виявлення, попередження й мінімізацію проявів піратства у кіберспорті.

Методи досліджень. Для розв’язання поставлених задач у даній кваліфікаційній роботі використано: теоретичний аналіз наукових джерел, технічної документації та актуальних звітів з кібербезпеки, методи порівняльного аналізу, методи технічного аналізу CVE-звітів.

Наукова новизна одержаних результатів. У роботі систематизовано та класифіковано сучасні вразливості ігрових рушіїв, античит-систем і клієнт-серверної архітектури з позицій ризиків безпеки інформаціних систем, запропоновано методи заходів для підвищення кібербезпеки ігрових платформ.

Практичне значення отриманих результатів. Практичне значення полягає у можливості застосування отриманих результатів для підвищення безпеки сучасних ігрових платформ, захисту ігрового контенту та стабільності кіберспортивної екосистеми.

Публікації та апробація кваліфікаційної роботи.

1. Багмет В.С. Дослідження механізмів піратства в кіберспорті та стратегії запобігання/ Матеріали науков-практичного симпозіуму «ЗАХИСТ ІНФОРМАЦІЇ», Тернопіль, 2024. – С. 96-98.

2. Багмет В.С, Дзядик В.А. Game vulnerabilities як загроза кібербезпеки / Збірник матеріалів науково-практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп’ютерно-інтегровані технології»(КБКІТ-2025), Тернопіль, 2025. - С. 81-84.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Піратство у відеоіграх

Проблематика піратства у сфері відеоігор зберігає свою актуальність від моменту становлення ігрової індустрії. З появою персональних комп'ютерів і консолей у 1980–1990-х роках несанкціоноване копіювання та поширення програмного забезпечення набуло масового характеру. Це явище зумовило значні фінансові втрати для компаній-розробників і видавців, а також уповільнило інноваційні процеси у галузі. У відповідь на такі виклики виробники почали впроваджувати технічні й організаційні механізми захисту авторських прав, спрямовані на запобігання несанкціонованому копіюванню й використанню програмного коду.

Розвиток мережевих ігор у 2000-х роках створив нові виклики для забезпечення інформаційної безпеки продуктів і контролю за їх легальним розповсюдженням. Поширення цифрових платформ, таких як Steam, полегшило легальний доступ користувачів до ігор, але водночас відкрило нові можливості для незаконного обігу контенту[1]. У відповідь IT-компанії почали застосовувати сучасні інструменти захисту, серед яких визначальне місце посіли технології керування цифровими правами (DRM) та антипіратські програмні рішення. Незважаючи на активний розвиток таких систем, піратство залишається поширеним явищем, оскільки вдосконалення захисних механізмів супроводжується одночасним удосконаленням методів їх обходу.

Піратство трактується як несанкціоноване відтворення, розповсюдження або використання об'єктів, захищених авторським правом, включно з відеоіграми. Його вплив виходить за межі діяльності розробників та видавців, охоплюючи весь ланцюг учасників індустрії — від інвесторів до кінцевих користувачів. Сфера відеоігор є одним із найбільш прибуткових секторів цифрової економіки, де розроблення, тестування та просування продуктів потребує значних інвестицій. Поширення неліцензійних копій безпосередньо знижує прибутковість компаній, ускладнює повернення інвестицій і зменшує мотивацію до подальших розробок.

З економічної позиції скорочення обсягів продажу легального контенту впливає на якість майбутніх продуктів. Відсутність фінансової віддачі стримує впровадження нових технологій, розвиток графічних рушіїв і вдосконалення ігрових механік. Таким чином, зростання рівня піратства негативно позначається не лише на комерційній діяльності компаній, а й на загальному темпі технологічного прогресу галузі.

Відповідно до дослідження Центру глобальної інноваційної політики Торгової палати США (2019 р.)[2], щорічні втрати економіки США від онлайн-піратства становлять близько 29,2 млрд доларів у вигляді недоотриманих доходів. У свою чергу, аналітична компанія Newzoo прогнозує, що обсяг світового ринку відеоігор перевищить 200 млрд доларів до 2023 року. Такі економічні показники засвідчують потребу у формуванні комплексної стратегії правового, технічного та організаційного захисту цифрових продуктів, спрямованої на зменшення рівня піратства та підтримання стійкості індустрії в умовах динамічного технологічного розвитку.

1.2 Технології захисту ігор від піратства

Одним із найпоширеніших технологічних рішень для захисту відеоігор від несанкціонованого копіювання є система DRM (Digital Rights Management), яка ґрунтується на шифруванні ігрового коду та контролі легальності копій. Такий механізм забезпечує перевірку автентичності програмного продукту під час його запуску або під час доступу до мережевих компонентів, що істотно ускладнює створення й використання піратських версій. Водночас технологія DRM нерідко піддається критиці через підвищене навантаження на обчислювальні ресурси користувача та потенційні ризики порушення конфіденційності персональних даних.

Паралельно з удосконаленням технічних механізмів розробники вдаються до зміни бізнес-моделей розповсюдження контенту. Моделі free-to-play та підпискові сервіси передбачають безкоштовний доступ до базової версії гри з подальшою монетизацією через мікротранзакції або додатковий контент. Такий

підхід забезпечує більшу доступність продуктів для широкої аудиторії та зменшує економічну мотивацію користувачів до незаконного копіювання[3].

Попри постійне вдосконалення антипіратських технологій, повна технічна гарантія захисту від несанкціонованого розповсюдження залишається недосяжною. Практика свідчить, що навіть найскладніші системи з часом піддаються зламу. Показовим прикладом є система StarForce, розроблена у середині 2000-х років, яка застосовувала низькорівневі драйвери та спеціальні нечитаємі сектори на оптичних дисках для запобігання копіюванню. Попри високий рівень захисту, система отримала значну критику через проблеми сумісності з операційними системами та випадки пошкодження користувацьких середовищ.

Подальший розвиток технологій привів до появи сучасніших рішень, серед яких Denuvo Anti-Tamper посідає провідне місце. Дана технологія, застосована у таких відомих проєктах, як FIFA, Assassin’s Creed та Resident Evil, використовує методи глибокого шифрування ігрового коду та багаторівневої обфускації, що значно ускладнює процес реверс-інжинірингу. На початкових етапах Denuvo продемонструвала високу ефективність: низка ігор залишалася захищеною від піратства протягом кількох місяців після релізу. Проте у 2016 році було зафіксовано випадок обходу системи, коли незалежний дослідник, відомий під псевдонімом Voksi, знайшов спосіб запуску піратських копій Doom, Total War: Warhammer та Just Cause 3 через платформу Steam. Після усунення вразливості вже за короткий час інша хакерська група — CONSPIR4CY — оприлюднила повністю зламану версію Rise of the Tomb Raider, яка до цього вважалася практично захищеною від нелегального копіювання[4].

Таким чином, еволюція антипіратських технологій свідчить про безперервне протистояння між розробниками систем захисту та фахівцями, які прагнуть їх обійти. Повна технічна ізоляція ігор від копіювання залишається недосяжною, однак поєднання DRM-рішень, мережевої автентифікації та адаптивних бізнес-моделей, орієнтованих на зручність і доступність користувача, дозволяє істотно знизити масштаби незаконного розповсюдження цифрового контенту та підвищити економічну стабільність галузі.

1.3 Альтернативні підходи та сучасні тенденції

На сучасному етапі розвитку індустрії відеоігор найвищу стійкість до піратства демонструють масові багатокористувацькі онлайн-ігри (MMO) та кіберспортивні дисципліни, функціонування яких базується на розподіленій серверній інфраструктурі та постійній взаємодії клієнтських додатків із центральними серверами. У таких системах клієнтська частина гри без підключення до серверів не має самостійної функціональної цінності, що фактично унеможливлює створення або використання повноцінних піратських копій. Додатковим елементом захисту виступає механізм мікротранзакцій, який одночасно виконує функції монетизації продукту та контролю користувацької активності, забезпечуючи автентифікацію й перевірку дій гравця на стороні сервера[5].

Попри неоднозначне сприйняття систем мікроплатежів з боку частини спільноти, вони зарекомендували себе як ефективний інструмент стабілізації бізнес-моделі розробників. Ігри на зразок Dota 2 та League of Legends доводять, що стратегія безкоштовного доступу до базової версії в поєднанні з добровільними внутрішньоігровими покупками дає змогу не лише зменшити рівень піратства, а й підтримувати сталий розвиток ігрової екосистеми.

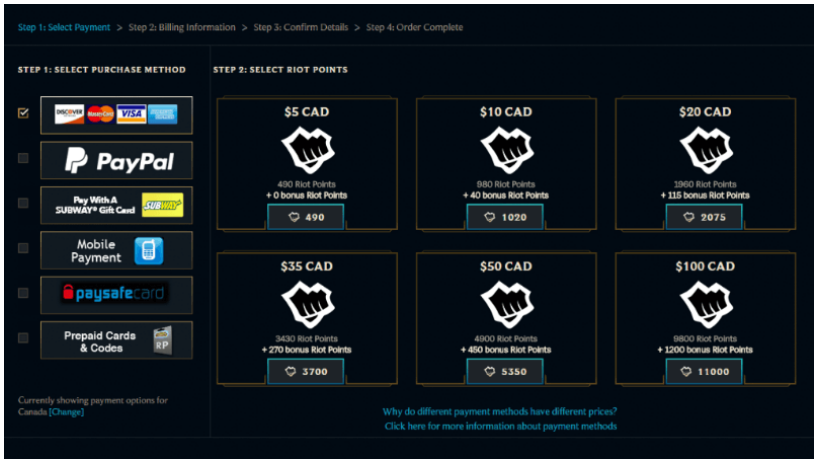


Рисунок 1.1 – Система оплати ігрового ПЗ

Така модель сприяє зростанню лояльності користувачів, стимулює тривале залучення аудиторії та забезпечує розробникам передбачувані джерела доходу без необхідності застосування надмірно жорстких технічних обмежень.

1.4 Еволюція підходів до антипіратського захисту та досвід розробників

Одним із додаткових напрямів зменшення рівня піратства у відеоігровій індустрії є регулярне оновлення контенту. У випадках, коли структура гри передбачає динамічні зміни контенту та постійне підключення до серверів, піратські копії швидко втрачають актуальність. Користувачі, які використовують нелегальні версії, змушені повторно завантажувати значні обсяги даних або залишатися без доступу до оновлень, що створює додаткові незручності й поступово знижує мотивацію користування піратськими ресурсами. Відсутність автоматичного оновлення та затримка в отриманні нових версій чи додаткових матеріалів зменшує привабливість неліцензійних копій, роблячи офіційні джерела контенту більш зручними та безпечними.

Деякі розробники усвідомлюють, що повне викорінення піратства в умовах цифрової економіки є малоймовірним, і намагаються адаптуватися до цього явища. Показовим є експеримент незалежної студії RedLynx, яка в день релізу власноруч розмістила піратську версію своєї гри у файлообмінних мережах. Єдиною відмінністю цієї копії була відсутність ключової функції — таблиці лідерів, тісно пов’язаної з серверною частиною гри. Такий підхід дав змогу зберегти інтерес користувачів до офіційної версії, адже лише вона забезпечувала повноцінну участь у спільноті гравців. Як зазначив генеральний директор студії, піратство вже стало частиною цифрової культури, тому доцільно використовувати його як інструмент маркетингу та залучення потенційних покупців[6].

Результати цього експерименту підтвердили ефективність подібного підходу: протягом перших вісімнадцяти місяців після релізу було продано понад 150 тисяч ліцензійних копій, тоді як піратська версія так і не отримала доступу до головного елементу гри — онлайн-таблиці лідерів. Досвід RedLynx засвідчив,

що поєднання технічних і соціальних стратегій може не лише зменшити негативний вплив піратства, а й сприяти зростанню продажів за рахунок формування спільнотної взаємодії та відчуття справжньої участі в ігровому процесі.

1.4.1 Початок розвитку антипіратського захисту

Період становлення антипіратського захисту у відеоіграх охоплює 1980–1990-ті роки, коли ринок тільки формувався. Перші ігри для платформ ZX Spectrum і Commodore 64 поширювалися на магнітних касетах, що робило їх копіювання технічно нескладним. Для створення дублікатів достатньо було побутового двокасетного магнітофона, тому несанкціоноване копіювання стало масовим явищем без жодних технологічних бар'єрів. Навіть перехід до дискет і компакт-дисків не усунув цієї проблеми, адже засоби дублювання залишалися доступними широкому колу користувачів[7].

Попри поширеність піратства, ринок ігор для Commodore 64 залишався стабільним і привабливим для розробників. Зниження інтересу до платформи зумовлювалося не зростанням обсягів нелегального копіювання, а появою більш потужних персональних комп'ютерів на базі DOS у середині 1990-х років.

На межі 1980–1990-х років розробники використовували переважно аналогові методи перевірки автентичності, які мали підтвердити наявність оригінальної копії гри. Одним із найвідоміших прикладів є Pool of Radiance, що постачалася з картонним «кодним колесом». Перед запуском гри користувач мав обрати правильну комбінацію рун, що відповідала даним на диску, — це мало підтвердити законність копії. Подібні механізми створювали видимість контролю автентичності, хоча фактично не забезпечували ефективного захисту від копіювання[8].

Попри технічну примітивність, саме ці ранні рішення заклали основу подальшого розвитку систем цифрового захисту. Аналогові засоби поступово були витіснені цифровими технологіями, що передбачали використання серійних ключів, перевірку наявності оригінального носія, а згодом — інтеграцію DRM-механізмів і мережевої автентифікації. Така еволюція

визначила напрямок формування сучасних систем безпеки у відеоігровій індустрії, які поєднують програмно-апаратні технології, економічні моделі та комунікаційні стратегії взаємодії зі спільнотою гравців.

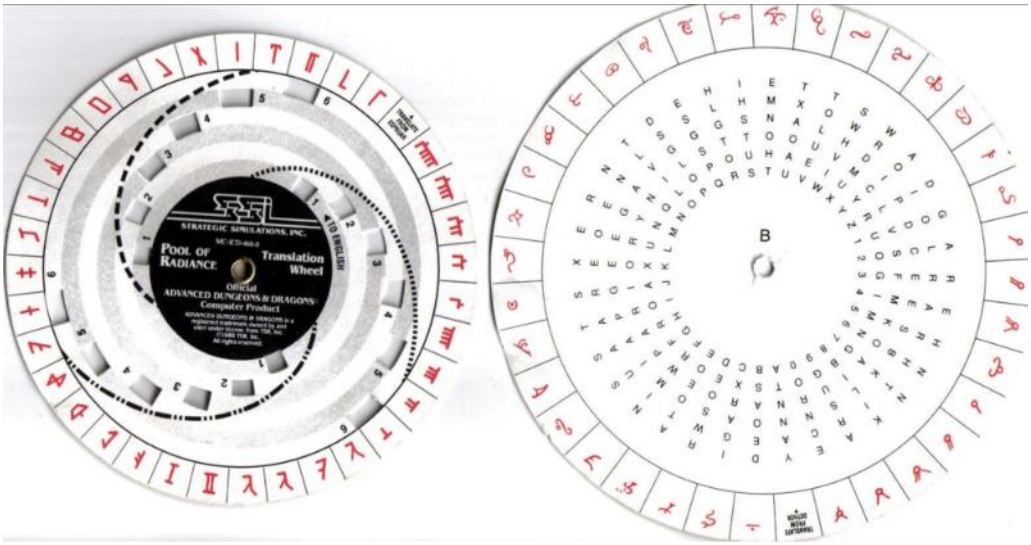


Рисунок 1.2 – Система захисту з використанням “Кодових коліс”

У пізніх 1980-х роках одним із найпоширеніших методів протидії несанкціонованому копіюванню ігор стало використання так званих «кодових коліс» — фізичних елементів автентифікації, відтворення яких вимагало спеціальних матеріальних засобів. Сутність цього підходу полягала у створенні об’єктів, що поєднували механічну складність виготовлення з інтеграцією у сам ігровий процес. Прикладом є гра Zany Golf, у якій використовувалася система з двох концентричних картонних дисків — зовнішнього та внутрішнього. Уздовж країв кожного з них були нанесені різні терміни, тоді як внутрішній диск містив вирізані віконця, розташовані по спіралі. Під час гри користувач отримував завдання вирівняти зазначені терміни із зовнішнього й внутрішнього кіл відповідно до інструкції, після чого у відповідному віконці з’являвся код, який необхідно було ввести для продовження гри. Для підсилення ефекту автентичності розробники застосували тематичну термінологію, безпосередньо пов’язану з гольфом, що підкреслювало стилістику гри.

Інноваційним для свого часу став підхід, реалізований у Alone in the Dark 2, де замість традиційного колеса використовувалася система ігрових карт. Цей

елемент водночас виконував функцію перевірки ліцензійності та доповнював художнє оформлення гри. У комплекті з продуктом постачався набір двосторонніх карт із різними мастями, значеннями та вирізаними отворами, розташованими у довільному порядку. Під час проходження гравець отримував завдання накласти дві карти певним чином (наприклад, «покласти трійку бубен поверх дами пік») і зчитати символ, що з'являвся у вікні на визначеній позиції[9].

Подібна система забезпечувала високу варіативність комбінацій, роблячи несанкціоноване відтворення практично неможливим. Використання кольорового кодування мастей додатково ускладнювало копіювання, оскільки більшість копіювальних пристроїв того часу працювали лише у чорно-білому режимі. Таким чином, фізичні елементи захисту — кодові диски, ігрові карти або спеціальні таблиці — стали ефективним засобом антипіратської політики періоду, який поєднував технічні обмеження з інтерактивними компонентами ігрового процесу, формуючи унікальне поєднання практичного захисту та дизайнерського рішення.

