

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій  
(повне найменування факультету)

Кафедра «Інформаційна безпека та наноелектроніка»  
(повне найменування кафедри)

**Пояснювальна записка**

до дипломного проєкту (роботи)

бакалавр  
(ступінь вищої освіти)

на тему Аналіз роботи DRM систем, та їх впливу на  
продуктивність у відеоіграх  
(назва теми)

Analysis of DRM systems and their impact on performance in video games

Виконав: студент 4 курсу, групи БК-710  
Спеціальності 125 Кібербезпека  
(код і найменування спеціальності)

Освітня програма (спеціалізація)  
Системи технічного захисту інформації,  
автоматизація її обробки

ЛЕВЧЕНКО І.А.  
(ПРІЗВИЩЕ та ініціали)

Керівник КОРОЛЬКОВ Р.Ю.  
(ПРІЗВИЩЕ та ініціали)

Рецензент МАЛИЙ О.Ю.  
(ПРІЗВИЩЕ та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
Національний університет «Запорізька політехніка»

Факультет інформаційної безпеки та електронних комунікацій  
Кафедра інформаційної безпеки та наноелектроніки  
Ступінь вищої освіти бакалавр  
Спеціальність 125 Кібербезпека  
(код і найменування)  
Освітня програма (спеціалізація) Системи технічного захисту інформації, автоматизація її обробки  
(назва освітньої програми (спеціалізації))

**ЗАТВЕРДЖУЮ**

Завідувач кафедри ІБтаН

Андрій КОРОТУН

«      »        20   року

**З А В Д А Н Н Я**  
**НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА**

ЛЕВЕНКО Івана Андрійовича

(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи) Аналіз роботи DRM систем, та їх впливу на продуктивність у відеоіграх

Analysis of DRM systems and their impact on performance in video games

керівник проєкту (роботи) доцент, к.т.н. КОРОЛЬКОВ Роман Юрійович.

(науковий ступінь, вчене звання, ПРИЗВИЩЕ, ім'я, по батькові)

затверджені наказом закладу вищої освіти від «03» травня 2024 року №190

2. Строк подання студентом проєкту (роботи) 03 червня 2024 року

3. Вихідні дані до проєкту (роботи) Проаналізувати вплив цифрових прав управління на продуктивність відеоігор

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Загальні положення цифрових прав управління, аналіз атак на системи цифрових прав управління, дослідження впливу DRM захисту на продуктивність відеоігор

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)

Презентація доповіді (в MS PowerPoint), 14 слайдів

6. Консультанти розділів проєкту (роботи)

| Розділ        | ПРИЗВИЩЕ, ініціали та посада консультанта | Підпис, дата   |                           |
|---------------|-------------------------------------------|----------------|---------------------------|
|               |                                           | завдання видав | прийняв виконане завдання |
| Розділи 1-3   | КОРОЛЬКОВ Р.Ю. доцент, к.т.н.             | 15.04.2024     | 27.05.2024                |
| Нормоконтроль | КОРОЛЬКОВ Р.Ю. доцент, к.т.н.             |                |                           |

7. Дата видачі завдання «15» Квітня 2024 року.

КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів дипломного проєкту (роботи)                        | Строк виконання етапів проєкту ( роботи ) | Примітка |
|-------|-----------------------------------------------------------------|-------------------------------------------|----------|
| 1     | Аналіз історії розвитку DRM систем                              | 1-2 тиждень                               | Виконано |
| 2     | Вивчення структури організацій, що займаються зломом ігор.      | 3 тиждень                                 | Виконано |
| 3     | Аналіз причин видалення або зберігання DRM захисту у відеоіграх | 3-4 тиждень                               | Виконано |
| 4     | Формування списку ігор для тестування                           | 5 тиждень                                 | Виконано |
| 5     | Забезпечення умов тестування. Збірка обладнання                 | 5 тиждень                                 | Виконано |
| 6     | Тестування ігор з різними конфігураціями систем                 | 6-7 тиждень                               | Виконано |
| 7     | Формування звіту і висновків тестування                         | 7 тиждень                                 | Виконано |

Студент(ка)

( підпис )

Іван ЛЕВЧЕНКО

(Ім'я ПРИЗВИЩЕ)

Керівник проєкту (роботи)

( підпис )

Роман КОРОЛЬКОВ

(Ім'я ПРИЗВИЩЕ)

## АНОТАЦІЯ

Пояснювальна записка до дипломної кваліфікаційної роботи бакалавра:  
67 с., 6 табл., 36 рис., 23 джерел.

АВТОРСЬКІ ПРАВА, ПІРАТСТВО, ЗАХИСТ, ЗАХИСТ ВІДЕОІГОР, РОЗВИТОК DRM, СУЧАСНІ DRM СИСТЕМИ, ПРОДУКТИВНІСТЬ ЗЛАМ ВІДЕОІГОР, ТЕСТУВАННЯ ІГОР, ЦИФРОВІ ПРАВА ВІДЕОІГРОВА ІНДУСТРІЯ.

Об'єкт дослідження: Цифрові права управління та їх вплив на продуктивність відеоігор.

Предмет дослідження: Впровадження та розвиток DRM систем в ігровій індустрії, а також атаки на ці системи та їх вплив на продуктивність відеоігор.

Мета дослідження: Проаналізувати вплив цифрових прав управління на продуктивність відеоігор, дослідити методи та засоби захисту від піратства, вивчити типи та організаційні структури груп, які займаються зломом відеоігор, та визначити реакцію розробників після злomu гри.

Практичне значення результатів: Результати дослідження висвітлюють важливі аспекти захисту відеоігор та їх вплив на продуктивність. Ця інформація може бути корисною для розробників програмного забезпечення, виробників відеоігор, а також для спеціалістів у галузі інформаційної безпеки та захисту авторських прав. Відомості, отримані в ході дослідження, можуть бути використані для покращення методів захисту відеоігор від незаконного копіювання та злomu, що покликане забезпечити кращий досвід для користувачів та збільшити прибуток для розробників.

## **ABSTRACT**

Explanatory note to the bachelor's diploma qualification work: 67 p., 6 tables, 36 figures, 23 sources.

COPYRIGHT, PIRACY, PROTECTION, VIDEO GAME PROTECTION, DRM DEVELOPMENT, MODERN DRM SYSTEMS, VIDEO GAME PERFORMANCE, GAME TESTING, DIGITAL RIGHTS, VIDEO GAME INDUSTRY.

Object of the study: Digital Rights Management and their impact on video game performance.

Subject of the study: The implementation and development of DRM systems in the gaming industry, as well as attacks on these systems and their impact on video game performance.

Purpose of the study: Analyze the impact of Digital Rights Management on video game performance, investigate methods and means of protection against piracy, study the types and organizational structures of groups involved in video game cracking, and determine the developers' reactions after a game is cracked.

Scientific and practical significance of the results: The results of the study highlight important aspects of video game protection and their impact on performance. This information can be useful for software developers, video game producers, as well as specialists in the field of information security and copyright protection. The findings from the research can be used to improve methods of protecting video games from illegal copying and cracking, which is aimed at ensuring a better user experience and increasing profits for developers.

## ЗМІСТ

|                                                                                             |    |
|---------------------------------------------------------------------------------------------|----|
| Перелік скорочень .....                                                                     | 7  |
| Вступ.....                                                                                  | 8  |
| 1 Загальні положення та застосування цифрових прав управління в відеоігровій індустрії..... | 9  |
| 1.1 Впровадження, розвиток та застосування цифрових прав управління .....                   | 9  |
| 1.2 Боротьба з піратством у минулому: методи та засоби захисту відеоігор ...                | 13 |
| 1.3 Сучасні DRM системи в ігровій індустрії .....                                           | 18 |
| 2 Атаки на системи DRM у відеоігровій індустрії.....                                        | 26 |
| 2.1 Фактори та мотивації злому відеоігор.....                                               | 26 |
| 2.2 Типи та організаційна структура груп, які займаються зломом відеоігор .                 | 29 |
| 2.3 Реакція розробників після злому гри: усунення чи збереження <i>denovo</i> ....          | 34 |
| 3 Практичне дослідження впливу DRM захисту на продуктивність відеоігор...                   | 39 |
| 3.1 Вибір ігор та розробка методології тестування.....                                      | 39 |
| 3.2 Порівняльний аналіз результатів тестування .....                                        | 42 |
| Висновки .....                                                                              | 64 |
| Перелік джерел посилання .....                                                              | 65 |

## ПЕРЕЛІК СКОРОЧЕНЬ

- ГП - Графічний процесор;
- ОЗУ - Оперативна запам'ятовуюча установа (оперативна пам'ять);
- ПК - Персональний комп'ютер;
- ЦП - Центральний процесор;
- DLC - Downloadable content (завантажуваний контент);
- DMCA - Digital Millennium Copyright Act (Закон про авторське право в цифрову епоху);
- DRM - Digital Rights Management (цифрове управління правами);
- FPS - Frames per second (кадри на секунду);
- NFO - Інформаційний файл (від англ. "info", часто використовується у спільнотах, пов'язаних з обміном файлів).

## ВСТУП

У сучасному світі відеоігрова індустрія займає одну з провідних позицій серед розважальних галузей, привертаючи увагу мільйонів гравців по всьому світу. З розвитком технологій і збільшенням обсягів цифрового контенту питання захисту інтелектуальної власності стає дедалі актуальнішим. Цифрові права управління (DRM) стали ключовим інструментом у боротьбі з піратством, забезпечуючи збереження авторських прав розробників і видавців відеоігор.

Ця робота присвячена вивченню загальних положень та застосування цифрових прав управління у відеоігровій індустрії. Аналізуються основні принципи впровадження, розвитку та застосування DRM систем, які пройшли значний шлях від початкових методів захисту на фізичних носіях до сучасних цифрових рішень. DRM технології постійно вдосконалюються, пристосовуючись до нових викликів та потреб індустрії, що робить їх невід'ємною частиною сучасного процесу розробки відеоігор.

Сучасні DRM системи в ігровій індустрії представляють собою складні технологічні рішення, що використовуються для захисту відеоігор від піратства. Важливою частиною дослідження є аналіз різних типів DRM, їхніх функцій та впливу на користувачів і розробників. Особлива увага приділяється оцінці ефективності DRM систем у сучасних умовах, їхньому впливу на продуктивність гри та користувацький досвід.

В Україні кримінальна відповідальність за порушення авторських прав передбачена статтею 176 Кримінального кодексу України. За незаконне відтворення, розповсюдження творів, а також інше порушення авторського права і суміжних прав може бути призначено покарання у вигляді штрафу, виправних робіт або позбавлення волі на строк до двох років. Якщо порушення вчинено повторно або завдало значної шкоди, термін позбавлення волі може бути збільшений до шести років.

# **1 ЗАГАЛЬНІ ПОЛОЖЕННЯ ТА ЗАСТОСУВАННЯ ЦИФРОВИХ ПРАВ УПРАВЛІННЯ В ВІДЕОІГРОВІЙ ІНДУСТРІЇ**

## **1.1 Впровадження, розвиток та застосування цифрових прав управління**

Впровадження, розвиток та застосування цифрових прав управління відіграли значну роль у становленні сучасної інформаційної епохи. Від моменту початкового виникнення систем управління цифровими правами (DRM) наприкінці 1980-х років до сьогоднішнього дня пройшло значне число років, протягом яких ці технології постійно еволюціонували та вдосконалювалися. Зародження DRM систем було ключовим етапом у формуванні сучасної інформаційної політики та правової практики в галузі захисту авторських прав.

Протягом цього періоду були впроваджені та стандартизовані різноманітні методи та технології управління цифровими правами. Важливими подіями у розвитку DRM були поява Software Service System у 1988 році, концепція Superdistribution у 1990 році, прийняття WIPO Copyright Treaty у 1996 році та Digital Millenium Copyright Act у 1998 році. Особливе значення має стандарт OMA DRM (від Open Mobile Alliance), представлений у трьох версіях: OMA DRM 1.0 (2004 рік), OMA DRM 2.0 (2006 рік) та OMA DRM 2.1 (2009 рік).

DRM - це комплекс технологій та стратегій, спрямованих на захист авторських прав та контроль над розповсюдженням цифрового контенту. DRM використовується у різних галузях, включаючи музику, кіно, літературу, програмне забезпечення, та, звичайно, відеоігри. Вона дозволяє контент-провайдерам обмежувати доступ до свого контенту та забезпечувати його цілісність, перешкоджаючи несанкціонованому використанню та поширенню. Перші концепції DRM з'явилися в кінці 20-го століття, а з розвитком технологій вони стали невід'ємною частиною цифрової індустрії.

Software Service System, розроблена для захисту програмного забезпечення від несанкціонованого використання та стимулювання плавного маркетингу, є першою згадкою прототипу DRM системи. Система не накладає жодних

обмежень на користувачів, за винятком запиту на відповідні платежі. Користувач може створити резервну копію програмного забезпечення та використовувати його в будь-якій частині файлової системи або комп'ютерної мережі. Програмне забезпечення може бути обмінюване не лише за допомогою дискет, але й будь-яким носієм, включаючи комунікаційний канал та трансляцію. Користувач може придбати програмне забезпечення на платній основі з будь-якого носія та здійснити його тестування або скасувати покупку у разі незадоволення. Для реалізації такої вільної схеми використання разом із захистом безпеки, а також дуже ефективного ринкового каналу, необхідно встановити автоматичне строге управління власністю для програмного забезпечення, а також уважно розроблену систему збору платежів. Введення загальних кредитів та програм дозволів служить для автоматизації управління програмним забезпеченням. Реалізація комп'ютера з функцією управління власністю та його операцій обговорюється для досягнення автоматизованого управління.

Superdistribution - це метод розповсюдження цифрових продуктів, таких як програмне забезпечення, відео та музика, через інтернет або мобільні мережі в зашифрованому вигляді. Власники продукту можуть зберігати контроль над його використанням, надаючи користувачам можливість обміну продуктом. Це створює ефективний канал розповсюдження без перешкод, дозволяючи будь-кому стати дистриб'ютором. Цей метод був винайдений в 1983 році японським інженером Рйюічі Морі та патентований ним у 1990 році. Ключові компоненти системи - криптографічна обгортка для продуктів, система управління цифровими правами та механізм безпечних платежів.

Міжнародний договір з авторського права, ухвалений державами-членами Всесвітньої організації інтелектуальної власності (WIPO) у 1996 році- це WIPO Copyright Treaty. Цей договір надає додаткові заходи захисту авторських прав у зв'язку з швидким розвитком інформаційних технологій. Він визначає права авторів на їхні твори, зокрема, забороняючи обхід технічних заходів захисту та несанкціоновані зміни інформації про управління правами в роботах. Також цей договір має за мету заохочувати творчість та забезпечувати авторам контроль над

їхніми творами. Він став важливим інструментом у сфері авторського права та захисту інтелектуальної власності у добу цифрової економіки та глобалізації.