Рисунок 1.3 – Система захисту з використанням "Ручного пошуку"

Одним із найпоширеніших методів антипіратського захисту у відеоіграх 1980–1990-х років став так званий «ручний пошук» (manual lookup). Сутність

цього підходу полягала у необхідності звернення користувача до фізичного посібника чи інструкції, що постачалися разом із ліцензійною копією гри. Такий метод створював прямий зв’язок між програмним продуктом і матеріальними компонентами комплектації, роблячи використання нелегальних копій менш зручним або взагалі неможливим.

Подібна техніка широко застосовувалася у низці відомих проєктів того періоду, зокрема у Populous, X-Com: UFO Defense, Railroad Tycoon та Prophecy. У грі Populous користувачу на певному етапі демонструвався герб одного з ігрових світів, після чого необхідно було ввести назву цього світу. Відповідний герб розміщувався на сторінках офіційного посібника, тож гравець мав фізично перегортати сторінки, щоб знайти правильний символ. Подібний механізм, попри свою простоту, виявився ефективним, оскільки вимагав наявності оригінальної документації[10].

У грі Sim City реалізовано більш складну форму автентифікації. До коробкового видання додавалася спеціальна таблиця High Scores, розміщена на кількох сторінках і така, що містила десятки кодів. Під час перевірки гра відображала інформацію про певне місто (населення, назву тощо), а користувач мав знайти відповідний запис у таблиці й ввести код. Для унеможливлення копіювання таблиця була надрукована чорним шрифтом на червоному фоні, що робило її нечіткою для копіювальних пристроїв, які у той час працювали переважно у чорно-білому режимі.

У деяких іграх використовувався спрощений формат ручного пошуку — підказка одразу містила посилання на сторінку чи абзац посібника. Так, у X-Com: UFO Defense пропонувалося знайти код на певній сторінці, тоді як в інших проєктах потрібно було ввести конкретне слово з визначеного рядка або абзацу. Цей підхід виконував подвійну функцію: забезпечував базовий рівень перевірки ліцензійності та підсилював відчуття автентичності, створюючи зв’язок між цифровим і матеріальним компонентами гри[11].

У подальшому подібна форма захисту виявилася малоефективною. З появою цифрових перевидань та електронних збірок старих ігор механізм ручного пошуку часто втрачав працездатність через зміщення нумерації сторінок

або зміну верстки. Внаслідок цього захисні функції втрачали сенс, і видавці змушені були публікувати коректні відповіді у відкритому доступі чи додавати їх у цифрові версії продуктів. Таким чином, «ручний пошук» став перехідним етапом між аналоговими й цифровими методами антипіратського захисту, відображаючи спроби індустрії поєднати фізичну автентифікацію з програмною логікою у добу становлення комп'ютерних ігор.

Рисунок 1.4 – Система захисту UFO Defence

Цікавим і водночас унікальним для свого часу методом автентифікації стала система, реалізована у грі Ultima VI. Разом із ліцензійною копією гри користувач отримував високоякісну тканинну карту світу, надруковану з великою точністю та художньою деталізацією. У процесі гри гравцеві пропонувалося визначити координати певного міста, позначеного на цій карті. Усі написи були виконані рунічним шрифтом, що робило завдання додатково інтерактивним: спочатку необхідно було розшифрувати руни, а потім знайти відповідне місце на карті[11].

Після визначення населеного пункту користувач мав обчислити його широту та довготу за допомогою шкали, нанесеної на самій карті, і ввести координати у програму. Такий підхід вимагав часу, однак сприяв глибшому зануренню у віртуальний світ, поєднуючи перевірку автентичності з

геймплейною взаємодією. Механізм автентифікації ставав невід'ємною частиною ігрового процесу, виконуючи не лише технічну, а й наративну функцію, що посилювала відчуття залученості до подій гри.

Подібні рішення відображають творчий підхід розробників до проблеми піратства в умовах обмежених технологічних можливостей. Замість запровадження виключно обмежувальних бар'єрів, розробники інтегрували елементи перевірки ліцензійності у структуру геймплею, створюючи синергію між автентифікацією та ігровим дизайном. Такий підхід можна вважати передвісником сучасних стратегій, коли антипіратські технології інтегруються у користувацький досвід так, щоб не порушувати його цілісності й водночас підсилювати художню складову гри.

Рисунок 1.5 – Система захисту Ultima VI

Доволі цікавий, але водночас жорсткий підхід до антипіратського захисту було реалізовано у відеогрі EarthBound, створеній компанією Nintendo. Розробники впровадили поведінкову систему автентифікації, що поєднувала технічні й психологічні елементи протидії піратству. Механізм захисту функціонував на основі аналізу автентичності носія та середовища запуску: якщо гра виявляла невідповідність оригінальним параметрам або ознаки несанкціонованого копіювання, рівень складності автоматично підвищувався у декілька разів[12].

Після активації захисного механізму у грі з'являлася значно більша кількість супротивників, а їхні характеристики — сила, витривалість і частота атак — перевищували стандартні показники. Таким чином, проходження ставало майже неможливим навіть для досвідчених гравців. Така модель мала подвійний ефект: з одного боку, вона безпосередньо карала користувача за використання піратської версії, а з іншого — створювала ілюзію підвищеного ігрового виклику, який на початкових етапах міг сприйматися як особливість дизайну гри.

Найрадикальнішим елементом системи була фінальна перевірка автентичності. Якщо користувачеві все ж вдавалося подолати численні бої й дістатися до фінального боса, гра навмисно провокувала зупинку процесу з подальшою рекомендацією перезапуску. Після цього здійснювалося повне видалення всіх збережених даних, що фактично нівелювало результати проходження та унеможливлювало відновлення прогресу.

Таким чином, компанія Nintendo створила приклад комплексного антипіратського рішення, у якому технічні засоби захисту поєднувалися з поведінковими стимулами. Подібна стратегія не лише перешкоджала поширенню неліцензійних копій, а й мала символічне значення, демонструючи своєрідне «покарання» за порушення авторських прав[13].

Приклад EarthBound є показовим для середини 1990-х років, коли розробники почали застосовувати не лише технічні бар'єри, а й креативні психологічні механізми взаємодії з користувачем. Такі рішення свідчать про еволюцію підходів до антипіратського захисту — від прямого обмеження до

інтеграції захисних елементів у структуру геймплею, що перетворювало сам процес перевірки ліцензійності на частину ігрового досвіду.

1.4.2 Перехід до цифрових форм антипіратського захисту: епоха SecuROM

Початок 2000-х років став періодом глибокої технологічної трансформації у сфері відеоігор. Відбувався поступовий відхід від фізичних носіїв — компакт-дисків, картриджів та інших матеріальних форматів — на користь цифрового розповсюдження та онлайн-платформ. Розвиток високошвидкісного інтернету, вдосконалення технологій зберігання даних і алгоритмів шифрування створили сприятливе середовище для зростання ринку цифрового контенту. Водночас саме ці процеси зумовили стрімке збільшення масштабів піратства, яке почало завдавати значних економічних збитків виробникам програмного забезпечення.

У 2000-х роках основним каналом поширення неліцензійного контенту стали файлообмінні мережі та торрент-треки, які забезпечували миттєве копіювання і передачу даних між користувачами. Якщо раніше отримання гри вимагало фізичного доступу до носія, то в епоху цифрової дистрибуції створення та розповсюдження копій стало майже безконтрольним. Це спонукало видавців і розробників до активного пошуку нових способів захисту своїх продуктів.

Одним із найвідоміших рішень у цій сфері стала система SecuROM, розроблена компанією Sony DADC — дочірнім підрозділом корпорації Sony Corporation. Технологію вперше представлено у 1997 році, однак саме у 2000-х вона отримала найширше застосування. Її основною метою було запобігання несанкціонованому копіюванню оптичних дисків і перевірка автентичності ліцензійних копій під час інсталяції програмного забезпечення. Принцип роботи базувався на механізмі цифрового підпису, який дозволяв перевірити справжність диска перед запуском або встановленням гри. У разі виявлення невідповідності інсталяція блокувалася, що забезпечувало певний рівень захисту, хоча й створювало додаткові обмеження для користувачів[14].

Система SecuROM застосовувалася у низці комерційно успішних і водночас популярних ігор, серед яких The Sims, Spore, BioShock, Batman: Arkham Asylum, Mass Effect та Grand Theft Auto IV. Особливо відомим став випадок із

грою Spore, виданою компанією Electronic Arts. Незважаючи на впровадження SecuROM, вона побила рекорди за кількістю піратських копій — лише протягом перших десяти днів після виходу було завантажено понад 500 тисяч неліцензійних версій. Цей парадокс став предметом активного обговорення у професійній спільноті (PC Gamer, 2008) і продемонстрував, що надмірна технічна жорсткість DRM може мати протилежний ефект.

Технологія SecuROM викликала численні нарікання через зниження продуктивності системи, проблеми сумісності та ризики пошкодження операційного середовища користувача. Деякі користувачі повідомляли про збої в роботі оптичних приводів, а в окремих випадках — про неможливість запуску легальних копій ігор. Це спричинило появу неофіційних модифікацій і патчів, що вимикали захисні функції, та сформувало негативне ставлення до самої технології, яку в інтернет-спільнотах почали іронічно називати «SuckuROM».

Паралельно із SecuROM у той самий період активно використовувався механізм CD-ключів, що передбачав введення унікального серійного номера під час інсталяції або мережевої активації гри. Такий підхід забезпечував базовий рівень контролю за поширенням копій і став основою для подальшої еволюції цифрових DRM-систем, таких як Steam DRM, Origin чи Denuvo.

Епоха SecuROM стала перехідним етапом між аналоговими методами захисту та сучасними цифровими DRM-рішеннями. Вона продемонструвала, що ефективність антипіратських технологій безпосередньо залежить від балансу між безпекою та зручністю користування. Надмірне обмеження функціональності призводить до зворотного ефекту — зростання рівня піратства та втрати довіри користувачів. Саме досвід SecuROM сформував підґрунтя для появи нової генерації DRM-технологій, орієнтованих не лише на контроль, а й на створення комфортного, стабільного та легітимного користувацького середовища[15].

1.4.3 Еволюція антипіратських технологій у 2000–2020-х роках: від модифікації консолей до онлайн-активації

Початок XXI століття став визначальним етапом для еволюції засобів антипіратського захисту у відеоігровій індустрії. На початку 2000-х років провідними платформами залишалися PlayStation 2, Xbox та Nintendo GameCube, для яких піратство стало не менш серйозною проблемою, ніж у середовищі персональних комп'ютерів. Попри посилення технічних обмежень і перевірок автентичності, розповсюдження нелегальних копій тривало, що призвело до виникнення явища модифікації ігрових консолей (mod-чипінгу).

Суть цього підходу полягала у встановленні до апаратної частини пристрою неофіційних мікросхем, які обходили регіональні блокування, DRM-механізми та захисні перевірки. Це дозволяло відтворювати скопійовані або імпортовані ігри без перевірки ліцензійності. Хоча процес модифікації вимагав певних технічних навичок, він набув масового поширення, поставивши виробників перед серйозним викликом. Поява нових консолей із можливістю підключення до інтернету надала компаніям додаткові інструменти протидії. Через систему оновлень виробники могли віддалено блокувати роботу зламаних пристроїв або виводити їх з ладу, що зробило втручання в апаратне забезпечення високоризикованою практикою.

Паралельно розвивалися онлайн-платформи розповсюдження контенту, серед яких провідні позиції зайняли Steam і Xbox Live. Їх поява започаткувала нову еру цифрової дистрибуції та змінила бізнес-модель галузі: продаж фізичних носіїв поступово поступався місцем DLC (Downloadable Content), мікротранзакціям і сервісним підпискам. Такі механізми не лише розширили джерела доходу, а й підвищили рівень контролю над користувацькими обліковими записами, зменшуючи стимули до піратства.

На початку 2010-х років активне зростання мобільного геймінгу та розвиток платформ Steam, Origin і App Store призвели до поступової відмови від традиційних DRM-систем, заснованих на фізичних носіях. Їм на зміну прийшли механізми онлайн-активації та автентифікації через облікові записи користувачів, що дозволили здійснювати централізований контроль ліцензій і обмежувати доступ до контенту у випадку порушень. Така модель підвищила

рівень безпеки, проте водночас викликала низку конфліктів, пов’язаних із надмірним контролем над користувачем[16].

У 2012–2013 роках зафіксовано низку критичних випадків, які продемонстрували межі ефективності DRM, що порушує ігровий досвід. Найвідомішим прикладом стала ситуація з Diablo III, де компанія Blizzard впровадила політику обов’язкового постійного підключення до інтернету, навіть для одиночного режиму. Сервери не витримували навантаження, користувачі втрачали доступ до гри, а неможливість створення локальних модифікацій викликала масове невдоволення. Аналогічна ситуація спостерігалася у грі SimCity (2013) від Electronic Arts, де вимога постійного інтернет-з’єднання призвела до численних технічних збоїв. Після хвилі критики компанія була змушена публічно вибачитися та впровадити офлайн-режим.

Ці випадки стали поворотними моментами у розвитку цифрового захисту, засвідчивши необхідність балансу між безпекою та зручністю користування.

1.4.4 Креативні антипіратські рішення

У відповідь на зростаюче невдоволення користувачів деякі студії почали застосовувати нетрадиційні, поведінкові форми захисту, інтегруючи антипіратські механізми безпосередньо у геймплей.

Компанія Nintendo, після збитків на понад 1 мільярд доларів США від неліцензійних копій ігор серії Pokémon Diamond, Pearl і Platinum, реалізувала внутрішньоігрові механізми, які обмежували функціональність піратських версій. У наступних релізах (HeartGold, SoulSilver) у разі виявлення неліцензійної копії бої ставали неможливими, а у версіях Black і White — покемони переставали отримувати досвід.

Розробники Maxis у грі The Sims 4 впровадили іронічний ефект: якщо система виявляла нелегальну копію, «піксельна цензура», що з’являється під час гігієнічних дій персонажів, поступово розповсюджувалася на весь екран, роблячи гру непридатною для користування.

У Game Dev Tycoon (2013) антипіратський захист став частиною самого ігрового сценарію — якщо система виявляла піратську версію, студія гравця

втрачала прибуток через «піратів», які масово копіюють її продукти. Таким чином, користувач безпосередньо стикався з наслідками порушення авторського права.

Компанія Rocksteady у грі Batman: Arkham Asylum застосувала прихований механізм: у неліцензійних копіях плащ героя не розкривався, унеможливлюючи проходження певних ділянок. Один із користувачів, звернувшись на форум за допомогою, отримав відповідь адміністратора: «Це не помилка гри — це збій вашого морального коду».

Аналогічні рішення впровадила Rockstar North у Grand Theft Auto IV: у піратських копіях камера оберталася хаотично, транспортні засоби ламалися при спробі руху, а деякі місії залишалися недоступними.

Нарешті, у The Witcher 2: Assassins of Kings реалізовано унікальний гумористичний підхід: у неліцензійних версіях сцени романтичного характеру модифікувалися — партнерку головного героя замінювала літня жінка, що створювало комічний, але водночас виховний ефект[17].

Еволюція DRM-технологій у 2000–2020-х роках демонструє поступовий перехід від апаратних обмежень до онлайн-активації, інтегрованих сервісів та поведінкових моделей захисту. Досвід впровадження рішень — від SecuROM до Steam DRM і Denuvo — підтвердив, що ефективність антипіратських технологій залежить від їхньої збалансованості між безпекою та користувацьким комфортом.

Сучасна індустрія відійшла від концепції жорсткого контролю на користь екосистемної безпеки, яка поєднує серверну аутентифікацію, хмарні сервіси, мікротранзакції, регулярні оновлення контенту та соціальну взаємодію користувачів. Такий підхід не лише знижує рівень піратства, а й формує довготривалу економічну стійкість і взаємну довіру між розробником і споживачем, визначаючи нову парадигму захисту цифрових продуктів у глобальному ігровому середовищі.

1.5 Перспективи розвитку систем захисту відеоігор

На сучасному етапі розвитку цифрової індустрії відеоігор провідну роль у забезпеченні антипіратського захисту відіграє механізм онлайн-активації, який передбачає обов’язкову реєстрацію користувача в системі розробника або видавця. Під час активації відбувається верифікація ліцензії через захищений сервер, що дозволяє підтвердити законність придбання гри та контролювати кількість пристроїв, на яких вона встановлена. Такий підхід не лише мінімізує ризики масового поширення неліцензійних копій, але й забезпечує постійний моніторинг використання продукту протягом усього життєвого циклу.

Іншим перспективним напрямом є впровадження удосконалених методів шифрування та перевірки цілісності даних, які використовують складні криптографічні алгоритми. Такі рішення унеможливлюють реверс-інжиніринг і модифікацію ігрових файлів, що значно ускладнює створення зламаних версій або несанкціонованих копій. Водночас, висока ступінь захисту створює додаткові обмеження для спільноти модифікаторів (modders), ускладнюючи внесення користувацьких змін у гру. Це формує дискусію навколо відкритості ігрового контенту, де інтереси збереження авторських прав розробників стикаються з культурою творчої взаємодії користувачів.

Особливого значення набуває розвиток систем післярелізного контенту (DLC, Downloadable Content) як складової сучасної бізнес-моделі. Механізм розширень дозволяє підтримувати інтерес до гри після виходу, продовжувати життєвий цикл продукту та забезпечувати стабільний фінансовий потік без необхідності створення нового проєкту. DLC стало не лише інструментом монетизації, але й елементом інтегрованої системи захисту, оскільки завантаження доповнень передбачає проходження процедур автентифікації та підтвердження прав користувача.

Сучасні DRM-рішення поступово переходять до інтегрованих багаторівневих моделей, у яких контроль безпеки охоплює не лише основну гру, але й усі додаткові компоненти — DLC, мікротранзакції, сезонні оновлення та онлайн-події. Характерним прикладом є технологія Denuvo SecureDLC,

розроблена компанією Irdeto. Вона замінює стандартні перевірки прав доступу, які зазвичай здійснюються платформами цифрової дистрибуції (Steam, Epic Games Store), на власний криптографічно захищений механізм аутентифікації. SecureDLC виступає проміжним рівнем між грою та платформою, здійснюючи шифровану перевірку ліцензійних прав користувача і запобігаючи несанкціонованому розблокуванню платного контенту[18].

Таким чином, еволюція антипіратських технологій у сучасній відеоіндустрії орієнтована не на створення ізольованих систем захисту, а на побудову комплексної екосистеми цифрової безпеки. У межах цієї моделі кожен компонент гри — від клієнтської програми до додаткових матеріалів — інтегрується в єдину систему перевірки, що поєднує серверну автентифікацію, шифрування даних та регулярне оновлення контенту. Такий підхід формує баланс між технологічною ефективністю та користувацькою зручністю, забезпечуючи одночасно правову стійкість, комерційну життєздатність і довготривалу взаємодію між розробником і споживачем.

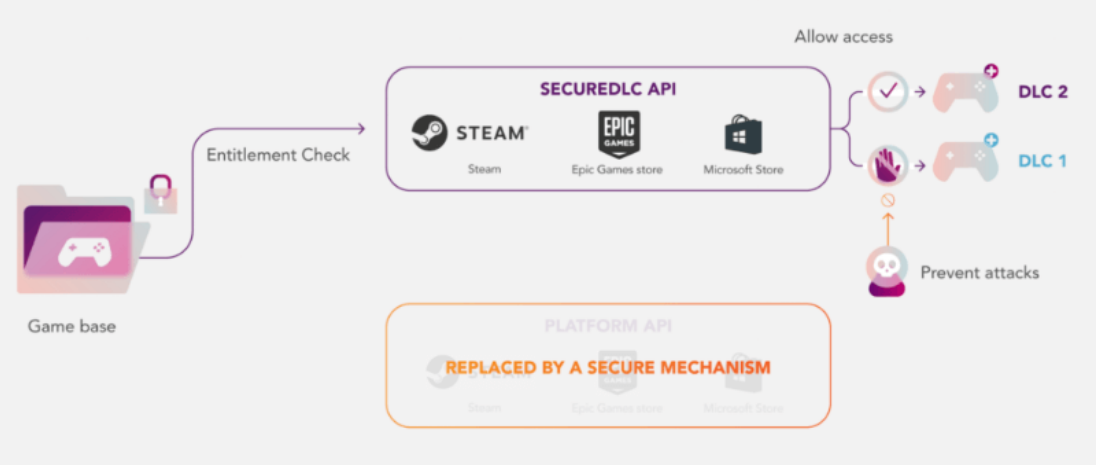


Рисунок 1.6 – Модель єдиної системи перевірки

Поряд із технічними рішеннями, спрямованими на запобігання несанкціонованому копіюванню програмного забезпечення, правові інструменти залишаються фундаментальним елементом системи захисту інтелектуальної власності у сфері відеоігор. Юридичний аспект є невід'ємною складовою комплексної антипіратської політики, оскільки саме він забезпечує узгодженість

між технологічними обмеженнями та правовими механізмами впливу на порушників.

У Сполучених Штатах Америки ключовим нормативно-правовим актом у цій сфері є Закон про авторське право в цифрову епоху (Digital Millennium Copyright Act, DMCA), ухвалений у 1998 році. DMCA визначає правові підстави захисту авторських прав на цифровий контент, включно з відеоіграми, програмним забезпеченням та іншими інтерактивними медіа. Закон надає розробникам і видавцям право ініціювати процедуру офіційного повідомлення про видалення контенту (takedown notice), яка зобов'язує власників вебсайтів або хостинг-провайдерів негайно припинити поширення піратських копій після отримання звернення правовласника. Такий механізм дозволяє забезпечити оперативне реагування без судового втручання на початкових етапах, що робить DMCA одним із найефективніших інструментів у практиці міжнародного цифрового права.

У Європейському Союзі аналогічну роль відіграє Директива 2001/29/ЕС про гармонізацію певних аспектів авторського права і суміжних прав у цифрову добу, яка встановлює загальні стандарти правового захисту комп'ютерних програм і відеоігор. Документ передбачає право правовласників вимагати блокування доступу до нелегального контенту, ініціювати судове переслідування порушників та зобов'язує інтернет-провайдерів співпрацювати з уповноваженими органами у виявленні джерел піратського розповсюдження. Таким чином, у межах європейського законодавства створено модель, у якій відповідальність за забезпечення правомірного цифрового обігу контенту поділяється між правовласниками, провайдерами та користувачами.

Завдяки впровадженню цих нормативних актів виробники відеоігор отримали можливість поєднувати технічні засоби DRM-захисту з правовими процедурами, що дозволяє діяти на декількох рівнях — від блокування доменів і конфіскації серверів до притягнення організаторів піратських платформ до кримінальної або цивільно-правової відповідальності.

Сучасна практика підтверджує, що найвищої ефективності у боротьбі з цифровим піратством досягають саме комплексні стратегії, які інтегрують

юридичні, технологічні та організаційні механізми захисту. Такий підхід не лише стримує розповсюдження нелегального контенту, але й формує правову культуру відповідального користування цифровими продуктами, що є ключовим чинником сталого розвитку глобальної ігрової індустрії.

2 НОРМАТИВНО ПРАВОВІ АСПЕКТИ У СФЕРІ КІБЕРСПОРТУ

2.1 Піратство у сфері кіберспорту в США

Піратство у сфері кіберспорту стало одним із ключових викликів для глобальної ігрової індустрії. На відміну від класичного розповсюдження неліцензійного програмного забезпечення, кіберспортивне піратство має багатовимірний характер і включає не лише копіювання ігор, але й незаконне використання трансляцій, підробку турнірних клієнтів, несанкціоноване створення серверів, викрадення облікових даних, а також неофіційне використання інтелектуальної власності турнірних організаторів. У сучасному контексті піратські дії в кіберспорті перетворилися на цілісну підпільну економіку, що базується на продажі несанкціонованих копій, нелегальних модифікацій, «чітів» і доступу до закритих турнірних систем.

США є одним із найбільших ринків відеоігор і водночас осередком наймасштабніших кейсів боротьби з піратством у кіберспорті. Одним із найвідоміших випадків стала справа проти групи Team Xecuter, яка розповсюджувала пристрої для обходу захисту Nintendo Switch і надавала змогу запускати піратські копії ігор, зокрема кіберспортивних дисциплін (Super Smash Bros., Rocket League). У 2022 році Міністерство юстиції США засудило організаторів групи до тюремних строків, а один із ключових фігурантів — Гері Боузер — отримав вирок із компенсацією понад 10 мільйонів доларів (U.S. Department of Justice, 2022).

Ще один напрям піратства в США пов’язаний із нелегальним стрімінгом турнірів. Під час чемпіонатів League of Legends (LCS) та CS:GO Major неодноразово фіксувалися випадки, коли сторонні платформи відтворювали відео з офіційних трансляцій без ліцензії Riot Games або ESL. Такі стріми збирали сотні тисяч переглядів і монетизувалися рекламою, порушуючи авторські права організаторів. У 2023 році компанія Riot Games подала позов проти кількох нелегальних трансляторів у США, вимагаючи компенсацію за збитки від втраченої реклами та продажів (Reuters, 2023).

Окремої уваги заслуговує проблема чіт-піратства — створення та продажу нелегальних модифікацій, які змінюють ігрову механіку. У 2021 році розробник з Каліфорнії був засуджений за продаж програм, що обходили систему захисту Overwatch та Call of Duty: Warzone. Компанія Activision довела в суді, що збитки від таких дій перевищують 3 мільйони доларів, оскільки піратські модифікації поширювалися у форматі підписки (Activision Lawsuit, 2021).

США формують прецедентну базу судових справ, яка впливає на весь ринок кіберспорту. Агресивна позиція розробників і федеральних агентств, таких як FBI Cyber Division, демонструє прагнення держави забезпечити кіберспорт правовим захистом, подібним до класичних спортивних дисциплін.

Європа, будучи другим за масштабом ринком eSports після Північної Америки, має власну специфіку у сфері піратства. Найбільш поширеною формою є створення неофіційних серверів для популярних ігор, що дозволяють обходити ліцензійні системи автентифікації. У Німеччині та Франції у 2020–2023 роках було зафіксовано понад 200 випадків розгортання піратських серверів World of Warcraft, Counter-Strike: Global Offensive і Valorant, які забезпечували доступ до гри без офіційного клієнта (European Union IP Observatory, 2023).

Значна кількість таких серверів діяла під виглядом «альтернативних кіберспортивних турнірів» з грошовими призами. Проте в більшості випадків ці платформи використовували зламані клієнти, що містили шкідливий код. У 2022 році кіберполіція Польщі та Чехії спільно з Europol виявили групу, яка підтримувала піратський кластер серверів CS:GO, залучаючи понад 50 тисяч користувачів. На серверах розміщувався прихований майнер криптовалюти, який використовував обчислювальні ресурси гравців (Europol Cybercrime Report, 2022)[19].

Проблемою для європейського кіберспорту є також незаконне поширення кіберспортивного контенту. У 2021–2022 роках Європейська комісія зафіксувала сотні випадків нелегального потокового передавання змагань FIFA eWorld Cup та Dota 2 Major. Особливістю є те, що частина таких трансляцій розповсюджувалася не з комерційною метою, а як «фанатські стріми». Попри це, вони порушували права видавців і підривали прибутковість ліцензійних каналів.

Європейська спільнота реагує на проблему комплексно. Так, у 2023 році було ухвалено Директиву ЄС 2022/790, що регламентує швидке блокування неліцензійних потоків і нелегальних джерел eSports-контенту. Підхід Європи демонструє тенденцію до узгодження авторського права з цифровими форматами, забезпечуючи оперативне реагування на піратські активності без шкоди для користувацьких ініціатив.

В Україні проблема піратства в кіберспорті тісно пов'язана з історично високим рівнем використання неліцензійного програмного забезпечення. За даними Business Software Alliance (BSA, 2022), частка неліцензійного софту в Україні все ще перевищує 50%, що створює сприятливі умови для поширення піратських копій ігор. Водночас розвиток українського кіберспорту за останні роки супроводжувався низкою резонансних інцидентів.

Одним із найбільш показових є випадки використання піратських клієнтів Dota 2 і CS:GO для організації локальних турнірів у 2018–2021 роках. За повідомленнями DOU.ua та AIN.UA, кілька неофіційних клубів у Харкові, Києві та Дніпрі проводили змагання з використанням нелегальних копій Steam-ігор без належних ліцензій. Такі події не лише порушували авторські права Valve, а й створювали ризики безпеки для учасників, оскільки піратські клієнти часто містили змінений код для обходу SteamGuard і VAC.

Ще одним вектором піратства є викрадення облікових записів кіберспортсменів. У 2020 році Служба безпеки України повідомила про ліквідацію угруповання, що спеціалізувалося на продажу украдених акаунтів CS:GO і PUBG на закритих форумах. Використовувалися фішингові копії сторінок турнірних платформ FACEIT і ESL. Збитки від діяльності групи оцінювалися у понад 2 млн грн (СБУ, 2020)[20].

Також фіксувалися випадки піратського відтворення трансляцій українських кіберспортивних турнірів. У 2022–2023 роках офіційні трансляції чемпіонатів UESF та WePlay! дублювалися на сторонніх YouTube-каналах, які отримували прибуток від реклами. Організатори спільно з YouTube і Cyberpolice Ukraine вживали заходів щодо блокування таких ресурсів, однак проблема залишається системною.

Варто зазначити, що українська кіберспортивна екосистема активно рухається до формування цивілізованої моделі правового захисту. З 2021 року кіберспорт офіційно визнаний видом спорту в Україні, що відкриває можливість регулювання авторських прав, прав учасників і спонсорів за аналогією до інших спортивних дисциплін. Це створює передумови для ефективної протидії піратству на законодавчому рівні.

Порівняння регіонів показує, що США орієнтуються на кримінальне переслідування і створення судових прецедентів, Європа — на гармонізацію законодавства і превентивні технологічні заходи, тоді як Україна перебуває на етапі формування інституційної культури захисту інтелектуальної власності. Попри різні підходи, спільним є зростання кількості піратських інцидентів, пов'язаних з кіберспортом — від нелегального стрімінгу до продажу піратських копій у Steam та Epic Games Store через сірі акаунти.

За оцінками Newzoo (2023), втрати від піратства в eSports-секторі щорічно перевищують 1,3 млрд доларів, з яких близько третини припадає на нелегальні трансляції. Розвиток технологій захисту контенту (DRM, водяні знаки, розпізнавання потоків) дає змогу зменшити ці втрати, однак піратство еволюціонує разом із ринком, використовуючи нові платформи — TikTok Live, Twitch Mirror та Discord Streams — як канали незаконного поширення контенту.

Піратство у кіберспорті в Україні, США та Європі є багаторівневим феноменом, який охоплює як технічні, так і соціальні аспекти. Його наслідки виходять за межі економічних втрат, оскільки піратські дії підривають довіру до кіберспортивної індустрії, створюють ризики для гравців та спонсорів і впливають на конкурентне середовище. Найефективнішими методами протидії залишаються комплексні заходи: міжнародна співпраця у сфері кібербезпеки, технологічні рішення для моніторингу контенту, а також формування правової культури серед гравців, організаторів і глядачів.

Кіберспорт є однією з найбільш динамічних сфер цифрової економіки, і саме тому боротьба з піратством у цій галузі має розглядатися не лише як технічне завдання, а як елемент національної та міжнародної кіберполітики.

2.2 Вразливості ігрових рушіїв та середовищ виконання

Ігрові рушії становлять собою комплексні програмні платформи, що поєднують у собі механізми рендерингу, фізичного моделювання, системи ресурсів та скриптування; їхня роль у виробництві сучасних ігор означає, що будь-яка конструктивна слабкість на рівні рушія має потенціал масштабного впливу. Традиційно найбільш критичними виявляються помилки пов’язані з невірною обробкою зовнішніх вхідних даних (наприклад, парсинг пакетів ресурсів, обробка URI/аргументів командного рядка чи API для імпорту активів), що можуть призводити до локального виконання довільного коду (RCE), до читання/витоку конфіденційних даних або до порушення цілісності ресурсів збірки. Поява в рушії механізму, який дозволяє підвантажувати зовнішні бібліотеки або обробляти спеціальні URI-схеми без достатньої валідації, створює атаку по ланцюгу постачання: attacker може підмінити модуль, упровадити шкідливу логіку на етапі запуску або змусити застосунок завантажити бібліотеку з незахищеного шляху. Останні інциденти підтверджують, що такі теоретичні ризики мають реальні прояви: наприклад, вразливість класифікована як CVE-2025-59489 дозволяла через аргументну інжекцію Unity Runtime завантажувати бібліотеки з непередбачуваних місць, що потенційно дає можливість виконати довільний код у контексті користувача або процесу гри; виробник оперативно випустив засоби ремедіації і закликав перевидавців оновити збірки.

На практиці експлуатація подібних дефектів може відбуватися двома взаємопов’язаними способами: локальне зараження (через модифікований інсталятор, сторонні патчі чи зламані пакети залежностей) та віддалене впровадження через інструменти підвантаження ресурсів (трансфер модів, контент-паків). Декомпіляція й реверс-інжиніринг також дозволяють зловмисникам виявляти логіку ліцензування і цілісні перевірки, створюючи умови для обходу захисту без необхідності прямої експлуатації низькорівневих багів. Тому на рівні рушія критичною є комбінація технічних підходів: контроль цілісності двійкових артефактів, цифрове підписування ресурсів, обфускація критичних секцій коду і «білий» список дозволених шляхів завантаження; разом

з цим — оперативний моніторинг і застосування патчів постачальника рушія, оскільки сам факт наявності довгоіснуючих дефектів (наприклад у старих гілках рушія) значно ускладнює безпечне підтримування релізів.

2.3 Проблеми DRM-систем та обхід ліцензійних механізмів

Системи цифрового управління правами (DRM) проєктуються з метою ускладнити несанкціоноване копіювання і запуск продукту, однак їхня архітектура часто поєднує клієнтські перевірки з серверними компонентами, що створює кілька характерних слабких місць. По-перше, клієнтська логіка перевірки — навіть якщо вона виконана з великою кількістю захисних механізмів — завжди розгорнута в довіреному середовищі користувача; аналіз двійкових файлів і відстеження виконання за допомогою відладчиків або емуляторів дозволяє визначити, в яких точках відбувається верифікація, і підмінити або «фабрикувати» відповідь. По-друге, серверна сторона, яка надає активаційні токени або перевірки, може бути емуляована сторонніми інструментами: створення емулятора API-відповідей часто дозволяло зламувальникам запускати ігри без легітимної активації або з підробленим профілем активації. Реальні кейси демонструють, що навіть складні комерційні рішення, які декларують складні криптографічні схеми, піддаються обходу — прикладом є історія навколо випуску великих проєктів у 2021 році, коли обходи та «зламані» релізи Resident Evil Village показали, що певні перевірки могли бути вилучені або замінені так, що піратська збірка функціонувала стабільніше на деяких конфігураціях; це ілюструє не лише проблему обходу захисту, але й ризики, пов’язані з неочікуваним впливом протекторів на продуктивність і сумісність.