Закон про авторське право в цифрову епоху (Digital Millennium Copyright Act, DMCA) 1998 року є важливим правовим документом, прийнятим для забезпечення дотримання авторських прав у цифрову еру. Він включає положення з Міжнародної конвенції з авторського права 1996 року та передбачає винятки для певних дій, пов'язаних з порушенням авторських прав, таких як безкоштовне використання в неприбуткових бібліотеках та освітніх закладах, оборотне проектування, дослідження шифрування, захист неповнолітніх, особиста приватність та тестування безпеки. Крім того, DMCA забороняє незаконне видалення технічних заходів захисту авторських прав та розповсюдження змінених матеріалів, захищених авторським правом. Цей закон виступає основою стандартів авторського права в Інтернеті і вирішує проблеми, що виникають внаслідок цифрових технологій у сфері захисту інтелектуальної власності.

OMA SpecWorks (раніше відома як Open Mobile Alliance) є організацією стандартизації, яка розробляє міжнародні технічні стандарти для мобільної телефонної індустрії. OMA DRM - це стандартна платформа для управління цифровими правами, розроблена Open Mobile Alliance для мобільних телефонів. Вона призначена для запобігання копіюванню та поширенню цифрового контенту власниками пристроїв, що використовують технології компаній-учасниць. Існують різні версії стандартів, такі як OMA DRM 1.0, OMA DRM 2.0 і OMA DRM 2.1.

OMA DRM 1.0, введена у 2004 році, встановила базові стандарти, які виробники пристроїв повинні були дотримуватися для впровадження OMA DRM у своїх продуктах. Ці стандарти включали методи DRM, такі як Forward Locking, який блокує можливість пересилання захищеного контенту між пристроями, та Combined Delivery, який дозволяв одночасно доставляти як контент, так і "Об'єкт прав" (ключ) в одному повідомленні DRM. Також був визначений метод Separate

Delivery, коли контент і Об'єкт прав доставлялися окремо. Контент та Об'єкт прав доставлялися за допомогою протоколів HTTP або WAP

OMA DRM 2.0, яка була запущена у 2006 році, представляє собою значний крок у розвитку цифрових технологій прав захисту. Нові функції безпеки, такі як Інфраструктура відкритих ключів (PKI) і протокол збирання об'єктів прав (ROAP), значно підвищили рівень захищеності цифрових контентів. PKI використовується для забезпечення безпеки підпису цифрових об'єктів та автентифікації користувачів, тоді як протокол ROAP дозволяє ефективно збирати та обробляти об'єкти прав, що забезпечує надійність та цілісність контенту. Однією з ключових переваг OMA DRM 2.0 є здатність використовувати ці технології для ефективного контролю за правами на контент, зберігаючи при цьому високий рівень безпеки використання цифрових об'єктів.

OMA DRM 2.1, представлена у 2009 році, впроваджує нові функції, включаючи вимірювання використання контенту, завантаження об'єктів прав та підтвердження їх встановлення. Серед інших нововведень слід зазначити введення Суб'єкта Контенту (СК), який відповідає за доставку захищеного контенту, та Суб'єкта Прав (СП), який відповідає за видачу об'єктів прав агенту DRM. Агент DRM контролює можливості користувачів щодо контенту, завантаженого з СП або СК, незважаючи на те, що користувач його контролює.

У сучасному світі DRM-платформи, інструменти та системи орієнтовані на швидкозростаючий відеоігровий ринок. З поширенням цифрового споживання медіаресурсів через стрімінгові сервіси, більшість компаній, що займаються DRM, звертають увагу на відеоігри та розробників програмного забезпечення. Геймінг на ПК часто стає жертвою піратства, тому впровадження DRM допомагає зменшити збитки. На сьогоднішній день все більше видавців вирішують створити власні "лаунчери" - програми, які надають доступ до ігор через власні магазини.

## 1.2 Боротьба з піратством у минулому: методи та засоби захисту відеоігор

У світі відеоігор існує довга історія боротьби з піратством. З моменту зародження ігрової індустрії виникали нові методи та технології, спрямовані на захист від несанкціонованого копіювання та поширення ігрових продуктів. Слід розглянути методи захисту від піратства, що застосовувалися у минулому, зокрема з кінця 1970-х до початку 2000-х років. Кожен з цих методів мав свої переваги та недоліки і відображав виклики та технічні можливості свого часу. Розглядаючи ці методи детальніше, можна краще розуміти історію боротьби з піратством у відеоігровій індустрії та їх вплив на сучасні DRM-технології.

У кінці 1970-х і на початку 1980-х років, персональні комп'ютери використовували перфокартки та касетні стрічки для зберігання та виконання програмного коду. Ці методи зберігання дозволяли легко створювати копії програм та розповсюджувати їх, оскільки не існувало ефективних технік захисту від несанкціонованого копіювання.

Копіювання програм і ігор було поширеним явищем у 1980-х роках. Однак, розробники вирішили впровадити методи захисту, щоб ускладнити це. Одним із таких методів був захист на основі диска. Це включало в себе маніпулювання даними на дискеті, щоб ускладнити їх копіювання. Наприклад, деякі програми форматували дискету у специфічному форматі, який був несумісний зі стандартними програмами копіювання, вимагаючи спеціальних інструментів для копіювання. Інші методи включали в себе додавання помилок до контрольних сум або приховування важливих даних в невикористаних секторах, ускладнюючи копіювання. Такі заходи допомагали значно ускладнити незаконне копіювання і розповсюдження програм та ігор у той час.

Методи захисту від копіювання, що базувалися на зовнішніх факторах, використовувалися у кінці 1980-х та на початку 1990-х років. Один із таких методів включав фізичний пристрій, званий кодовим колесом, який постачався разом з програмним забезпеченням. Під час установки програма запитувала від

користувачів конкретні коди з колеса, що робило копіювання без фізичного пристрою складним. Також використовувалися посібники з розблокованими кодами, які були необхідні під час установки для унеможливлення копіювання без посібника. Крім того, деяке програмне забезпечення мало в собі спеціальні програми захисту від копіювання, які перевіряли наявність оригінальних носіїв даних перед дозволом на установку.

У період з 1980-х по початок 1990-х років фізичні замки стали поширеним методом захисту від несанкціонованого доступу до рівнів в конкретних іграх. Ці заходи варіювалися від спеціально розфарбованих лінз для відстеження певних об'єктів до набору лінз з призмами, який отримав назву Lenslok.

Lenslok використовував лінзу з призмами для декодування двохлітерного коду, необхідного для завантаження програми. Однак основною проблемою цього методу було те, що лінзи не були відкалібровані для різних розмірів телевізорів, тому якщо екран був замалий чи зовеликий, зчитування коду ставало дуже складною задачею. Крім того, для кожної гри була індивідуальна лінза, і траплялись випадки, коли їх плутали на виробництві, через що доступ до гри був неможливий.

Додатково, існував метод захисту від копіювання за допомогою Dongles, які вимагали підключення до порту зв'язку на комп'ютері для виконання коду. Цей метод, в основному, використовувався з високоякісним програмним забезпеченням, хоча деякі відеоігри також використовували його.

Ідентифікаційні коди та буквено-цифрові ключі у 1990-ті роки стали найпопулярнішими способами захисту від копіювання відеоігор та комп'ютерних програм загалом. Під час установки користувачу треба було ввести унікальний серійний номер або код, що складався з букв і цифр. Кожен примірник відеоігри був прив'язаний до свого унікального коду або номера, який використовувався разом із перевіркою CD для запуску програми після встановлення.

Штучні файли, фальшиві таблиці змісту та надвеликі CD, метод був ефективним, але не на довго. Розробники ігор створювали штучні великі файли та таблиці змісту (TOC), щоб унеможливити запис на CD, і це працювало. Проте

з часом нові CD-приводи набули здатності бачити ці файли та обходити їх при записі, тому гра містилася на звичайний 600-Mб CD-ROM.

Історія SecuROM почалася у 1997 році, коли була заснована німецька компанія Sony DADC (Digital Audio Disc Corporation). SecuROM став однією з найпопулярніших систем захисту від копіювання у світі комп'ютерних ігор та програмного забезпечення. Він вперше з'явився на ринку у 1997 році і використовувався відтоді у багатьох виданнях ігор та програм.

Принцип роботи SecuROM полягав у тому, що він вбудовувався безпосередньо в програмне забезпечення або гру. Він захищав від несанкціонованого копіювання шляхом встановлення захищеної області на диску, шифрування файлів або застосування інших технічних методів. Під час установки програми або гри користувачеві часто потрібно було вводити унікальний серійний номер або активаційний ключ для отримання доступу до продукту.

Крім того, SecuROM також міг використовувати техніки антипіратства, такі як відстеження IP-адрес, обмеження кількості активацій та обмеження доступу до онлайн-серверів для тих, хто використовував неліцензійні копії.

Цей захист використовувався в багатьох відомих відеоіграх та програмах, включаючи такі блокбастери, як "Mass Effect", "Bioshock", "The Sims" та "Spore". Однак SecuROM був предметом критики з боку споживачів та геймерських спільнот за його негативний вплив на продуктивність, проблеми сумісності з певними конфігураціями апаратного забезпечення та проблеми з вилученням програмного забезпечення після видалення гри.

З часом SecuROM почав втрачати свою популярність, особливо з поширенням цифрових платформ і стрімінгових послуг, які пропонували більш зручні та користувачам доступні способи отримання відеоігор. Деякі випадки поганої роботи захисту та піратства також сприяли припиненню використання SecuROM компаніями-розробниками та видавцями програмного забезпечення. Наприкінці 2016 року Sony DADC офіційно припинила підтримку SecuROM, оголосивши про закриття цієї служби.

Хоча SecuROM відігравав важливу роль у захисті від несанкціонованого копіювання, він також викликав багато суперечок і протестів серед споживачів. Багато геймерів скаржилися на обмеження, які вводилися цим захистом, такі як обмеження на кількість активацій програми або неможливість грати без підключення до Інтернету. Деякі геймери також зазнали проблем зі сумісністю програми зі своїм апаратним забезпеченням або операційною системою, що призвело до виникнення труднощів у встановленні або запуску гри.

Крім того, в той час як SecuROM був спроектований для захисту від піратства та незаконного копіювання, деякі хакерські групи розробили засоби, які дозволяли обходити цей захист, створюючи "краки" або "патчі", які дозволяли гравцям використовувати неліцензійні копії гри. Це зробило SecuROM менш ефективним і згубним для бізнесу, оскільки він не завжди забезпечував запланований рівень захисту.

Незважаючи на це, SecuROM залишається важливим кроком у розвитку методів захисту від копіювання відеоігор та програмного забезпечення загалом. Його вплив на індустрію піратства та співвідношення між захистом та обхідними методами прослідковується в історії геймінгу і комп'ютерної індустрії.

SafeDisc був однією з провідних систем захисту від копіювання, використовуваних у комп'ютерних іграх і програмах з кінця 1990-х років до 2009 року. Розроблений компанією Macrovision, SafeDisc став популярним вибором для захисту CD-ROM і DVD-ROM від несанкційного копіювання та розповсюдження.

Принцип роботи SafeDisc полягав у створенні зашифрованої версії програми, яка була записана на диск разом із певними захисними механізмами. Ці механізми перешкоджали відтворенню або копіюванню диску за допомогою звичайних програм копіювання. Зазвичай це включало в себе створення певних секторів диска, які містили помилкові дані, а також застосування криптографічних методів захисту.

SafeDisc був широко використовуваний у відомих комп'ютерних іграх, таких як "The Sims", "Command & Conquer", "Half-Life" та інші. Протягом багатьох

років він вважався досить ефективним засобом захисту від копіювання, але з часом були розроблені методи обхідного захисту, які дозволяли обійти систему SafeDisc і копіювати захищені диски.

Одним з основних недоліків SafeDisc було те, що він створював певні технічні проблеми для користувачів. Наприклад, деякі програми для запису дисків або відтворення ігор несправно працювали з захищеними дисками, що викликало негативні реакції від користувачів. Крім того, обхідні методи, такі як використання спеціалізованих програм, дозволяли обійти захист і створити копію диска без проблем.

У 2009 році після ряду судових справ із-за обмежень SafeDisc, компанія Macrovision вирішила припинити підтримку та розвиток цієї системи захисту. Таким чином, SafeDisc припинив своє існування, а інші методи захисту, такі як SecuROM та інші, стали більш популярними серед розробників програмного забезпечення.

StarForce DRM був ще однією технологією захисту, що здобула популярність у 2000-х роках. Ця система вперше з'явилася в 1998 році і стала широко використовуватися різними видавництвами програмного забезпечення та розробниками відеоігор як засіб запобігання піратству.

Основна концепція StarForce DRM полягала у використанні спеціального захищеного прошарку на диску, який ускладнював або унеможлиблював копіювання або зміну даних. Цей захищений пласт містив криптографічні ключі та інші захисні механізми, що перешкоджали несанкціонованому доступу до вмісту.

Однією з особливостей StarForce DRM була його висока надійність. Система була досить ефективною у запобіганні несанкціонованому копіюванню, і її важко було обійти. Багато ігор і програм, захищених StarForce DRM, залишалися недоступними для копіювання або злому.

Проте StarForce DRM також мав свої недоліки. Більшість критиків StarForce DRM вказували на те, що ця технологія може призвести до проблем для користувачів, таких як зменшення продуктивності комп'ютера або несправності

оптичних приводів. Деякі користувачі також стикалися з проблемами в установці або запуску захищених ігор або програм.

Негативні відгуки і високі витрати на ліцензії для використання StarForce DRM сприяли зменшенню його популярності серед розробників програмного забезпечення. У результаті технологія почала втрачати свою значимість і застосування.

Насамкінець, у 2016 році компанія StarForce Technologies, розробник StarForce DRM, припинила оновлення та підтримку цієї технології. Це означало кінець ери StarForce DRM і перехід до інших, більш передових та ефективних методів захисту від піратства.

У минулому, захист відеоігор від піратства відбувався переважно шляхом використання фізичних обмежень та ідентифікаційних кодів. Перші спроби обмежити копіювання включали в себе різноманітні фізичні блокування, які змушували користувачів отримувати доступ до гри через спеціальні ключі чи пристрої. Пізніше, ідентифікаційні коди та буквено-цифрові ключі стали популярними, вимагаючи від користувачів введення унікальних серійних номерів або ключів під час установки гри. Ці методи забезпечували деякий рівень захисту, але з часом вони ставали менш ефективними через розвиток технологій копіювання.

### 1.3 Сучасні DRM системи в ігровій індустрії

У сучасному світі комп'ютерних ігор, захист від піратства став досить складною та актуальною, як ніколи раніше, проблемою. DRM-системи використовуються для захисту інтелектуальної власності та запобігання несанкціонованому копіюванню та розповсюдженню ігор. На сьогоднішній день серед найпоширеніших методів захисту від піратства в комп'ютерних іграх є використання ігрових лаунчерів та системи Denuvo. Ці технології спрямовані на

забезпечення безпеки інтелектуальної власності, контроль над доступом до ігор та обмеження несанкціонованого використання. Ігровий лаунчер - це програма для керування та запуску комп'ютерних ігор, що також може виконувати функції спільноти та забезпечувати безпеку через захисні механізми, такі як DRM.