Відповідь на ці виклики вимагає системного підходу: поєднання апаратних опор (наприклад, прив’язка ключа до TPM), серверної валідації критичних операцій та мінімізації критичної логіки на клієнті. Також важливими є контролі цілісності збірок після збірки (за допомогою підписів артефактів і перевірок у CI/CD), аудит сторонніх компонентів і опціональна відмова від агресивних

механізмів DRM у тих випадках, коли вони негативно впливають на користувацький досвід — практика, що іноді спричиняє видалення певних рішень з випущених продуктів. У будь-якому разі, технічні заходи мають поєднуватися із правовими та операційними політиками, оскільки сам по собі технологічний захист без підтримки екосистеми реагування на інциденти залишається обмеженим.

2.4 Вразливості клієнт-серверної архітектури

Клієнт-серверна модель, що лежить в основі багатьох мультиплеєрних ігор, передбачає розподілене виконання і суттєву частину логіки, яка може опинитися або на стороні клієнта, або на сервері. Проблеми виникають коли критичні перевірки або бізнес-логіка залишаються в клієнтському коді або коли канали комунікації не забезпечують належного рівня шифрування і цілісності. Наприклад, незашифрований або неправильно захищений трафік відкриває можливості для перехоплення і модифікації пакетів (Man-in-the-Middle), що в контексті ігор може означати підробку стану матчу, повторну відправку (replay) корисних дій або ін’єкцію некоректних команд. Результатом таких атак стає порушення чесності змагань, крадіжка сесійних токенів і потенційний витік персональних даних. Клас дефектів, пов’язаних із недостатньою валідацією на сервері, проявляється у вигляді уразливостей API і вразливостей серверних компонентів рушіїв, що у минулому призводило до віддаленого виконання коду або DoS-сценаріїв у ігрових інфраструктурах; відповідні CVE, що стосуються компонентів рушіїв і серверних плагінів, ілюструють, наскільки важливо обробляти всі вхідні дані як недовірені та виконувати всю критичну логіку перевірок виключно на серверній стороні.

Запобігання цим проблемам включає обов’язкове застосування сучасних протоколів захисту транспорту (наприклад, TLS 1.3 або новіших специфікацій), впровадження тимчасових маркерів і одноразових токенів для захисту проти replay-атак, та сувору серверну валідацію всіх клієнтських запитів. Поряд із цим, архітектурні рішення мають прагнути до мінімізації довіри до клієнта: будь-яка

операція, яка може вплинути на результати гри або грошові трансакції, повинна супроводжуватися серверними контрольно-перевірочними процедурами і конфіденційною обробкою даних, а інструменти моніторингу поведінки й аналіз журналів повинні оперативно виявляти аномалії, що можуть свідчити про систематичні зловживання.

2.5 Вразливості античит-систем

Античит-рішення еволюціонували від простих користувацьких-рівневих інструментів до компонентів, що працюють на найнижчих рівнях системи, іноді з встановленням драйверів у режимі ядра (kernel-mode). Така ескалація має подвійний ефект: з одного боку, kernel-рівень дає потужні засоби виявлення і перешкоджання чітам; з іншого боку, самі драйвери античита стають «більшою мішенню», оскільки уразливості в них відкривають шлях до локального підвищення привілеїв або навіть віддаленого виконання, якщо їх можна експлуатувати через некоректну обробку запитів чи даних. Прикладом реальної проблеми є виявлена в 2024 році вразливість у комерційному kernel-драйвері («ACE-BASE.sys»), що отримала класифікацію CVE-2024-22830; цей інцидент показав, що використання сторонніх kernel-модулів в якості античита без належного аудиту робить екосистему вразливою до широкого спектра атак.

Окрім технічних вад, існує ще одна важлива проблема: використання механізмів низького рівня вимагає довіри користувача і може створювати конфлікт між безпекою і приватністю. Драйвери, що працюють на рівні ядра, мають доступ до системних ресурсів, і помилки в їхній логіці або валідації можуть бути використані не тільки для обходу античита, а й для створення бекдорів чи ескалації доступу. Це породжує необхідність трьох невід’ємних практик: регулярного технічного аудиту драйверів сторонніми фахівцями, мінімізації привілеїв і областей моніторингу до критично необхідних, а також прозорої політики оновлень і повідомлення користувачів про ризики. У сукупності, удосконалення античит-рішень має відбуватися у двох напрямах: технічне підвищення стійкості до обхідних технік (через евристичні і поведінкові

алгоритми, ML-аналіз) і одночасний захист самої інфраструктури античита від можливих векторів компрометації.

2.6 Аналіз вразливсотей популярних ігрових платформ

У екосистемі Wargaming найбільш відомі інциденти безпеки, зафіксовані в публічних базах даних, стосуються не стільки ядра гри World of Tanks Blitz як мережевого серверного коду, скільки супутніх мобільних і десктопних застосунків і інфраструктурних компонентів, що взаємодіють із сервісами компанії. Так, приклад проблеми, що ілюструє характер і масштаби ризиків у мобільних супровідних додатках, становить випадок, коли клієнт World of Tanks Assistant для Android не здійснював коректної валідації X.509-сертифікатів, що відкривало можливість проведення атаки «людина-посередині» з перехопленням чутливих даних користувача; цю уразливість було класифіковано як CVE і задокументовано в національній базі NVD, що підкреслює, що слабкі місця часто виникають через помилки в обробці TLS/SSL у додатковому ПЗ, а не тільки в ігровому сервері.

Важливо розуміти, що Wargaming як великий мультиплатформенний сервіс в минулому реагував також на широкі інтернет-вразливості, які не були специфічні для гри, але могли ускладнити безпеку екосистеми, — прикладом є реагування компанії на вразливість Heartbleed в OpenSSL у 2014 році, коли загроза компрометації зашифрованих каналів змусила розробників оперативно перевіряти і оновлювати свої криптографічні стек-компоненти. Така ситуація підкреслює принцип, що ризики для гравців і сервісів часто походять із третьосторонніх бібліотек і компонентів інфраструктури, а не лише з внутрішнього ігрового коду.

Щодо Steam як платформи і клієнта, на основі доступних публічних записів можна констатувати, що клієнт Steam неодноразово фігурував у CVE-звітності з різними класами уразливостей, серед яких були як локальні ескалації привілеїв через ненадійні права доступу під час інсталяції, так і вразливості у компонентах, що виконують веб-контент або завантажують і виконують

сторонні дані. Однією з помітних документованих проблем було виявлення умов, за яких інсталятор Steam дозволяв локальному користувачу підвищити свої привілеї до рівня системи через слабкі права на певні каталоги в момент критичного феномену — цю проблему офіційно занесли в реєстр CVE і описали у NVD як приклад того, як механіка встановлення програмного забезпечення може стати вектором для ескалації привілеїв.

Окрім цього, у відкритих джерелах та базах помічено вразливості, пов’язані з компонентами Steam, які обробляють веб-контент або пригрузку пейджів у внутрішніх браузерних процесах, що може призводити до віддаленого виконання коду у допоміжних процесах (наприклад, у steamwebhelper або steamwebhelper-подібних компонентах), і декілька досліджень та звітів на платформах винагород за помилки (bug bounty) демонструють, що неправомірно сформований веб-контент або шкідливі сторінки могли стати фактичним механізмом реалізації RCE у користувацьких середовищах Steam Deck і десктоп-клієнтах. Ці знахідки ілюструють системний ризик, що походить від використання вбудованих браузерних рушіїв і від необхідності виконання стороннього HTML/JS в межах клієнта платформи.

Найсвіжіші публічні маркери безпеки свідчать про те, що навіть у 2024–2025 роках реєстри CVE продовжують фіксувати нові вразливості для Steam-клієнта, зокрема випадки ескалації привілеїв, пов’язані з обробкою завантажуваних двійкових файлів або динамічних бібліотек, що підкреслює необхідність постійного оновлення клієнта та ретельного аудиту прав доступу в процесі інсталяції. Одне з таких записів, доданих у 2025 році, описує можливість ескалації через змодельований шкідливий виконуваний модуль або DLL, що підкреслює хронічну природу ризику, коли механізми оновлення і інсталяції створюють тимчасові вікна підвищеного ризику для локальної системи користувача.

Підсумовуючи, загальна картина публічно задокументованих CVE у контексті World of Tanks Blitz та Steam показує, що основні вектори ризику зосереджені навколо супровідного програмного забезпечення і клієнтських компонентів, зокрема валідації сертифікатів у мобільних додатках, обробки веб-

контенту в браузерних компонентах клієнта, а також механік інсталяції/оновлення, які можуть створювати вікна для локальної ескалації привілеїв. Через ця обставина ефективна практика пом’якшення загроз вимагає систематичного оновлення клієнтів і бібліотек, аналізу прав доступу під час інсталяції та незалежного аудиту вбудованих рушіїв, оскільки саме ці елементи найчастіше фігурують у записах CVE та супутніх технічних звітах. Для детального технічного аналізу окремих CVE у відкритих реєстрах можна звернутися до баз даних NVD і CVE Details, де збережені технічні описи, часові відмітки публікації та інформація про статус виправлень.

3 АНАЛІЗ ВРАЗЛИВОСТЕЙ ІГРОВИХ ПЛАТФОРМ

3.1 Аналіз вразливостей сучасних ігрових платформ

Нещодавно було опубліковано опис двох вразливостей клієнта цифрової платформи (ідентифікатори CVE-2019-14743 та CVE-2019-15316)[21], у якому також наведено хроніку спроб повідомлення постачальника про виявлені дефекти. У повідомленні описано, що початкові спроби коректного репортування вразливостей не дали очікуваних результатів, включно з тимчасовим блокуванням доповідача в каналізованих програмах винагороди за виявлення вразливостей. Тільки після публічного розкриття й втручання спільноти вдалося домогтися реакції від постачальника; подальші повідомлення було передано через офіційні платформи обробки вразливостей (наприклад, HackerOne), що у третьому циклі забезпечило конструктивну взаємодію з боку вендора.

Описана технічна проблема належить до класу вразливостей, що допускають створення або модифікацію файлів із частково керованим вмістом у контексті сервісного процесу платформи. Уразливість виявлена у конкретній версії сервісного компоненту, який відповідає за фонові операції клієнтської частини платформи. Технічною суттю проблеми є поєднання двох факторів: можливості впливу на шлях пошуку або місця зберігання компонентів сервісу з боку неповноважених з погляду доменних привілеїв користувачів, а також відсутності належних перевірок цілісності або валідації вмісту, який підвантажується в контексті сервісного процесу. Така комбінація дозволяє зловмисникові змоделювати умови, за яких сервіс може оперувати з неочікуваними або частково контрольованими файлами.

Наслідки експлуатації носять широку природу ризику: можливе виконання небажаного коду в контексті сервісу, ескалація привілеїв залежно від облікового запису, під яким запущено службу, а також встановлення персистентних механізмів доступу або витік конфіденційних артефактів. Оскільки сервіс є компонентом клієнтської інсталяції, компрометація може мати як локальні наслідки для робочої станції, так і потенційні наслідки для довіреної

мережевої інфраструктури, у випадку наявності довірених зв’язків або синхронізованих облікових даних.

У частині процедурного забезпечення було відзначено, що права доступу (ACL) і політики запуску сервісу мають критичне значення: некоректно надані дозволи або надто широкі права запису у «сховищах конфігурації» створюють додаткові вектори впливу. Також ідентифіковано, що відсутність валідації шляхів і перевірок підписів/контрольних сум модулів погіршує стійкість до атак, які використовують підстановку файлів або «поверхневі» маніпуляції зі шляхами пошуку компонентів. На рисунку 3.1 приведено найбільш популярні вразливості ігрової платформи Steam.

Рисунок 3.1- Вразливості ігрової платформи steam

Із практичної точки зору інцидент також підкреслює важливість відпрацьованих каналів відповідального розкриття вразливостей, прозорих процедур для валідації репортів та своєчасної комунікації вендора зі спільнотою тестувальників. Наявність механізмів багатостороннього розгляду — включно з використанням платформ для винагороди за виявлення вразливостей — сприяє оперативнішому усуненню дефектів та зниженню ризику їх експлуатації після публікації.

Рекомендовано наступні загальні заходи пом’якшення: обмеження прав доступу до конфігураційних сховищ і каталогів, що використовуються сервісом; забезпечення запуску служб із найменшим необхідним набором привілеїв; використання абсолютних, контрольованих шляхів під час підвантаження компонентів; впровадження перевірок цілісності й підписування бінарних модулів; ретельна валідація вхідних шляхових рядків і нормалізація шляхів перед їх використанням; а також моніторинг і аудит змін у каталозі виконуваних модулів. Окремо слід підсилити процес обробки повідомлень про вразливості внутрішніми процедурами відповідального огляду та забезпеченням зворотного зв’язку заявникам. Проведемо моделювання атаки як показано на схемі, що на рисунку 3.2.

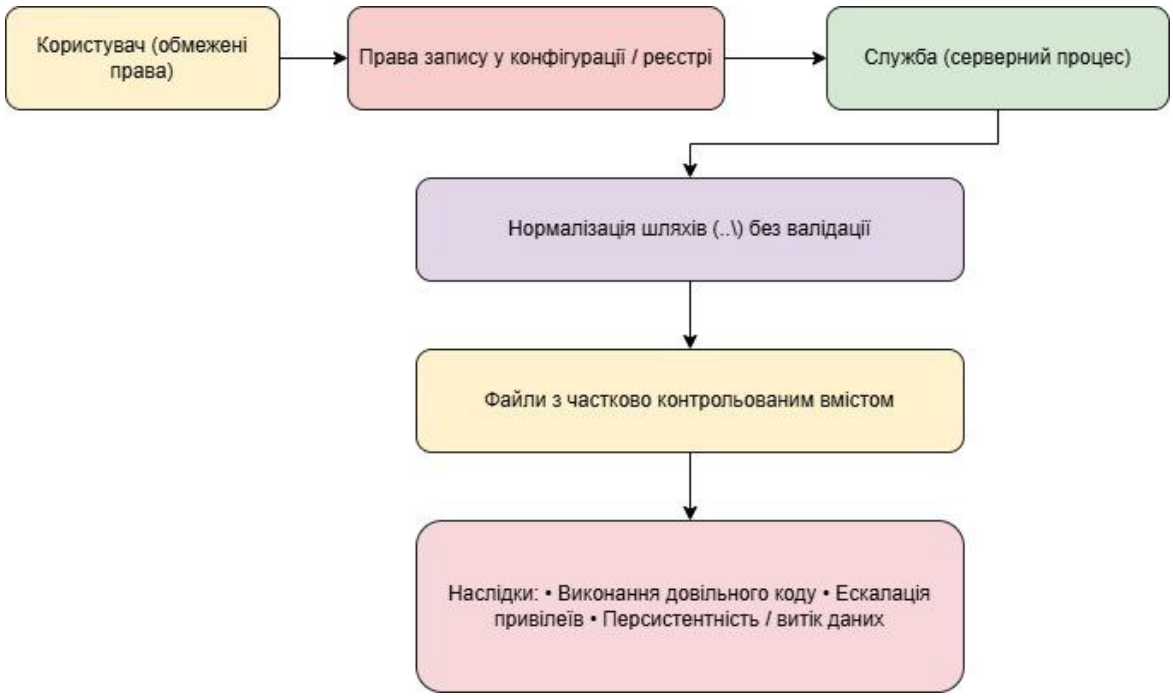


Рисунок 3.2 – Схема експлуатації вразливості, що веде до ескалації привілеїв

Для експлуатації вразливостей, необхідно завершити програму Steam та зупинити сервіс «Steam Client Service», якщо вони запущені. Найчастіше користувачі без прав адміністратора не можуть запускати та зупиняти будь-які сервіси. Але для цього сервісу Valve встановили права, що дозволяють всім користувачам зупиняти і запускати його.

Необхідно створити папку в будь-якому доступному для користувача місці (наприклад, «C:\test»). У цю папку необхідно скопіювати файли Steam.exe і steamclient.dll з вихідної папки Стіма (за замовчуванням це C:\Program Files (x86)\Steam). Створюємо порожню підпапку logs («C:\test logs»).

Тепер виправимо реєстр: у гілці "HKLM\Software\wow6432node\valve\steam" змінимо значення параметра "InstallPath" на "C:\test\1\..". Зазвичай користувачам без прав адміністратора гілки реєстру всередині HKLM недоступні для запису, але не в даному випадку(рисунок 3.3). При установці Valve встановили такі права на свою гілку всередині HKLM, що в ній всім користувачам доступні будь-які дії (Full control для групи Users).

Запустимо сервіс "Steam Client Service". Після того, як він зупиниться (це відбудеться автоматично через кілька секунд), перевіримо вміст папки "C:\test\logs" - виявимо там файл "service_log.txt". Вміст лога буде приблизно таким:

11/11/2025 14:25:01 : ERROR: SteamService: Invalid file signature C:\test\1\..\bin\SteamService.dll

Звернемо увагу, що шлях "C:\test\1\.." еквівалентний шляху "C:\test", тому для роботи Windows використовував другий, а в повідомлення потрапив перший. Видалимо файл "service_log.txt" і продовжимо.

Цікавий факт: коли Windows працює з шляхами, що містять "\..", вона автоматично спрощує такі шляхи. Не проводячи жодних перевірок для проміжних папок.