Створений у 2003 році компанією Valve Corporation, Steam спочатку функціонував як платформа для оновлень ігор, які розроблялись самою Valve. Проте згодом він перетворився на повноцінний цифровий магазин ігор, де можна купувати, завантажувати та грати у ігри, які не обов'язково були розроблені Valve.

Одним із найважливіших аспектів Steam є його захист від несанкціонованого використання та копіювання ігор. Для цього платформа використовує кілька методів захисту, що надаються розробникам ігор.

Перший метод захисту полягає в використанні Steamworks API, який інтегрується безпосередньо в код гри та дозволяє перевіряти, чи має користувач ліцензію на запуск гри, інтегруючись з ігровим процесом. Це забезпечує, що гра може бути запущена тільки на акаунті, на якому вона була куплена, та що користувач має відповідні права.

Другий метод - Steam Bind може використовуватись якщо, з якоїсь причини, перший спосіб не підходить. Він дозволяє захистити існуючі файли гри шляхом їх шифрування та перевірки цілісності. Це робить гру менш вразливою до несанкціонованого доступу та модифікацій.

Третій метод - Steam Custom Executable Generation - полягає в створенні персоналізованих виконуваних файлів для кожного користувача. Це може включати в себе індивідуальні налаштування та ключі шифрування, що робить кожен копію гри унікальною та важкою до злому.

Крім того, Steam дозволяє використовувати сторонні системи DRM, які надають додатковий захист ігор від піратства та незаконного розповсюдження.

Кожен з цих методів має свої переваги та недоліки, і вибір конкретного методу захисту може залежати від різних чинників, таких як фінансові можливості розробника, рівень захисту, потреби користувачів тощо. Наприклад, Steamworks API може бути більш зручним для розробників, які вже

використовують Steam для розповсюдження своїх ігор, оскільки він інтегрується безпосередньо з платформою Steam і забезпечує легкий доступ до функцій захисту.

Загалом, захист від піратства є важливим аспектом цифрового розповсюдження ігор, і Steam продовжує вдосконалювати свої методи захисту, щоб забезпечити максимальний рівень безпеки для розробників та користувачів.

Origin - це цифрова платформа, розроблена компанією Electronic Arts (EA), що дозволяє користувачам придбавати та завантажувати комп'ютерні ігри через Інтернет. Запущений початково як EA Store, цей сервіс був перейменований на Origin 3 червня 2011 року. Створений як конкурент Steam, Origin швидко розвинувся від платформи для покупки ігор до повноцінної екосистеми, що включає в себе соціальні функції, управління профілем і інтеграцію з іншими платформами, такими як Facebook, Xbox Live і PlayStation Network.

Щодо захисту ігор, Origin використовує кілька методів. По-перше, він використовує власне API від EA, яке дозволяє розробникам перевіряти легальність доступу до гри через обліковий запис Origin. Крім цього, Origin застосовує методи шифрування та захисту файлів гри, щоб ускладнити процес несанкціонованого копіювання або внесення змін у програмний код. Варто також відзначити, що ігри видавництва EA запускаються тільки через лаунчер Origin, незалежно від того, в якому магазині була куплена гра.

У 2022 році компанія EA припинила підтримку Origin і замінила його новим додатком - EA app.

ZLOEmu - це альтернативний сервер для багатьох ігор, розроблений для обходу офіційних серверів Electronic Arts (EA). Цей проект був створений ентузіастами з метою створення можливості для гри в ігри від EA без необхідності користуватися офіційними серверами.

Історія ZLOEmu почалася у середині 2010-х років, коли група розробників почала досліджувати можливості створення альтернативних серверів для гри в ігри від EA. У 2013 році вони вперше випустили свій власний сервер для гри в

гру Battlefield 3, який став популярним серед гравців, які шукали альтернативу офіційним серверам EA.

Принцип дії ZLOEmu полягає у створенні альтернативних серверів, які сприяють підключенню гравців до гри в ігри від EA, обходячи офіційні сервери. Головна перевага цього проекту полягає в тому, що він надає можливість грати в ігри без необхідності придбання ліцензійних копій ігор від EA або підписки на їх сервіси. Однак варто зазначити, що використання ZLOEmu може супроводжуватися ризиком порушення ліцензійних угод або правил використання певних ігор.

Загалом, ZLOEmu став спільнотою гравців, яка шукає альтернативні шляхи для гри в ігри від EA та інших великих видавців і розробників, які встановлюють обмеження на доступ до своїх офіційних серверів.

Uplay - це лаунчер від Ubisoft, який з'явився разом з виходом гри Assassin's Creed II у листопаді 2009 року. Але сам клієнт Uplay був випущений лише у липні 2012 року. Цей лаунчер дозволяє користувачам купувати та запускати ігри. Для його використання необхідно мати обліковий запис Uplay, який може використовуватися на різних платформах та для доступу до інших сервісів Ubisoft.

У більшість ігор Ubisoft, доступних через платформу Uplay, вбудований спеціальний механізм DRM, який контролює легальність використання гри. Спочатку Uplay вимагав постійного підключення до Інтернету для гри, але цей підхід був критикований через обмеження, які він насував на гравців. Пізніше Uplay перейшов до одноразової перевірки під час запуску гри, що дозволило гравцям грати в ігри без постійного Інтернет-з'єднання. Однак, окремі ігри вимагають активне Інтернет-з'єднання для доступу до мережевого контенту або багатокористувацької гри.

Для захисту від несанкціонованого копіювання та перепродажі дисків, деякі ігри Ubisoft також використовують одноразові мережеві абонементи, відомі як "Uplay Passport", які надають доступ до мережевих функцій та додаткового контенту. Проте, після численних скарг гравців та критики, у жовтні 2013 року

Ubisoft вирішила припинити використання цих абонементів для майбутніх ігор, надавши безкоштовний "Uplay Passport" для Assassin's Creed IV: Black Flag, який з початку йшов з платним одноразовим "Uplay Passport".

З 29 жовтня 2020 року сервіси Uplay і Ubisoft Club об'єдналися в Ubisoft Connect. Тут була впроваджена нова система лояльності, де гравці можуть підвищувати рівень облікового запису та отримувати бали Units за виконання різних завдань. Ці бали можна витратити на покупку внутрішньоігрових предметів. Також введено збереження прогресу на всіх пристроях, на яких користувач входить в Ubisoft Connect.

Epic Games Launcher від Epic Games — це цифрова дистрибуційна платформа, розроблена компанією Epic Games, яка дозволяє користувачам придбати та грати в комп'ютерні ігри. Платформа була вперше анонсована у грудні 2018 року. Історія Epic Games Launcher почалася з випуску гри Fortnite, яка стала великим успіхом для компанії Epic Games. Завдяки популярності Fortnite, платформа отримала значний приріст користувачів, а також велику увагу гравців та розробників.

Epic Games дозволяє розробникам використовувати будь-яку DRM-систему, яка є зручною для них. Це означає, що розробники можуть обирати між різними методами захисту, включаючи власні системи або сторонні рішення, такі як Denuvo або Easy Anti-Cheat. Такий підхід дає розробникам більшу свободу в обранні стратегії захисту своїх ігор.

Denuvo — це програмне забезпечення для управління цифровими правами та захисту від несанкціонованого доступу, розроблене компанією Denuvo Technologies GmbH, що виникла після придбання Sony DADC, філії Sony, яка працювала над технологією DRM SecuROM.

Першу реалізацію Denuvo було впроваджено з грою від EA - FIFA 15, у вересні 2014 року. Громада "кракерів" була здивована, не помітивши злomu протягом перших 30 днів після випуску гри.

Перша успішна спроба злому Denuvo відбулася в грудні 2014 року, коли китайська група 3DM випустила робочий крак для гри Dragon Age: Inquisition від EA. Однак версія гри від 3DM була нестабільною та повна помилок.

У 2016 році болгарський зломщик під псевдонімом Voksi зміг обійти автентифікацію для декількох ігор, використовуючи вразливість, виявлену в демо-версії гри Bethesda DOOM, що використовувала Denuvo.

Після цього відкриття Denuvo почала працювати над новою версією свого програмного забезпечення для захисту від втручання. Однак групи, які створюють краки, тримали темп, і час між випуском гри з використанням Denuvo та її подальшим зламанням релізом продовжував скорочуватися, іноді досягаючи 30-денного вікна продажів, а в окремих випадках - навіть нульової дати, що означає, що захист гри був обійдений в ті ж дні, що і день випуску.

У серпні 2015 року компанією Denuvo Technologies GmbH було подано заявку на патент, яка описує процес і застосування техніки для забезпечення номінального потоку виконуваного файлу. Цей патент описує метод, в якому номінальні константи використовуються для перетворення та розшифрування частин виконуваного файлу. Використовується алгоритм, який використовує ці номінальні константи. У патенті, як приклад, показано використання номінальної константи, відомої як  $\Pi$  (3,1415), яка потрібна для обчислення об'єму циліндра. Цю номінальну константу отримують за допомогою серії обчислень, які базуються на хеш-значеннях інформації про апаратне забезпечення, що збирається з клієнтської машини. Тобто, система, яка складається з клієнта, сервера та захисного двигуна, використовується для отримання інформації про апаратне забезпечення та їх шифрування за допомогою хеш-значень. Якщо ці хеш-значення обчислюються випадковим чином, вони можуть створити точну номінальну константу, яка використовується для забезпечення номінального потоку, що підтверджує відповідність виконуваного файлу. Цей процес може бути запущений під час робочого часу або під час отримання клієнтом інформації від сервера для цілей автентифікації. У патенті також згадується використання

цієї техніки в середовищі DRM як спосіб захисту виконуваних файлів від несанкціонованого запуску.

Ще один метод, який використовує Denuvo для захисту від копіювання, - це внутрішні події гри.

У 2017 році групування Codex випустила зламану версію файтингу Injustice 2: Legendary Edition. У цьому виданні група розкрила, як Denuvo використовує внутрішні події гри для захисту від копіювання.

У зазначеному прикладі групою вказано, що коли персонаж Робін виконує в грі певну дію, таку як "кидання димової бомби на землю", Denuvo розпочинає процес запису приватного ключа в пам'ять з адреси пам'яті 000000014C113692 створюючи виклик пам'яті (рис. 1.1)

|                  |                      |                           |
|------------------|----------------------|---------------------------|
| 000000014C113692 | 44 88 07             | mov byte ptr ds:[rdi],r8b |
| 000000014C113695 | 5F                   | pop rdi                   |
| 000000014C113696 | 50                   | push rax                  |
| 000000014C113697 | 21 C0                | and eax,eax               |
| 000000014C113699 | 9C                   | pushfq                    |
| 000000014C11369A | 44 01 C1             | add ecx,r8d               |
| 000000014C11369D | 4C 89 F0             | mov rax,r14               |
| 000000014C1136A0 | 48 89 C1             | mov rcx,rax               |
| 000000014C1136A3 | 48 C7 C0 00 00 00 00 | mov rax,0                 |
| 000000014C1136AA | 48 09 D0             | or rax,rdx                |
| 000000014C1136AD | 48 83 C1 01          | add rcx,1                 |
| 000000014C1136B1 | 49 89 CE             | mov r14,rcx               |
| 000000014C1136B4 | C1 C1 08             | rol ecx,8                 |
| 000000014C1136B7 | 9D                   | popfq                     |
| 000000014C1136B8 | 58                   | pop rax                   |

Рисунок 1.1– Виклик пам'яті створений записом ключа

Виклик пам'яті, згенерований внутрішньою подією гри: для запису приватного ключа змінні пересилаються з реєстру r8b, додаються до значень у реєстрі r8d та переміщуються в реєстр r14, де чекають на виконання.

Після завершення цього виклику пам'яті Denuvo заповнює буфер за адресою 000000014779F593. Після того, як буфер буде заповнений та приватний ключ з сервера Denuvo буде отриманий, виконуються функції протидії втручанням з адреси пам'яті 000000014774C37E, що породжує відповідь пам'яті (рис 1.2).

|                  |                      |                                  |
|------------------|----------------------|----------------------------------|
| 000000014774C37E | 41 89 7D 00          | mov dword ptr ds:[r13],edi       |
| 000000014774C382 | 48 29 F3             | sub rbx,rsi                      |
| 000000014774C385 | 41 54                | push r12                         |
| 000000014774C387 | C1 CB 0D             | ror ebx,D                        |
| 000000014774C38A | BE D4 72 4D 3E       | mov esi,3E4D72D4                 |
| 000000014774C38F | 4C 8D 25 4F B5 06 FE | lea r12,qword ptr ds:[1457B78E5] |
| 000000014774C396 | 4C 33 24 24          | xor r12,qword ptr ss:[rsp]       |
| 000000014774C39A | 48 8B 1C 24          | mov rbx,qword ptr ss:[rsp]       |
| 000000014774C39E | 4C 21 E3             | and rbx,r12                      |
| 000000014774C3A1 | 4C 09 24 24          | or qword ptr ss:[rsp],r12        |
| 000000014774C3A5 | 0F BA F8 06          | btc eax,6                        |
| 000000014774C3A9 | 0F BA F6 0D          | btr esi,D                        |
| 000000014774C3AD | 48 29 1C 24          | sub qword ptr ss:[rsp],rbx       |
| 000000014774C3B1 | 4C 89 E3             | mov rbx,r12                      |
| 000000014774C3B4 | 48 23 1C 24          | and rbx,qword ptr ss:[rsp]       |
| 000000014774C3B8 | 4C 0B 24 24          | or r12,qword ptr ss:[rsp]        |
| 000000014774C3BC | 49 29 DC             | sub r12,rbx                      |
| 000000014774C3BF | C3                   | ret                              |

Рисунок 1.2– Відповідь пам'яті на функції протидії втручання

Відповідь пам'яті, створена Denuvo: після отримання приватного ключа з серверів Denuvo, приватний ключ, що був обчислений у попередньому виклику пам'яті, вилучається з реєстру r12 і порівнюється з приватним ключем сервера Denuvo.

Ця відповідь використовується Denuvo для перезапису будь-яких патчів, які раніше були застосовані до цих адрес за допомогою функцій, витягнутих з реєстра, викликаного кодом Denuvo; в цьому випадку реєстр відомий як r13.

Те, що розкрив Codex у цьому описі, полягає в тому, що їх крак читає велику кількість зашифрованого коду і вносить патчі до викликів, таким чином обходячи систему затемнення Denuvo. Група також заявила, що цей конкретний процес призводить до мікрозависань і статтерів, оскільки процес сильно залежить від центрального процесора (ЦП), що призводить до підвищеного використання ЦП, у деяких випадках понад 99%, що відповідає за статтери.

## 2 АТАКИ НА СИСТЕМИ DRM У ВІДЕОІГРОВІЙ ІНДУСТРІЇ

### 2.1 Фактори та мотивації злому відеоігор

Відеоігрова індустрія зараз є однією з найприбутковіших сфер розваг і не планує збавляти оберти. Аналітики прогнозують лише ріст цього сектору. У 2023 році капіталізація відеоігор досягла вражаючої суми в 187,7 мільярдів доларів(рис 2.1).