Наприклад, шлях "C:\1\<test>\.." буде перетворено на "C:\1", незважаючи на те, що в імені папки не можна використовувати символи кутових дужок.

На першому кроці ми прописали шлях у реєстрі, тепер додамо до нього перенесення рядків. Це можна зробити, написавши простий код, але реально зробити з інтерфейсу regedit. Достатньо відкрити гілку реєстру "HKLM\Software\wow6432node\valve\steam" і вибрати "Modify binary data.." в контекстному меню параметра "InstallPath". З'явиться щось на кшталт хекс-редактора, де можна зробити необхідні правки.

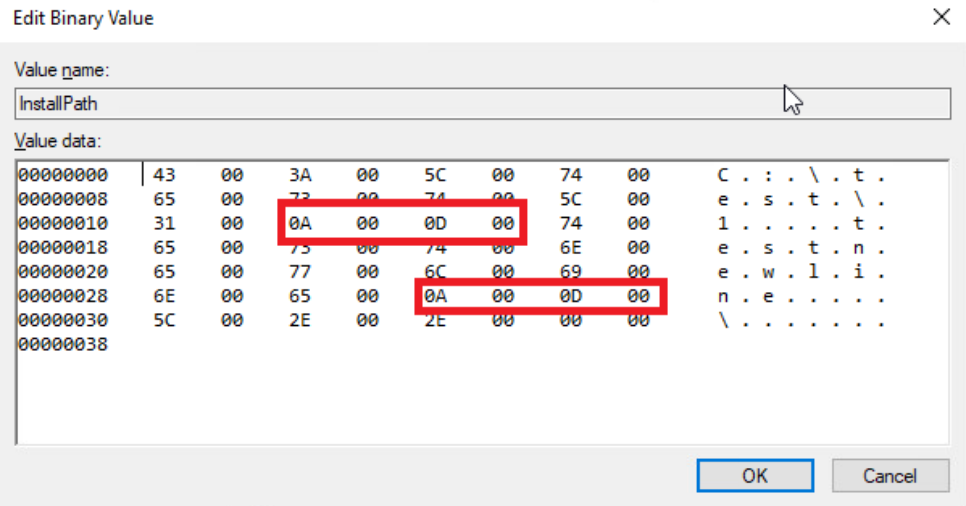


Рисунок 3.3 – Зміна бінарного ключа реєстру

Проведемо ще один тестовий запуск сервісу та перевіримо результат проведених дій приведено на рисунку 3.4.

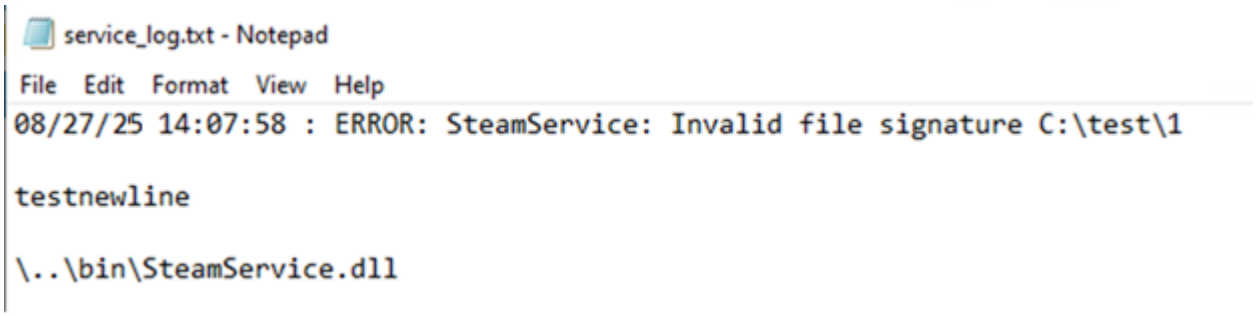


Рисунок 3.4 – Результат запуску тестового файлу

Після тесту необхідно видалити файл «service_log.txt». Користувачі без прав адміністратора не можуть створювати символічні посилання з одного файлу до іншого. Але є прихована можливість – можна об'єднати інші види посилань, які доступні користувачам без прав адміністратора, щоб отримати ефект, близький до симлінку з файлу на файл.

Спочатку створимо NTFS reparse point (інша назва NTFS mount point) з папки "C:\test\logs" на "RPC Control\". "RPC Control" - це не звичайна папка в

звичному розумінні, її не можна подивитися, наприклад, в експлорері. Це системна об'єктна директорія, усередині якої знаходяться, наприклад, іменовані м'ютекси, події та інші подібні об'єкти. Чому для неї працює перенаправлення через NTFS reparse point незрозуміло, швидше за все, справа у використанні однакових абстракцій для папок у файловій системі та об'єктних директорій. З об'єктної директорії можна створити симлінк на файл без прав адміністратора. Створимо символ типу "\RPC Control\service_log.txt" <-> «C:\Шлях\к\файлу».

В результаті будь-які звернення до "C:\test\logs\service_log.txt" будуть перенаправлені на файл "C:\Шлях\до\файлу". Щоб створити таке перенаправлення є дві основні вимоги - папка, з якої створюється NTFS reparse point, повинна бути порожньою, і вона повинна бути доступна для запису користувачеві. Саме для виконання першої умови ми після кожного тесту видаляли файл «service_logs.txt», друга умова забезпечується тим, що вихідну папку ми створили в контрольованому користувачем місці.

Існує спеціальна утиліта, яка створює такі пари симлінків - CreateSymlink і доступна для завантаження на GitHub. Використання утиліти:

CreateSymlink.exe <звідки> <куди>

У нашому випадку це буде:

CreateSymlink.exe "C:\test\logs\service_log.txt" "C:\Шлях\до\файлу"

Збираючи всі разом, отримуємо, що при старті сервісу «Steam Client Service» буде створено файл на шляху, який був вказаний при створенні симлінку, і в цьому файлі буде вміст, який ми можемо проконтролювати (за винятком першого та останнього рядка). Якщо вкажемо шлях до існуючого файлу, вміст буде дописано до кінця файлу. Все це буде виконано від імені сервісу Steam Client Service із правами NT AUTHORITY\SYSTEM.

3.1.2 Аналіз вразливостей CVE-2020-6016, CVE-2020-6017, CVE-2020-6018 та CVE-2020-6019

У ході дослідження, проведеного фахівцями компанії Check Point Research, було виявлено чотири критичні вразливості — CVE-2020-6016, CVE-2020-6017, CVE-2020-6018 та CVE-2020-6019 — у мережевій бібліотеці Steam Sockets, яка

використовується як базовий транспортний рівень для обміну даними у багатьох ігрових проєктах, створених на базі технологій Valve. Зазначена бібліотека входить до складу офіційного плагіна, який Valve надає стороннім розробникам для інтеграції мережевих функцій у власні ігри.

Виявлені вразливості могли дозволити зловмисникам здійснити повне захоплення ігрового сервера, викликати збої у роботі застосунків або навіть отримати віддалений контроль над комп'ютером користувача. Основна причина полягала у помилках обробки мережевих пакетів у процесі повторної збірки даних (CVE-2020-6016) та у некоректній реалізації ітераторів у C++, що уможливлювало надсилання спеціально сформованих пакетів із подальшим переповненням буфера стека.

Компанія Check Point Research повідомила розробників Valve про вразливості у вересні 2020 року. Протягом трьох тижнів після отримання звіту Valve провела оновлення власних ігор і розповсюдила виправлення серед партнерських студій, які використовують Steam Sockets у своїх проєктах.

Для користувачів, що грають у продукти Valve через платформу Steam, ризики експлуатації цих вразливостей відсутні, оскільки виправлення вже інтегровані у поточні версії клієнта. Проте розробникам сторонніх ігор рекомендовано перевірити, чи було здійснено останнє оновлення їхніх продуктів. Переконатися в цьому можна за допомогою розділу «Завантаження» у клієнті Steam, який відображає список нещодавніх оновлень, або через вкладку «Переглянути новини» в центрі новин платформи, де публікуються записи про зміни та патчі. У разі відсутності актуальних оновлень Check Point рекомендує зв'язатися безпосередньо з розробником гри для уточнення інформації про стан її безпеки.

3.2 Експлуатація методу BaitAndSwitch

Узагальнено процес реалізації експлуатації описаної вразливості можна представити як послідовність з трьох логічних етапів. Перший етап полягає у підготовці робочого середовища, причому для досягнення цілей атаки існують

альтернативні підходи, що використовують різні конфігураційні або налаштувальні недоліки системи. На другому етапі здійснюється примусова ініціація механізмів платформи для підвантаження сторонніх компонентів у контексті довіреного процесу. Третій етап передбачає, що завантажуваний модуль відповідає певним умовам сумісності, необхідним для його коректного виконання в середовищі цільової служби.

Важливо підкреслити, що технічно реалізація кожного з цих етапів може бути здійснена локальним користувачем або програмою, запущеною від імені такого користувача. У разі успішної експлуатації можливими наслідками є виконання довільного коду з підвищеними привілеями — класична подія escalation of privileges (EoP) або local privilege escalation (LPE). Набуття максимальної привілейованості процесу значно збільшує потенційні наслідки компрометації: від вимкнення засобів захисту й інсталяції привідних модулів до встановлення персистентних компонентів, прихованого майнінгу або масового викрадення конфіденційних даних.

У публічних обговореннях часто зустрічаються спрощені твердження типу «у гілку реєстру HKLM користувач не може записувати» або «створення символічних посилань вимагає адміністраторських прав». Такі узагальнення не витримують перевірки, оскільки політики доступу визначаються для конкретних ключів або об’єктів, а не накладають універсальні заборони. У практичному середовищі безпека залежить від того, які саме ACL (Access Control List) застосовано до конкретних гілок реєстру, файлів або служб; надмірно ліберальні дозволи в окремих гілках можуть зробити можливим непрогнозовані вектори впливу.

Не існує одного універсального правила щодо запису в гілки системного реєстру або управління службами: для кожного ключа реєстру та кожного сервісу система застосовує власні правила доступу. Унаслідок цього певні записи конфігурації або параметри запуску служб можуть стати доступними для модифікації користувачем із обмеженими привілеями, якщо відповідні ACL були налаштовані невірно. Аналогічно, можливість ініціювати керування службами (запуск/зупинка) залежить від конкретних дозволів, які встановлені для даного

сервісу. Valve виставила права повного доступу для всіх користувачів на гілку HKLM \ SOFTWARE \ Wow6432 Node \ Valve \ steam, і тому в цій гілці будь-який користувач може робити, що хоче.

Символічні посилання, NTFS-точки монтування та привілеї Поняття «символічний лінк» у Windows охоплює кілька різновидів механізмів зв'язування об'єктів файлової системи й реєстру (символічні посилання на файли, жорсткі посилання, NTFS-reparse-points/точки монтування тощо). Не всі ці механізми однаково вимагають підвищених привілеїв для створення: частина типів посилань може бути створена в межах поточної сесії або за наявності відповідних прав до каталогу без потреби у глобальних адміністративних привілеях. NTFS-reparse-point (інколи позначається як mount point) дозволяє використовувати один каталог як вказівник на інший і за певних умов може бути створений користувачем, що має права на запис у вихідному каталозі. Така функціональність може використовуватися як легітимний інструмент адміністрування, але в умовах некоректної конфігурації — й як вектор для перенаправлення операцій з файловою системою.

Opportunistic locks (OpLock) як елемент файлової координації Opportunistic lock (OpLock) — це механізм взаємодії між процесами та файловою системою, що дозволяє захопити тимчасовий контроль над доступом до ресурсу з метою оптимізації продуктивності або синхронізації. Існують різні режими й умови застосування такої блокування, проте сутність полягає в можливості відкласти обробку звернення до певного файлу до закінчення внутрішньої операції або до активного сигналу від процесу, який встановив OpLock. Механізми OpLock широко застосовуються в системах клієнт-серверного доступу до файлів і можуть мати специфічні наслідки для поведінки прикладного програмного забезпечення при одночасному або послідовному доступі до ресурсів.

BaitAndSwitch -це назва прийому, який комбінує створення лінків та встановлення оплотів, щоб виграти TOCTOU (time of check\time of use). Суть простіше пояснити з прикладу.

Уявіть, що є деяка програма, яка поспіль робить щось на кшталт такого:

ReadContentFromFile("C:\test\myfile.txt");

ReadContentFromFile("C:\test\myfile.txt");

Це просто читання одного і того ж файлу двічі поспіль. Чи завжди буде прочитане одне й те саме. Ні, не обов'язково.

Спочатку створимо дві папки з файлами C: test1 myfile.txt і C: test2 myfile.txt. А папку C: Test взагалі очистимо і створимо reparse point на C: Test1. Поставимо оплок на файл із першої директорії та запускаємо програму. Як тільки вона відкриє файл, спрацює оплок. Ми поміняємо reparse point і C: Test буде вказувати на C: Test2. Тепер після того, як оплок буде знято, програма прочитає файл вдруге вже з іншого файлу.

Потрібно трохи підготувати робоче оточення. Почнемо з того, що необхідно взяти файли CreateMountPoint.exe і SetOpLock.exe.

Тепер потрібно провести невеликі зміни у файловій структурі Стім. Наше завдання – отримати папку з двома файлами Steam.exe та steamclient.dll та обов'язковою відсутністю папки bin. Це можна зробити двома способами.

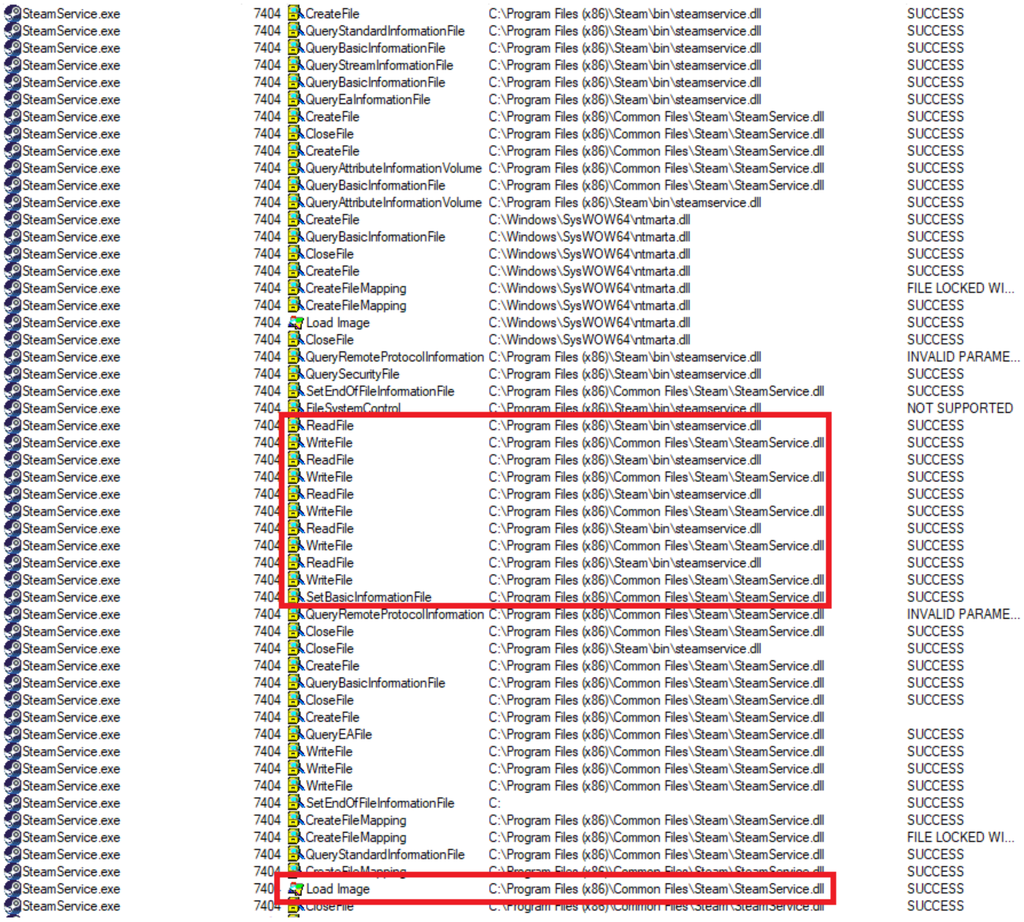
Перейменувати\видалити папку bin із основної папки Steam. Все, ви чудові (Стим при установці дає будь-якому користувачеві права на все в його папці).

У ключі реєстру HKLM\SOFTWARE\Wow6432Node\Valve\steam змінити параметр InstallPath на якусь нашу папку. У цю папку закинути Steam.exe та steamclient.dll з основної папки Стім.

Нехай будь-яким із способів ми підготували папку C:\Steam (шлях може бути будь-який, але в прикладах я використовуватиму цей). Тепер створимо в ній ще папки b1, b2, b3 та b4. У перші три закинемо файл steamservice.dll (з комплекту Стіма, в оригіналі він лежав у папці bin), а в папку b4 закинемо спеціально сформовану бібліотеку з тим самим ім'ям - steamservice.dll. Докладно про підготовку бібліотеки буде у 3 пункті.

Відкриваємо два віконця консолі. На цьому підготовку оточення завершено.

Скріншот із ProcMon приведено на рисунку 3.3.