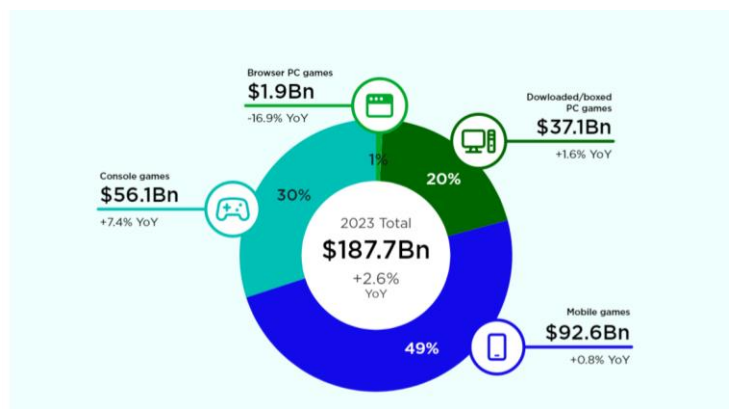


Рисунок 2.1– Капіталізація секторів відеоігрової індустрії за 2023 рік

Порівняно з іншими галузями розваг, такими як музична індустрія та кінотеатри, цифри вражають: капіталізація музичної індустрії склала 28,6 мільярдів, тоді як загальні збори у кінотеатрах становили 33,9 мільярдів.



Рисунок 2.2– Порівняння капіталізації найпопулярніших сфер розваг за 2023 рік

За даними на кінець 2023 року, загальна аудиторія геймерів перевищила 3 мільярди людей по всьому світу.

2023 Global players  
Per region

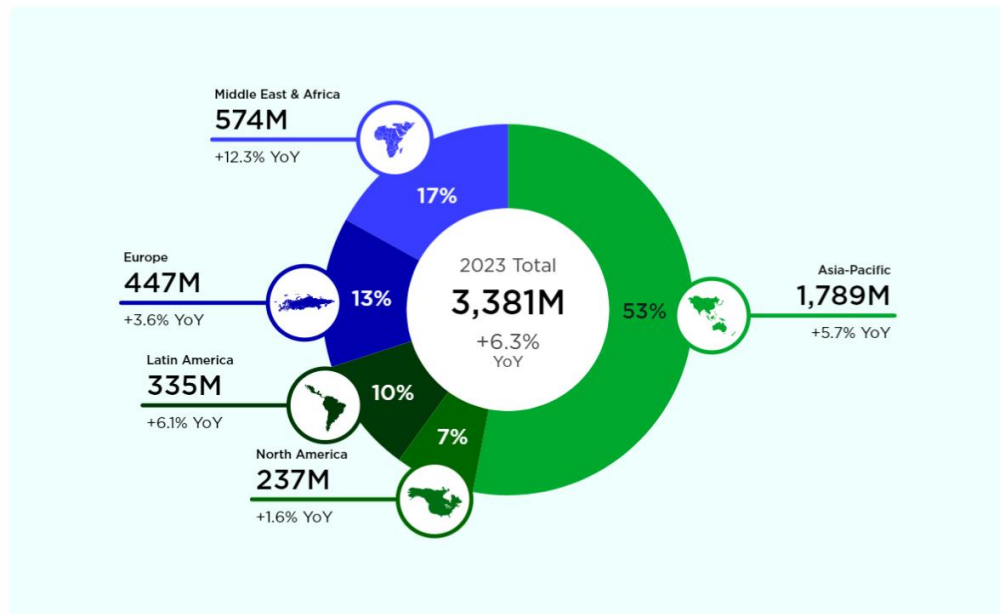


Рисунок 2.3– Кількість геймерів на різних континентах на кінець 2023 року

Незважаючи на такий вражаючий успіх, відеоігрова індустрія стикається з серйозними викликами, одним із яких є піратство. Найбільш уразливими до цього явища є комп'ютерні ігри, які стають об'єктом злому. Хакери та зловмисники шукають слабкі місця у системах захисту, щоб отримати несанкціонований доступ до вмісту ігор. Причини цього можуть бути різноманітні: від бажання випробувати нові ігри безкоштовно до встановлення рекордів у світі злому, де хакери змагаються між собою за титул кращого зломщика. Такі атаки піддають ризику не лише фінансовий успіх розробників, а й інтелектуальну власність, безпеку користувачів та стабільність галузі в цілому.

У світі відеоігор проблеми з авторськими правами часто призводять до видалення ігор з продажу. Наприклад, у випадку оригінальної гри "Мафія" спочатку її зняли з продажу на платформі GOG, а потім знову ввели, але вже у вигляді обмеженої версії. Також, у "Grand Theft Auto 4" оригінальний плейлист

радіостанції Владивосток ФМ доступний лише у піратських версіях гри, оскільки закінчилися договори з музичними виконавцями, такими як "Глюк'Оза" та група "Кіно".

Пірати також активно боролися з відключенням багатокористувацьких тайтлів від серверів. У прикладі гри "World of Warcraft" багато гравців виявили незадоволення оновленнями, які вводила компанія Blizzard Entertainment. Замість того, щоб приймати ці зміни, вони шукали можливість грати у версію гри, яка існувала на початку, так званий ванільний варіант. Це призвело до того, що вони зверталися до неофіційних серверів. Blizzard активно боролася з цим явищем, у 2016 році за вимогою компанії було відключено сервер з понад 150 тисячами активними акаунтами. Незважаючи на це, попит на ванільну версію гри був значним, і це надихнуло Blizzard на випуск спеціальної версії гри "WoW Classic". Це рішення відображає реальний попит на такий тип гри, який став очевидним завдяки популярності неофіційних серверів.

87% ігрових тайтлів, випущених до 2010 року, неможливо отримати легальними шляхами, наприклад, гра "NFS Most Wanted" 2005 року випуску недоступна для придбання в магазинах та платформах, окрім піратських сайтів. Крім того, у магазині Steam продається недороблена версія гри "Vampire: The Masquerade - Bloodlines", де присутні баги і незавершений контент. Протягом 20 років фанати цієї гри активно працювали над її поліпшенням, відновили вирізаний контент, виправили помилки і оптимізували її під сучасні системи і виправлена версія є тільки на піратських сайтах. У деяких регіонах недоступні ігри або їх локалізація, що також спонукає користувачів до пошуку альтернативних шляхів доступу до контенту. Використання системи захисту, такої як Denuvo, може суттєво знижувати продуктивність системи, особливо на момент релізу, що стає однією з причин, чому деякі гравці шукають нелегальні копії ігор.

## 2.2 Типи та організаційна структура груп, які займаються зломом відеоігор

Розглядаючи типи та організаційну структуру груп, що займаються зломом відеоігор, стає очевидним, що це феномен відображає складність сучасної кібербезпеки. Деякі видавці, зіткнувшись з високим рівнем піратства на ринку ПК, відмовляються виходити на нього, а ті, хто все ж ризикують, намагаються мінімізувати цей ризик, встановлюючи подвійні DRM системи.

Пірати модифікують файли DRM систем, які перевіряють легітимність гри та блокують незаконне копіювання. Протидіяти цьому покликані технології захисту від несанкціонованого злomu, такі як Denuvo, яка є однією з найпоширеніших сучасних DRM систем. Проте, навіть такі складні системи, як Denuvo, можуть бути зламані. DRM можна також обійти, використовуючи модифіковані файли (краки), які замінюють або доповнюють оригінальні файли гри, дозволяючи запускати її без перевірки легітимності.