SteamService.exe	7404	CreateFile	C:\Program Files (x86)\Steam\bin\steamservice.dll	SUCCESS
SteamService.exe	7404	QueryStandardInformationFile	C:\Program Files (x86)\Steam\bin\steamservice.dll	SUCCESS
SteamService.exe	7404	QueryBasicInformationFile	C:\Program Files (x86)\Steam\bin\steamservice.dll	SUCCESS
SteamService.exe	7404	QueryStreamInformationFile	C:\Program Files (x86)\Steam\bin\steamservice.dll	SUCCESS
SteamService.exe	7404	QueryBasicInformationFile	C:\Program Files (x86)\Steam\bin\steamservice.dll	SUCCESS
SteamService.exe	7404	QueryEaInformationFile	C:\Program Files (x86)\Steam\bin\steamservice.dll	SUCCESS
SteamService.exe	7404	CreateFile	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	CloseFile	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	CreateFile	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	QueryAttributeInformationVolume	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	QueryBasicInformationFile	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	QueryAttributeInformationVolume	C:\Program Files (x86)\Steam\bin\steamservice.dll	SUCCESS
SteamService.exe	7404	CreateFile	C:\Windows\SysWOW64\ntmarta.dll	SUCCESS
SteamService.exe	7404	QueryBasicInformationFile	C:\Windows\SysWOW64\ntmarta.dll	SUCCESS
SteamService.exe	7404	CloseFile	C:\Windows\SysWOW64\ntmarta.dll	SUCCESS
SteamService.exe	7404	CreateFile	C:\Windows\SysWOW64\ntmarta.dll	SUCCESS
SteamService.exe	7404	CreateFileMapping	C:\Windows\SysWOW64\ntmarta.dll	FILE LOCKED WI...
SteamService.exe	7404	CreateFileMapping	C:\Windows\SysWOW64\ntmarta.dll	SUCCESS
SteamService.exe	7404	Load Image	C:\Windows\SysWOW64\ntmarta.dll	SUCCESS
SteamService.exe	7404	CloseFile	C:\Windows\SysWOW64\ntmarta.dll	SUCCESS
SteamService.exe	7404	QueryRemoteProtocolInformation	C:\Program Files (x86)\Steam\bin\steamservice.dll	INVALID PARAME...
SteamService.exe	7404	QuerySecurityFile	C:\Program Files (x86)\Steam\bin\steamservice.dll	SUCCESS
SteamService.exe	7404	SetEndOfFileInformationFile	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	FileSystemControl	C:\Program Files (x86)\Steam\bin\steamservice.dll	NOT SUPPORTED
SteamService.exe	7404	ReadFile	C:\Program Files (x86)\Steam\bin\steamservice.dll	SUCCESS
SteamService.exe	7404	WriteFile	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	ReadFile	C:\Program Files (x86)\Steam\bin\steamservice.dll	SUCCESS
SteamService.exe	7404	WriteFile	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	ReadFile	C:\Program Files (x86)\Steam\bin\steamservice.dll	SUCCESS
SteamService.exe	7404	WriteFile	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	ReadFile	C:\Program Files (x86)\Steam\bin\steamservice.dll	SUCCESS
SteamService.exe	7404	WriteFile	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	ReadFile	C:\Program Files (x86)\Steam\bin\steamservice.dll	SUCCESS
SteamService.exe	7404	WriteFile	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	SetBasicInformationFile	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	QueryRemoteProtocolInformation	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	INVALID PARAME...
SteamService.exe	7404	CloseFile	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	CloseFile	C:\Program Files (x86)\Steam\bin\steamservice.dll	SUCCESS
SteamService.exe	7404	CreateFile	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	QueryBasicInformationFile	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	CloseFile	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	CreateFile	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	
SteamService.exe	7404	QueryEAFile	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	WriteFile	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	WriteFile	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	WriteFile	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	SetEndOfFileInformationFile	C:	SUCCESS
SteamService.exe	7404	CreateFileMapping	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	CreateFileMapping	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	FILE LOCKED WI...
SteamService.exe	7404	QueryStandardInformationFile	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	CreateFileMapping	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	Load Image	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS
SteamService.exe	7404	CloseFile	C:\Program Files (x86)\Common Files\Steam\SteamService.dll	SUCCESS

Рисунок 3.3 – Моніторинг діяльності Steam

Це частина лога типового старту сервісу Steam Client Service. Зверніть увагу на частину, де dll спочатку копіюється в C: Program Files (x86) Common Files Steam, а потім завантажується. Зробимо так, щоб скопіювалася наша бібліотека з C:\Steam\b4. На жаль, спочатку йдуть перевірки, у тому числі перевіряється підпис бібліотеки, щоб його не можна було підмінити (о, іронія).

Для кожного кроку буде вказано де що запускати і що відбувається (різні вікна консолі названо cmd1 і cmd2.

1. Створюємо папку C:\Steam\bin і в cmd1 виконуємо:

CreateMountPoint.exe 3:\Steam\bin C:\Steam\b1

2. У cmd1 ставимо оплок:

SetOpLock.exe C:\Steam\b1\steamservice.dll

3. Запускаємо сервіс Steam Client Service, бачимо в cmd1, що зловили звернення до файлу.

4. Видаляємо C:\Steam\bin, створюємо на його місці папку C:\Steam\bin і в cmd2 виконуємо:

CreateMountPoint.exe З:\Steam\bin C:\Steam\b2

5. У cmd2 ставимо оплок:

SetOpLock.exe C:\Steam\b2\steamservice.dll

6. У cmd1 відпускаємо оплок, бачимо, що cmd2 зловили звернення до файлу.

7. Видаляємо C:\Steam\bin, створюємо на його місці папку C:\Steam\bin і cmd1 виконуємо:

CreateMountPoint.exe З:\Steam\bin C:\Steam\b3

8. У cmd1 ставимо оплок:

SetOpLock.exe C:\Steam\b3\steamservice.dll

9. У cmd2 відпускаємо оплок, бачимо, що cmd1 зловили звернення до файлу.

10. Видаляємо C:\Steam\bin, створюємо на його місці папку C:\Steam\bin і cmd2 виконуємо: CreateMountPoint.exe З:\Steam\bin C:\Steam\b2

11. У cmd2 ставимо оплок:

SetOpLock.exe C:\Steam\b2\steamservice.dll

12. У cmd1 відпускаємо оплок, бачимо, що cmd2 зловили звернення до файлу.

13. Видаляємо C:\Steam\bin, створюємо на його місці папку C:\Steam\bin і cmd1 виконуємо:

CreateMountPoint.exe З:\Steam\bin C:\Steam\b3

14. У cmd1 ставимо оплок: SetOpLock.exe C:\Steam\b3\steamservice.dll

15. У cmd2 відпускаємо оплок, бачимо, що cmd1 зловили звернення до файлу.

16. Видаляємо C:\Steam\bin, створюємо на його місці папку C:\Steam\bin і cmd2 виконуємо: CreateMountPoint.exe З:\Steam\bin C:\Steam\b4

17. У cmd1 відпускаємо оплок

Схема експлуатації вразивості приведена на рисунку 3.4.

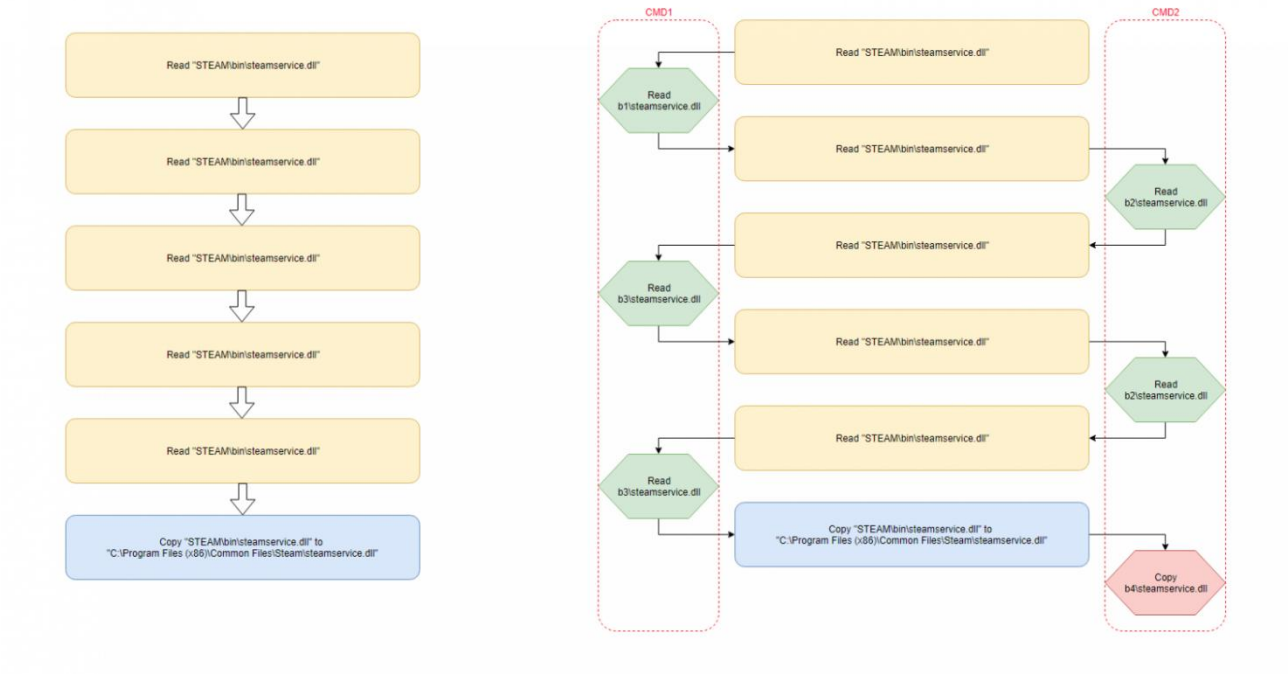


Рисунок 3.4 – Поведінка Steam сервісу з нормальним запуском та при експлуатації вразливості

Для емуляції корисного навантаження спочатку скористаємося найбільш типовою dll, яка в DllEntry створює інтерактивну консоль. Оскільки код із dll буде виконано в контексті Steam Client Service, він буде виконаний з тими ж правами, що й сам сервіс – NT AUTHORITY\SYSTEM. Але внаслідок експлуатації консоль не з'явилася.

Після завантаження сервіс Steam все ж таки розуміє, що йому підсунули липу, і завершує роботу, тому корисне навантаження dll не встигло виконатися.

Після завантаження dll сервіс перевіряє існування функцій:

int WINAPI SteamService_RunMainLoop()

void WINAPI SteamService_Stop()

Більше того, сервіс викликає першу функцію, де розміщено корисне навантаження (запуск інтерактивної консолі з правами сервісу – NT AUTHORITY\SYSTEM). Ось тепер зовсім все – повторюємо всі дії та отримуємо консоль із максимальними правами.

3.3 Методика запобігання піратства в кіберспорті

Запобігання піратству в кіберспорті є комплексним процесом, що поєднує технічні, правові, організаційні та соціальні заходи, спрямовані на забезпечення цілісності ігрового середовища та захист інтелектуальної власності розробників. У сучасних умовах кіберспорт функціонує як частина глобальної цифрової економіки, у якій ключову роль відіграють онлайнові сервіси, платформи дистрибуції та серверна інфраструктура. Тому головна мета антипіратських заходів полягає не лише у недопущенні несанкціонованого копіювання програмного забезпечення, а й у збереженні стабільності і справедливості ігрового процесу, від якої безпосередньо залежить довіра учасників і комерційна привабливість змагань.

Основним технічним засобом протидії піратству в кіберспортивному середовищі є використання серверно-клієнтської архітектури, у якій усі ключові обчислення, автентифікація користувачів та зберігання даних здійснюються на стороні розробника. Це виключає можливість функціонування неліцензійних копій без постійного зв’язку з офіційними серверами. Захист доповнюється технологіями DRM і цифровими підписами, що забезпечують перевірку автентичності під час запуску гри або отримання оновлень. Додаткову роль відіграє впровадження систем античиту, здатних виявляти несанкціоновані модифікації клієнта, сторонні інжекції коду чи спроби обману ігрової логіки, що одночасно виступає і запобіжником проти порушень чесної конкуренції.

Правовий аспект політики боротьби з піратством охоплює регулювання авторських прав, ліцензування ігрового контенту та співпрацю з платформами розповсюдження. Використання міжнародних інструментів, таких як DMCA у США чи Директива 2001/29/ЕС у Європейському Союзі, дозволяє швидко реагувати на випадки незаконного поширення контенту через механізм офіційних повідомлень про видалення матеріалів. У межах кіберспортивної індустрії це означає можливість блокування піратських серверів, підроблених турнірних платформ і нелегальних трансляцій змагань.

Важливим елементом протидії піратству є також вдосконалення економічних моделей. Поширення форматів free-to-play і систем мікротранзакцій зробило ігри доступнішими для користувачів, що суттєво знизило стимули до використання неліцензійних версій. Додатковий захисний ефект забезпечують регулярні оновлення, сезонні івенти та серверна синхронізація, завдяки яким піратські копії швидко втрачають актуальність і не можуть повноцінно взаємодіяти з офіційним контентом.

Рисунок 3.5 - Методика запобігання піратства у кіберспорті

Особливе значення має комунікаційна та освітня складова антипіратської політики. Формування свідомого ставлення гравців до питань авторського права, проведення роз’яснювальних кампаній і створення позитивного іміджу легального користування сприяють формуванню сталого середовища кіберспортивної етики. Такий підхід дозволяє зміцнити взаємну довіру між розробниками, кіберспортивними організаціями та спільнотою гравців, що є фундаментальною умовою сталого розвитку галузі.

У підсумку заходи запобігання піратству в кіберспорті базуються на принципі взаємодії трьох складових — технологічної безпеки, правового захисту та соціальної відповідальності. Саме поєднання цих аспектів створює цілісну систему протидії, здатну ефективно реагувати на виклики цифрової епохи та

забезпечувати стабільність, легітимність і економічну життєздатність кіберспортивного сектору.

Окремо потрібно виділити заходи безпеки для ігрових платформ, котрі потрібно впроваджувати, ще на початку їх розробки, як архітектурне рішення. На рисунку 3.6 приведено схему заходів для підвищення кібербезпеки ігрових платформ.

Рисунок 3.6 - Схема заходів для підвищення кібербезпеки ігрових платформ

Безпека ігрових платформ, зокрема таких як Steam, є одним із ключових аспектів кіберзахисту сучасної ігрової індустрії. Ці платформи виконують функції не лише дистрибуції цифрового контенту, а й управління ліцензіями, обліковими записами користувачів, фінансовими транзакціями, внутрішньоігровими активами та соціальними взаємодіями. Саме тому вони становлять цінну ціль для кіберзлочинців, що зумовлює необхідність створення багаторівневої системи безпеки, яка охоплює як технічні, так і організаційні заходи.

Архітектура Steam базується на поєднанні серверної інфраструктури Valve, клієнтського програмного забезпечення та механізмів автентифікації користувачів. Ключовим елементом захисту є багатофакторна аутентифікація (Steam Guard), яка забезпечує додатковий рівень безпеки через підтвердження входу на нових пристроях за допомогою електронної пошти або мобільного

застосунку. Це рішення мінімізує ризики несанкціонованого доступу, навіть у випадку компрометації пароля. Водночас платформа використовує криптографічні алгоритми для захисту даних, що передаються між клієнтом і сервером, а також для шифрування збережених сесій користувача.

Особливу увагу приділено захисту внутрішньоігрових активів, які часто мають реальну грошову вартість у межах торговельних майданчиків Steam. Для зниження ймовірності шахрайства та крадіжок цифрових предметів запроваджено механізми торговельних обмежень, що тимчасово блокують передавання активів після зміни пароля або входу з нового пристрою. Такі заходи дозволяють виявляти підозрілі дії та запобігати миттєвому виведенню вкрадених предметів на сторонні платформи.

Крім того, безпека платформи підтримується через активну політику оновлення програмного забезпечення та системи виявлення вразливостей. Valve використовує модель відповідального розкриття (Responsible Disclosure Policy), яка передбачає офіційну взаємодію з дослідниками кібербезпеки через платформу HackerOne. Це дозволяє оперативно реагувати на виявлені дефекти, зокрема ті, що стосуються локальної ескалації привілеїв (CVE-2019-14743, CVE-2019-15315) чи можливостей віддаленого виконання коду. Регулярні оновлення Steam Client Service спрямовані на усунення помилок у правах доступу, механізмах реєстру Windows та системних службах.

Суттєву роль у забезпеченні стійкості платформи відіграє модель сегментації доступу та принцип найменших привілеїв. Користувацький клієнт має обмежений набір дозволів у системі, тоді як критичні операції — наприклад, встановлення оновлень або керування службами — виконуються окремими процесами з ізольованим контекстом безпеки. Така архітектура зменшує потенційну площину атаки, унеможливлює ескалацію привілеїв із клієнтського рівня та знижує ризик компрометації системи.

Важливим аспектом є також захист соціальної взаємодії користувачів, оскільки чати, спільноти та внутрішньоігрові повідомлення часто стають інструментом фішингових атак. Valve впроваджує фільтри для виявлення підозрілих посилань, системи репутації користувачів та автоматизовані

алгоритми блокування зловмисних акаунтів. Одночасно з цим ведеться моніторинг активності з метою виявлення бот-мереж, несанкціонованого фармінгу предметів і шахрайських транзакцій.

Таким чином, система безпеки Steam функціонує як багаторівнева модель, у якій поєднано криптографічні, поведінкові та адміністративні заходи. Її ефективність ґрунтується на безперервному моніторингу, автоматизованому аналізі аномалій, тісній співпраці з кіберспільнотою та гнучкому реагуванні на нові загрози. У результаті формується захищена екосистема, здатна не лише мінімізувати ризики піратства та зловживань, але й забезпечити стабільність функціонування всієї ігрової інфраструктури.

ВИСНОВКИ

Проаналізовано особливості піратства у сфері відеоігор, визначено основні чинники його поширення, форми реалізації та економічні наслідки для розвитку індустрії, що дало змогу окреслити ключові загрози ліцензійному програмному забезпеченню та встановити залежність між рівнем піратства і темпами інновацій у геймдев-секторі.

Вивчено правове регулювання боротьби з піратством у кіберспортивному секторі США, зокрема дію DMCA та механізми примусового видалення нелегального контенту, що дозволило оцінити ефективність нормативної бази у захисті інтересів індустрії.

Узагальнено проблеми функціонування DRM-систем, виявлено механізми їх обходу та визначено технологічні й архітектурні причини їхньої вразливості, що дозволило оцінити межі ефективності традиційних методів цифрового захисту.

Досліджено структуру клієнт-серверних рішень у відеоіграх, визначено типові моделі атак на мережеву взаємодію та слабкі місця серверної логіки, що дало змогу сформувати перелік критичних ризиків для кіберспортивних платформ.

Проаналізовано принципи роботи античит-систем та характерні технічні недоліки їх реалізації, що дозволило визначити потенційні способи обходу механізмів контролю та загрози для чесності змагального процесу.

Виконано систематизацію відомих CVE, що стосуються платформ на кшталт Steam, визначено домінуючі класи вразливостей (ескалація привілеїв, інжекція, файлові маніпуляції, RCE), що забезпечило формування узагальненого профілю ризиків ігрових екосистем.

Проведено детальне дослідження технічних вразливостей сучасних платформ, включно з Steam, визначено їх архітектурні передумови та можливі сценарії експлуатації, що дозволило встановити пріоритетні напрями підвищення безпеки.

Описано принцип роботи методу BaitAndSwitch, проаналізовано

можливість його використання для ескалації привілеїв через маніпуляції файловими шляхами та правами доступу, що дало змогу продемонструвати практичні ризики для платформізованих ігрових сервісів.

Розроблено комплексну методику запобігання піратству у кіберспорті, яка охоплює технічні, організаційні, поведінкові та правові заходи, що забезпечило формування цілісного підходу до захисту кіберспортивних екосистем від порушень авторських прав та експлуатації вразливостей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2163-19 (дата звернення: 05.11.2025). Закон України+1

2. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР (чинна редакція) // База даних «Законодавство України». URL: https://cis-legislation.com/document.fwx?rgn=11676 (дата звернення: 05.11.2025). cis-legislation.com

3. Кримінальний кодекс України : Кодекс України від 05.04.2001 № 2341-III (із змінами) // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/laws/show/en/2341-14 (дата звернення: 05.11.2025). Закон України

4. Про авторське право і суміжні права : Закон України від 01.12.2022 № 2811-IX // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/2811-20 (дата звернення: 05.11.2025). Закон України+1

5. Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 19.06.2019 № 518 // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/go/518-2019-%D0%BF (дата звернення: 05.11.2025). Закон України+1

6. Деякі питання об’єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 09.10.2020 № 1109 (чинна редакція) // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/go/1109-2020-%D0%BF (дата звернення: 05.11.2025). Закон України

7. Деякі питання реагування суб’єктами забезпечення кібербезпеки на різні види подій у кіберпросторі : Постанова Кабінету Міністрів України від 04.04.2023 № 299 // База даних «Законодавство України». URL:

https://zakon.rada.gov.ua/go/299-2023-%D0%BF (дата звернення: 05.11.2025). Закон України

8. Методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі : наказ Адміністрації Держспецзв'язку від 03.07.2023 № 570 // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/go/v0570519-23 (дата звернення: 05.11.2025). Закон України

9. Правила надання та отримання телекомунікаційних послуг : Постанова Кабінету Міністрів України від 11.04.2012 № 295 (у частині захисту прав споживачів електронних комунікацій) // База даних «Законодавство України». URL: https://zakon.rada.gov.ua/go/295-2012-%D0%BF (дата звернення: 05.11.2025). Закон України

10. (Довідково щодо оформлення посилань) ДСТУ 8302:2015. Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. Київ : Мінекономрозвитку України, 2016. URL: https://kubg.edu.ua/images/stories/podii/2017/06_21_posylannia/dstu_8302.pdf (дата звернення: 05.11.2025). Київський університет бориса грінченка

11. Online piracy study: Europeans are consuming more pirated TV shows and live sports : EUIPO, 2024. URL: https://www.euipo.europa.eu/sk/news/online-piracy-study-europeans-are-consuming-more-pirated-tv-shows-and-live-sports (дата звернення: 05.11.2025). euipo.europa.eu

12. How does Europe fight piracy of online sports events? : European Audiovisual Observatory, 2021. URL: https://www.obs.coe.int/en/web/observatoire/home/-/asset_publisher/wy5m8bRgOygg/content/how-does-europe-fight-piracy-of-online-sports-events- (дата звернення: 05.11.2025). obs.coe.int

13. Sports events piracy continues to rise : LaLiga, 11.03.2025. URL: https://www.laliga.com/en-GB/news/sports-events-piracy-continues-to-rise (дата звернення: 05.11.2025). Página web oficial de LALIGA | LALIGA

14. ARCOM reports illegal sports site & domain blocking for 2022–2024 and 2025 through April : Piracy Monitor, 15.05.2025. URL:

https://piracymonitor.org/france-arcom-reports-illegal-sports-site-domain-blocking-for-2022-2024-and-2025-through-april/ (дата звернення: 05.11.2025). piracymonitor.org

15. Strategic Intelligence: Media Piracy in Sport 2024 : Research and Markets, 21.11.2024. URL: https://www.globenewswire.com/news-release/2024/11/21/2985037/28124/en/The-Rise-of-Media-Piracy-in-Sports.html (дата звернення: 05.11.2025). GlobeNewswire

16. Video Game Piracy as Viral Vector and National Security Threat : Indiana Law Journal, 2018. URL: https://www.repository.law.indiana.edu/context/ilj/article/11304/viewcontent/Typhoid_Mario___Video_Game_Piracy_as_Viral_Vector_and_National_Security_Threat.pdf (дата звернення: 05.11.2025). repository.law.indiana.edu+1

17. Unveiling the Connection Between Malware and Pirated Software : University of Nebraska-Lincoln, 2024. URL: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1377&context=csearticles (дата звернення: 05.11.2025). digitalcommons.unl.edu

18. OECD. Piracy of Digital Content (з кейсом щодо спортивних прав) : OECD/SROC, 2009. URL: https://www.sroc.info/wp-content/uploads/2018/02/OECD_study_-_piracy.pdf (дата звернення: 05.11.2025). sroc.info

19. MUSO says 2024 piracy was down somewhat from 2023… : Piracy Monitor, 11.06.2025. URL: https://piracymonitor.org/muso-says-2024-piracy-was-down-marginally-from-2023-except-for-publishing/ (дата звернення: 05.11.2025). piracymonitor.org

20. The growing problem of live sports broadcast piracy : Addisons, 15.03.2024. URL: https://addisons.com/article/the-growing-problem-of-live-sports-broadcast-piracy-copyright-protection-and-available-counter-technologies/ (дата звернення: 05.11.2025). Addisons | Sydney Law Firm

21. CVE-2015-7985 : National Vulnerability Database (NVD). URL: https://nvd.nist.gov/vuln/detail/CVE-2015-7985 (дата звернення: 05.11.2025).

Дублет: CVE Details. URL: https://www.cvedetails.com/cve/CVE-2015-7985/ (дата звернення: 05.11.2025). nvd.nist.gov+1

22. CVE-2019-14743 : CVE Details. URL: https://www.cvedetails.com/cve/CVE-2019-14743/ (дата звернення: 05.11.2025). Додатково: аналітичний опис. URL: https://www.northit.co.uk/cve/2019/14743 (дата звернення: 05.11.2025). cvedetails.com+1

23. CVE-2019-15315 : National Vulnerability Database (NVD). URL: https://nvd.nist.gov/vuln/detail/CVE-2019-15315 (дата звернення: 05.11.2025). Дублет: CVE Details. URL: https://www.cvedetails.com/cve/CVE-2019-15315/ (дата звернення: 05.11.2025). nvd.nist.gov+1

24. CVE-2019-17180 : National Vulnerability Database (NVD). URL: https://nvd.nist.gov/vuln/detail/CVE-2019-17180 (дата звернення: 05.11.2025). Дублет: CVE Details. URL: https://www.cvedetails.com/cve/CVE-2019-17180/ (дата звернення: 05.11.2025). nvd.nist.gov+1

25. (Огляд/контекст) Третя уязвимость Steam Windows Client, але не 0-day : Habr, 01.10.2019. URL: https://habr.com/ru/companies/pm/articles/469507/ (дата звернення: 05.11.2025). Habr

26. Regulatory and legal framework (довідник актів з кіберзахисту, у т.ч. Постанова КМУ № 518) : Урядова команда реагування CERT-UA/CSIRT-НКЦКІ. URL: https://csirt.csi.cip.gov.ua/en/pages/regulatory-and-legal-framework (дата звернення: 05.11.2025). CSIRT

27. CERT-UA: Перелік категорій кіберінцидентів (таксономія) : cert.gov.ua. URL: https://cert.gov.ua/recommendation/16904 (дата звернення: 05.11.2025).

ДОДАТОК А

Копії публікацій

ГРОМАДСЬКА ОРГАНІЗАЦІЯ
«КІБЕРБЕЗПЕКА І АВТОМАТИЗАЦІЯ»

Матеріали
науково-практичного симпозіуму
«ЗАХИСТ ІНФОРМАЦІЇ»

30 листопада 2024
Тернопіль

У збірнику опубліковано матеріали науково-практичного симпозіуму «Захист інформації», Тернопіль, 2024. - 130с.

Технічний редактор: Давлетова А.Я.

Адреса редакції:
Громадська організація «Кібербезпека і автоматизація»
м. Тернопіль
Контактний телефон: (066)043-42-10
e-mail: conferencekb@gmail.com

УДК 004.056.5

Владислав БАГМЕТ

Західноукраїнський національний університет

ДОСЛІДЖЕННЯ МЕХАНІЗМІВ ПІРАТСТВА В КІБЕРСПОРТІ ТА СТРАТЕГІЇ ЗАПОБІГАННЯ

Вступ. Кіберспорт сьогодні є однією з найперспективніших галузей цифрової економіки, яка стрімко розвивається і привертає увагу мільйонів людей у всьому світі. Проте із зростанням його популярності виникає проблема піратства, що завдає серйозної шкоди правовласникам, організаторам турнірів, платформам і гравцям. Піратство у кіберспорті не лише зменшує доходи індустрії, але й підриває довіру до легальних платформ. Саме тому дослідження механізмів піратства у цій сфері та розробка ефективних стратегій запобігання є актуальним завданням.

Метою цього дослідження є вивчення сучасних механізмів піратства у кіберспорті та створення нових підходів, які дозволять ефективніше боротися із цим явищем.

1. Аналіз предметної області та існуючих підходів

За останнє десятиліття сфера кіберспорту стала невід'ємною частиною сучасної цифрової культури. У 2022 році обсяг глобального кіберспортивного ринку перевищив 1,3 мільярда доларів США, а аудиторія зросла до 532 мільйонів осіб, що свідчить про його важливість у світовій економіці. Проте розвиток індустрії супроводжується значними викликами, серед яких домінує проблема піратства [1].

Піратство у кіберспорті проявляється у кількох формах: нелегальні трансляції турнірів, крадіжка цифрового контенту (геймплей, відео, графіка), а також нелегальне використання облікових записів для отримання доступу до преміум-послуг. Згідно з даними досліджень, понад 50% нелегальних трансляцій кіберспортивних змагань припадають на соціальні платформи, такі як YouTube і Twitch. Ці ресурси надають можливість піратам легко монетизувати контент через рекламу або прямі донати, що створює значні фінансові втрати для правовласників. Сучасні технології іноді виявляються недостатньо гнучкими для адаптації до нових форм піратства. Наприклад, швидкий розвиток соціальних мереж і платформ для обміну відео значно ускладнює моніторинг та блокування нелегального контенту. Крім того, деякі платформи не зацікавлені у суворому дотриманні правил, оскільки піратський контент може залучати нову аудиторію [2].

Таким чином, аналіз предметної області показує, що для ефективної боротьби з піратством у кіберспорті необхідно вдосконалювати існуючі технології, підвищувати рівень співпраці між правовласниками, платформами та урядами, а також розробляти нові методи, які відповідають сучасним викликам.

2. Розробка стратегії запобігання піратству

Штучний інтелект (AI) є одним із ключових компонентів для боротьби з піратством. Технології AI забезпечують автоматичне виявлення піратського контенту, зокрема нелегальних трансляцій, через аналіз метаданих, вмісту відео та аудіо, а також зображень у

реальному часі. Інструменти, засновані на глибокому навчанні, дозволяють порівнювати піратські копії з оригінальним контентом і оперативно блокувати доступ. Наприклад, такі сервіси як Content ID від YouTube або Audible Magic широко застосовуються для моніторингу і блокування контенту.

Для кіберспортивних платформ можна запропонувати адаптацію цих технологій шляхом інтеграції в системи стримінгу. Наприклад, алгоритми машинного навчання можуть допомогти ідентифікувати нелегальні трансляції під час живих турнірів, одночасно подаючи запити на видалення до відповідних платформ або серверів, що розповсюджують піратський контент.

Блокчейн забезпечує прозорість у відстеженні прав на контент, надаючи можливість створення незмінних записів про авторські права та ліцензії. У кіберспорті блокчейн може використовуватися для реєстрації унікальних цифрових підписів кожного відео, стриму або іншого виду контенту. Смарт-контракти можуть автоматизувати ліцензування, забезпечуючи, що доступ отримують тільки ті користувачі, які сплатили за перегляд або мають офіційну підписку [3].

Окрім цього, впровадження криптовалют може стати частиною антипіратської стратегії, забезпечуючи легальний обіг коштів і знижуючи ризики використання нелегальних платіжних систем для монетизації піратського контенту.

Освітні програми спрямовані на інформування користувачів про ризики і негативні наслідки споживання піратського контенту. Кампанії можуть включати:

- Промо-відео, які пояснюють втрати індустрії від піратства.
- Проведення лекцій та вебінарів для геймерів і фанатів кіберспорту щодо етичного використання контенту.
- Інтерактивні заходи, наприклад, участь у легальних турнірах з доступом до ексклюзивного контенту.

Стратегія боротьби з піратством у кіберспорті повинна включати ряд комплексних заходів. Пропонується використання стратегії що на рисунку 1.

Рисунок 1 - Схема запропонованої стратегії боротьби з піратством у кіберспорті

Ключовим фактором ефективної стратегії є співпраця між платформами стримінгу, організаторами кіберспортивних заходів і урядовими організаціями. Пропонується створення альянсу, в якому учасники зможуть обмінюватися інформацією про піратський контент, об'єднувати ресурси для боротьби з незаконним використанням контенту, а також координувати дії щодо вдосконалення законодавства. Використання технологій для захисту авторських прав на контент, що транслюється можна з допомогою DRM(Digital Rights Management), котрий обмежує копіювання, запис та розповсюдження відео трансляцій, ігор чи іншого цифрового контенту. Відео та аудіоконтент часто позначають невидимими водяними знаками, які дозволяють відстежувати джерело витоку. Країни приймають закони, що охоплюють захист контенту в кіберспорті. Наприклад, закони DMCA (Digital Millennium Copyright Act) у США. Такі ініціативи, як Global Esports Federation, можуть стати основою для створення загальної бази даних піратських ресурсів, спрощуючи моніторинг і контроль.

Одним із способів стимулювання користувачів до використання легального контенту є створення привабливих економічних пропозицій. Це може включати:

- Програми лояльності для підписників офіційних платформ.
- Знижки на підписки, спонсорські програми або доступ до ексклюзивних турнірів.
- Розіграш призів серед тих, хто підтримує легальний контент, наприклад, доступ до закритих ігор чи прямого спілкування з професійними гравцями.

На рівні законодавства важливо розробити комплексні норми, які передбачають:

- Автоматичне блокування ресурсів, що порушують авторські права.
- Швидку процедуру подачі скарг для правовласників.
- Впровадження штрафів для хостингів та платформ, які ігнорують звернення правовласників.

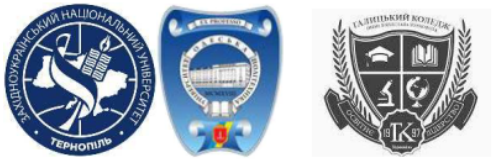
Висновок. Кіберспорт як одна з найперспективніших сфер цифрової економіки стикається з численними викликами у забезпеченні захисту інтелектуальної власності. Піратство, яке проявляється у формі нелегальних трансляцій, крадіжки контенту та зловживання обліковими записами, завдає значних економічних втрат і підриває довіру до галузі. Проблема піратства у кіберспорті є багатогранною і потребує комплексного підходу для її вирішення. Попри наявність значних зусиль з боку індустрії, проблема залишається актуальною через швидку еволюцію методів піратства та недостатню координацію між правовласниками, платформами і регуляторами. Важливим аспектом є координація дій на міжнародному рівні, яка сприятиме більш ефективній протидії порушенням авторських прав.

Перелік використаних джерел.

1.Малюк Є. О. «Social transformations and distribution of pirated media content on the example of video games.» - Науковий журнал «Схід», 2022. С. 40-46.

2. AlAbdali, H., AlBadawi, M., Sarrab, M., & AlHamadani, A., 2021. Privacy Preservation Instruments Influencing the Trustworthiness of e-Government Services. Computers, Vol. 10, No. 9, p114

3. Effah J., Nuhu H. 2017. Institutional barriers to digitalization of government budgeting in developing countries: A case study of Ghana. The Electronic Journal of Information Systems in Developing Countries, Vol. 82, No. 1, pp 1-17.



ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»
ГАЛИЦЬКИЙ ФАХОВИЙ КОЛЕДЖ ІМ. В'ЯЧЕСЛАВА ЧОРНОВОЛА

КІБЕРБЕЗПЕКА ТА КОМП'ЮТЕРНО-ІНТЕГРОВАНІ ТЕХНОЛОГІЇ (КБКІТ – 2025)

науково-практична конференція
молодих вчених, аспірантів та студентів

28–29 серпня 2025
Тернопіль

Збірник матеріалів науково-практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп'ютерно-інтегровані технології» (КБКІТ - 2025), Тернопіль, 2025. - 154 с.

Адреса редакції:
Західноукраїнський національний університет, кафедра кібербезпеки,
вул. Олени Теліги 8, м. Тернопіль 46003
Контакти:
*e-mail:*conferencekb@gmail.com

ЗМІСТ

СИСТЕМИ ТА ТЕХНОЛОГІЇ КІБЕРБЕЗПЕКИ

УДК 004.056.5

Владислав БАГМЕТ[1], Віктор ДЗЯДИК[2]

[1]Західноукраїнський національний університет
[2]Галицький фаховий коледж ім. В'ячеслава Чорновола

GAME VULNERABILITIES ЯК ЗАГРОЗА КІБЕРБЕЗПЕКИ

Вступ. Баги та вразливості у комп'ютерних іграх є поширеним явищем, особливо в продуктах, що були випущені значний час тому. Така тенденція пояснюється тим, що розробники зосереджують основні ресурси на створенні нових проєктів, тоді як підтримка старих версій поступово скорочується. D наслідок цього популярні ігри з часом перетворюються на зручне середовище для дослідження та експлуатації вразливостей. До кола потенційних цілей кіберзловмисників належать як розробники, так і користувачі ігор, а в окремих випадках навіть організації, у межах яких ці користувачі працюють.

Мета: дослідити поширені вразливості у популярних продуктах гейміндустрії.

1. Загрози використання службових ПК з ігровим ПЗ

Комп'ютерна гра є програмним продуктом, тому може містити помилки в реалізації чи пропуски під час тестування. Наявність таких дефектів підтверджується публічними реєстрами (CVE), які фіксують відомі вразливості та їхню класифікацію за рівнем загрози. З метою дослідження цієї проблеми було проведено аналіз даних агрегатора вразливостей і перевірено інформацію щодо окремих проєктів на платформі Steam. Для прикладу було відібрано CVE, пов'язані з клієнтом гри Dota 2, середній рейтинг тяжкості яких за шкалою CVSS становив 7,8 із 10 [1].

Серед виявлених інцидентів, найсерйозніша була зафіксована у 2023 році внаслідок дослідження, проведеного фахівцями Avast: клієнт Dota 2 використовував застарілу версію рушія JavaScript (V8), яка містила вразливість, що дозволяла виконувати небажаний JavaScript-код на машині користувача. Наслідком дефектів може бути несанкціоноване виконання коду на комп'ютері жертви та повна компрометація її середовища.

Подібні ситуації відзначалися й у інших популярних проєктах. Так, для серії Counter-Strike виявлено кілька CVE із середнім значенням CVSS близько 7,76, а у грудні 2023 року було продемонстровано реалізацію XSS-вектору в контексті нової функції додавання зображень у чаті, що створювало можливості цілеспрямованих атак на користувачів. У випадку GTA Online дефект, позначений як CVE-2023-24059, було виявлено та виправлено на початку 2023 року. Цей збій дозволяв не лише отримати дані облікових записів, а й розміщувати шкідливе програмне забезпечення (ПЗ)на пристроях жертв.

Слід підкреслити, що запис у реєстрі CVE відображає лише вразливості, які вже стали загальновідомими і, як правило, були усунуті та опубліковані. Отже, загальна кількість дефектів у продуктах ігрової індустрії, ймовірно, значно перевищує кількість задокументованих CVE. Додатково практикою є те, що постачальники ПЗ іноді мають відомості про певні вразливості, але затримують їх

усунення через пріоритети розробки або інші операційні причини. Прикладом є ситуація з проєктом Call of Duty: Black Ops III (реліз 2015 року), де було задокументовано повідомлення про RCE-вразливості, які залишалися невиправленими тривалий час. В наслідок відсутності офіційних виправлень частина спільноти розробників-ентузіастів змушена була створювати власні модифікації та виправлення, доступні у відкритих репозиторіях.

Отже, із встановленим ігровим ПЗ з'являється низка ризиків: від локальних компрометацій окремих робочих станцій до потенційного розповсюдження загроз у внутрішній корпоративній мережі. Це обґрунтовує необхідність оцінки ризиків використання ігрового ПЗ на службі та запровадження політик контролю встановлення й оновлення програмного забезпечення, а також засобів виявлення й реагування на інциденти кібербезпеки.

2. Основні загрози ігровим акантам

Переважна більшість інцидентів із компрометацією облікових записів геймерів мають соціо-інженерний характер, причому найпоширенішим інструментом виступає фішинг. Атаки такого типу організовуються через чати, тематичні форуми та інші майданчики спільнот; їхня популярність пояснюється простотою реалізації та низькими витратами для зловмисника. Типовим прикладом є шахрайські схеми «я продав тобі, але ти не заплатив», які спрямовані на отримання облікових даних або доступу до платіжних інструментів жертви.

Технічно складніші вектори, що використовують програмні вразливості ігрових клієнтів або плагінів, зустрічаються рідше, оскільки вимагають відповідних навичок і часу на розробку експлойтів. Водночас такі атакувальні сценарії не є поодинокими і використання вразливостей може призводити до віддаленого виконання коду, підміни сесійних токенів або похищення облікових даних без прямого залучення користувача. Наслідком експлуатації вразливостей найчастіше стає крадіжка акаунтів, що, з огляду на розвиток внутрішньоігрових ринків, може мати значну матеріальну шкоду. Прикладом є інцидент 2022 року з відомим колекціонером предметів у грі серії Counter-Strike, в результаті якого було втрачене право розпоряджатися скінами загальною вартістю близько мільйонів доларів.

Значну загрозу також становить використання модифікованих або нелегально отриманих інсталяційних образів. Піратський софт, поширюваний через торренти й подібні ресурси, часто постачається разом із бекдорами та іншими типами шкідливого ПЗ, що робить його джерелом компрометації кінцевих пристроїв. У багатьох випадках саме завантаження та запуск модифікованих інсталяторів стають початковою точкою проникнення.

Окрему категорію ризиків формують користувацькі практики, які навмисно або мимоволі знижують рівень захисту кінцевої системи. Частина гравців вимикає антивірусні рішення або брандмауери, посилаючись на їх вплив на продуктивність або сумісність із грою. Інші користувачі взагалі відмовляються від активних засобів захисту. Ефективність таких налаштувань у сенсі підвищення продуктивності є предметом дискусій, натомість їхній внесок у підвищення вразливості системи виявлена й документована, зокрема зниження рівня захисту істотно збільшує ймовірність успішної компрометації облікових

записів і пристроїв.

Загрози ігровим акаунтам мають багатовимірний характер, від простих соціо-інженерних схем до технічно складних експлуатацій вразливостей і постачання шкідливого ПЗ разом із піратським контентом.Ускладнює ситуацію також поведінка користувачів, що іноді свідомо знижують заходи захисту. Це підкреслює необхідність комплексного підходу - поєднання технічних засобів, освітніх ініціатив для спільнот і проактивного моніторингу інцидентів.

3. Загрози додаткового ПЗ

Багато загроз також несуть у собі програми, які геймери активно використовують крім ігор. Вони теж можуть містити критичні дефекти безпеки, як це показано в таблиці 1.

Таблиця 1 – Вразливості ігрових майданчиків та спеціального ПЗ

Steam та інші майданчики для розміщення ігор	Особливо небезпечна вразливість у Steam була виявлена у 2020 році. Використовуючи її, зловмисник міг захопити сотні тисяч комп'ютерів, не вимагаючи від геймерів натискати на шкідливий лист або посилання. На відміну від інших уразливостей, жертви несвідомо траплялися під вплив хакера. Для цього їм потрібно було просто увійти до гри. У 2023 році зловмисники зламали облікові записи сотні розробників на платформі Steam і додали до їхніх ігор шкідливе ПЗ. Але вендор швидко виявив проблему і повідомив про це користувачам.
Discord та інші утиліти для спілкування з командою	Повідомлень про проблеми у продукті чимало. Наприклад, минулого року розробник визнав витік даних 760 тис. користувачів, яка сталася з вини співробітника.
GeForce Experience, OBS Studio та інші програми для запису відео, оцінки FPS тощо.	У 2020 році розробник GeForce Experience залатав відразу дві серйозні дірки. Одна з уразливостей (CVE-2020-5977) отримала CVSS 8,2 і могла призвести до безлічі шкідливих атак на порушені системи, включаючи виконання коду, відмову в обслуговуванні, підвищення привілеїв та розкриття інформації.
AutoHotKey та аналоги для налаштування кнопок клавіатури та миші	З його допомогою злочинці поширювали трояни для віддаленого доступу до пристроїв жертв, у тому числі Revenge RAT, LimeRAT, AsyncRAT, Houdini та Vjw0rm.
Spotify та інші сервіси для прослуховування музики під час гри	У 2020 році через виток даних Spotify скинув 350 тис. паролів користувачів. Хоча в офіційній заяві власник продукту повідомив, що проблема торкнулася лише невеликої частини акаунтів.

CVE-2020-5977 - уразливість типу «небезпечний/неконтрольований пошук шляху завантаження модулів» (untrusted search path) в компоненті, що

використовує середовище виконання Node.js. Через цю слабину процес, який завантажує модулі Node.js (через require() / import), може підхопити шкідливий модуль із непередбачуваного або керованого зловмисником каталогу. Унаслідок цього можливе виконання довільного коду в контексті вразливого процесу, що може призвести до локальної компрометації системи.

Схема вразливості CVE-2020-5977 приведена на рисунку 1.

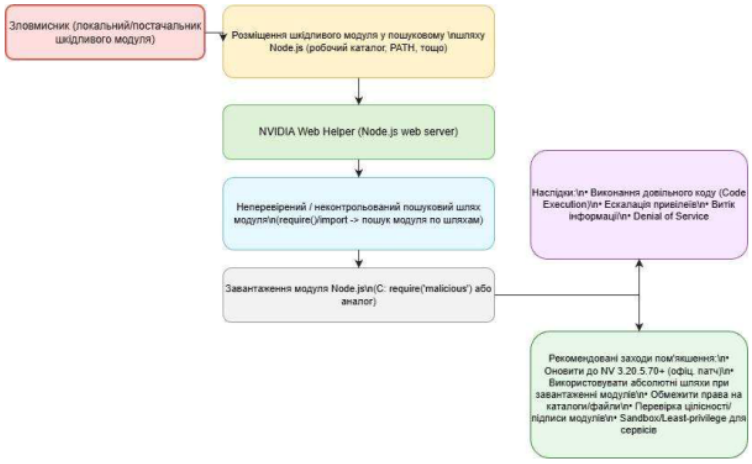


Рисунок 1 - Схема вразливості CVE-2020-5977

CVE-2020-5977 належить до класу вразливостей, які використовують недоліки в управлінні шляхами завантаження модулів у середовищах виконання, таких як Node.js. Механізм експлуатації є концептуально простим, проте практичні наслідки можуть бути критичними. Найефективнішими заходами захисту є своєчасне оновлення ПЗ, управління правами доступу, використання перевірок цілісності модулів та впровадження контролю завантажених компонентів у рантаймі.

Висновок. Безпека відеоігор є багатовимірною проблемою, що поєднує технічні вразливості програмного коду, ризики соціальної інженерії та операційні загрози, пов'язані з практиками розповсюдження та використання ПЗ. Наслідки експлуатації вразливостей охоплюють як індивідуальні втрати користувачів, так і бізнес-ризики для розробників та їхньої інфраструктури. Ефективна протидія потребує комбінованого підходу, що включає безпечну розробку, регулярне патчування, контроль цілісності файлів і жорстке управління правами доступу. Додатково необхідні механізми та інструменти моніторингу (EDR, HIDS, SIEM), а також просвітницькі заходи для користувацької спільноти щодо фішингу та безпечних практик. Лише системне поєднання технічних, організаційних і правових заходів здатне істотно знизити експлуатаційний ризик і підтримати довгострокову стійкість ігрової екосистеми.

Перелік використаних джерел.

1. CVE-2015-7985. [Електронний ресурс]. - Режим доступу: https://nvd.nist.gov/vuln/detail/CVE-2015-7985.

2. CVE-2020-5977. [Електронний ресурс]. - Режим доступу: https://nvd.nist.gov/vuln/detail/CVE-2020-5977.

ДОДАТОК Б.

Вразливості ігрових платформ

CVE (рік)	Компонент / вплив	Стислий опис вразливості	Тактики / техніки експлуатації (TTP)	Рекомендовані контрзаходи
CVE-2019-14743 (2019) (cvedetails.com)	Steam Client (Windows) — неправильні права в реєстрі	Наявність надмірних прав (Full control для групи Users) на гілці реєстру `HKLM\SOFTWARE\Wow6432Node\Valve\Steam` дозволяла локальному користувачеві ескалювати привілеї до SYSTEM.	Тактики: локальна ескалація привілеїв через зміни в реєстрі; заміна/повернення (rollback) компонентів; створення/запис шкідливих значень реєстру; запуск троянізованих бінарів з підвищеними правами.	Видалення зайвих прав для непотрібних груп; патч від постачальника; перевірка цілісності компонентів при запуску; обмеження write/modify прав у файловій/реєстровій системі; моніторинг змін реєстру (HIDS/EDR). (cvedetails.com)
CVE-2019-15315 (2019) (nvd.nist.gov)	Steam Client (Windows) — можливість заміни файлів	Дозволяла локальній загрозі замінити SteamService.exe/SteamService.dll старішими уразливими версіями (rollback), що призводило до ескалації привілеїв (NT AUTHORITY\SYSTEM).	Тактики: заміна бінарників/rollback атака; використання сервісного механізму для запуску керованого коду в контексті SYSTEM; підготовка троянів у директоріях з ослабленими правами.	Застосування захисту від rollback: підписування бінарників та перевірка цифрового підпису при запуску; налаштування ACL на папки встановлення; блокування можливості запису для неприпустимих користувачів; контроль версій у процесі оновлення;

				integrity-check при інсталяції. (nvd.nist.gov)
CVE-2019-17180 (2019) (CloudDefense.AI)	Steam Client — маніпуляція файловою системою	Вразливість дозволяла створювати або апендувати частково контрольований вміст у файлах, що могло привести до модифікації файлів у контексті SYSTEM (DoS/EoP/несанкціоновані зміни).	Тактики: створення/апендування файлів із керованим контентом; підміна файлів, що виконуються під SYSTEM; інжекція даних у конфіг/лог-файли; тригеринг процесів для виконання модифікованого вмісту.	Закриття можливостей запису в критичних папках; перевірка дозволів; обмеження прав сервісів; integrity/white list-підхід до критичних файлів; моніторинг файлових змін. (CloudDefense.AI)
CVE-2015-7985 (2015) (vulners.com)	Steam Client — слабкі дозволи на папку інсталяції	Недостатньо суворі ACL для папки встановлення (Users мали write/modify), що дозволяло локальним користувачам підкласти шкідливі steam.exe тощо.	Тактики: Trojan-horse (підміна steam.exe), місцевий запуск шкідливого бінарника, ескалація прав через сервіс, виклик виконання через автозапуск/сервіс.	Встановлення мінімально необхідних прав для папок встановлення; digital signature verification; захист від запуску з неочікуваних шляхів; контроль запуску сервісів; HIPS/EDR. (vulners.com)
CVE-2021-30481 (2021) (cvedetails.com)	Source Engine (Steam) — buffer overflow via Steam invite	Коли установлена гра на Source engine отримувала Steam-invite, буферне переповнення могло дати віддалене (аутентифіковане) виконання коду у контексті клієнта. Вразливість впливала на багато ігор на Source engine.	Тактики: remote authenticated code execution (RCE) через спеціально створене Steam-invite; доставка payload у форматі запрошення; підштовхування жертви натиснути/відкрити	Оновлення рушія/гри (виробник випустив фікс); фільтрація/валідація вхідних параметрів у Steam-invite обробках; застосування принципу least privilege

			запрошення; подальше локальне виконання коду.	для клієнтських компонентів; sandboxing і monitoring процесів гри; розумна політика прийому запрошень (UX-фільтр). (nvd.nist.gov)
CVE-2025-27998 (2025) (nvd.nist.gov)	Steam Client — ескалація привілеїв через crafted executable /DLL (зв'язано з CWE-94)	Нова вразливість, пов'язана з можливістю ескалації привілеїв шляхом спеціально створеного виконуваного файлу або DLL (code injection / code exec). (Офіційні advisories / оновлення — див. джерела).	Тактики: підміна DLL (DLL hijacking), запуск зламаного exe, інжекція/підвантаження шкідливого коду в процеси з підвищеними правами, exploitation через неперевірені шляхи/параметри.	Негайне застосування оновлення від Valve; цифрове підписування і валідація DLL/EXE; обмеження write-доступу до директорій; контроль запуску сервісів; застосування ASLR/DEP/CFG для зменшення успішності інжекцій. (nvd.nist.gov)