Піратські групи поділені за ролями у виготовленні та розповсюдженні краків.

Представниками Warez scene є такі відомі групи, як Codex, Conspiracy, Steampunks, Reloaded, Fairlight.

Варез (англ. warez — сленгова версія «wares», скорочення від «software» — «програмне забезпечення») — це комерційні програми, які поширюються безкоштовно (рідше — на носіях за символічну плату) незаконним шляхом без дозволу автора. Варез обов'язково містить зміни і/або доповнення, що дозволяють використовувати його безкоштовно.

The Warez scene, часто згадується як The Scene, — це всесвітня підпільна організована мережа піратських груп, що спеціалізується на отриманні та незаконному розповсюдженні цифрових медіа безкоштовно до їх офіційної дати продажу. The Scene розповсюджує всі форми цифрових медіа, включаючи комп'ютерні ігри, фільми, телевізійні шоу, музику. The Scene повинна залишатися прихованою від публіки, і її матеріали поширюються лише серед членів

спільноти. Однак, оскільки файли часто витікають за межі спільноти і стають популярними, деякі індивідууми з The Scene починають завантажувати їх на файлохости, торренти.

Відомі своєю послідовністю, надійними та безпечними краками, ці групи дотримуються встановлених стандартів. Вони обмежені методами злому, щоб переконатися, що краки працюватимуть на будь-якій конфігурації ПК.

На початку 2021 року було введено новий набір правил для комп'ютерних ігор. Гра має бути створена у файлі ISO для Microsoft Windows, хоча релізи для інших операційних систем можуть використовувати формат Apple .dmg або інші образи дисків. Групі, яка першою випускає злом, надається обмежене за часом ексклюзивне право на оновлення гри. Це право триває 60 днів, протягом яких група може випускати оновлення на свій розсуд.

Після цього терміну інші групи можуть випускати свої версії оновлень. Великою популярністю користуються так звані "репаки" — перепакзовані версії ігор з меншим об'ємом, що дозволяє економити пропускну здатність. Одним із провідних імен у цій ніші є FitGirl, яка часто використовує релізи сцени для створення оптимізованих версій.

Ця структура дозволяє групам ефективно координувати свої зусилля та забезпечувати високий рівень якості та стабільності краків, що робить їх популярними серед користувачів.

У разі використання забороненого методу, крак стає "nuked". У вarez-сцені nuke означає позначити вміст як "поганий" з причин, які можуть включати непридатне програмне забезпечення, погану аудіовізуальну якість, заражений вірусами вміст, оманливо позначений (фальшивий) вміст або недотримання правил. Дублікати та вкрадені релізи інших піратів, які не вказують на оригінальних піратів, також будуть "nuked". Коли реліз сцени "nuked", до його списку додається повідомлення, яке інформує інших учасників про його статус та конкретний характер проблеми.

Заборонено робити мультиплеєрні краки. Якщо повідомляється, що крак погано працює на деяких системах, то крак "nuked" творцями або іншими

групами. Після цього зазвичай випускається правильний крак, який виправляє неполадки.

Після релізу крака його завантажують на підпільні топсайти, після чого він витікає у приватні та загальнодоступні трекери. Topsite — це термін, який використовується на вarez-сцені для позначення підпільних, дуже секретних, високошвидкісних FTP-серверів, які використовуються "реліз групами" і кур'єрами для розповсюдження, зберігання та архівування релізів вarezів. Топсайти мають дуже високу пропускну здатність підключення до Інтернету, зазвичай підтримуючи швидкість передачі від сотень до тисяч мегабіт на секунду; достатньо, щоб передати повний диск Blu-ray за секунди. Топсайти також мають дуже велику ємність для зберігання. На початку через ці сайти Warez переважно розповсюджували програмне забезпечення, таке як ігри та програми, після того як реліз групи зняли будь-який захист. Тепер вони також є джерелом інших захищених авторським правом творів, таких як фільми та музика. Сайтам суворо заборонено стягувати плату за доступ до вмісту через низьку безпеку, а сайти, які це роблять, уникаються спільнотою топсайтів.

У релізі знаходяться крак-файли та установник гри з ISO файлом. ISO файл може по-різному бути встановлений, як зручніше користувачу, після чого залишається встановити гру і скопіювати крак в папку з грою. Завдяки простоті та надійності використання Warez scene групи є наріжним каменем ігрового піратства і є об'єктом незліченних рейдів правоохоронних органів по всьому світу. Сцен-групи є вкрай конфіденційними і не дають інтерв'ю. Натомість вони прикріплюють NFO-інструкції до крака. Ці NFO відрізняються своїми ASCII малюнками.



Рисунок 2.1— NFO файл до злому Conspiracy гри «Sonic Forces»

Сцен-групи не мають сайтів та не шукають вигоди, навпаки, вони рідко можуть заробити хоч якусь копійку. Вони займаються цим на ентузіазмі, змагаючись з іншими угрупованнями, що пояснює швидкість та якість Сцени.

Peer to Peer (P2P) - це широке поняття, що охоплює усі угруповання, відмінні від сцен. Найбільш відомі серед них - 3DM, Revolt. P2P виконують різноманітні завдання, від поширення краків сцен до самостійного злому. Вони не обмежені стандартами сцен та можуть використовувати різні методи. Наприклад, хакер

Voksi з групи Revolt використовував драйвер ядра (Kernel driver), щоб обійти захист Denuvo, що заборонено за стандартами сцен. Завдяки різноманітному інструментарію P2P можуть швидше випускати краки, ніж сцени. Проте якість таких краків залишає бажати кращого, вони далеко не такі якісні, як ті, що представлені сценами. Перший крак Denuvo був створений P2P групою 3DM і містив багато помилок та нестабільностей. P2P також можуть вирішувати проблему мультиплеєра. Наприклад, FiveM зламала онлайн версію GTA5, а 4 delta 1 зламала Call of Duty Modern Warfare 2 та 3. P2P не такі закриті, як сцени, деякі хакери спілкуються з пресою та піратською спільнотою, учасники групи 3DM взагалі мають особисті профілі з їх справжніми фотографіями та іменами. Іноді учасники P2P влаштовують збори пожертв. P2P зайняли свою нішу, з ранніми, але дуже не стабільними краками, з доступом до мультиплеєра.

Репакери - остання та найраціональніша категорія серед піратських угруповань. Відмінною рисою репакерів є те, що вони не займаються безпосереднім зломом ігор. Натомість, їх діяльність полягає у стисненні релізів сцен і P2P до менших розмірів. Після цього стислі файли поміщаються у набори з індивідуальним інсталятором і поширюються як репаки.

Репакери також поділяють файли за мовами, що дозволяє користувачам завантажувати лише потрібні мовні пакети. Це значно економить місце на диску та час завантаження. Такий метод користується популярністю серед піратів, які мають обмежене сховище або повільний інтернет. Репаки жертвують часом встановлення гри заради швидкості завантаження та меншого обсягу файлів.

Репакери активно намагаються монетизувати свою діяльність через збори пожертвувань, розміщення реклами на своїх сайтах та вбудовування майнерів у свої файли. Завантаження репаку несе великий ризик. Відомі випадки, коли репаки містили віруси та майнери. Наприклад, репакер SATA впровадив майнер у свої репаки для Just Cause 3 та Rise of the Tomb Raider, що призвело до зараження систем користувачів вірусами-хробаками та іншими шкідливими програмами. Пізніше SATA визнав свою провину та вибачився.

Найбезпечніший метод отримання ігор - це офіційне придбання, що гарантує відсутність шкідливих програм і вірусів.

### 2.3 Реакція розробників після злomu гри: усунення чи збереження Denuvo

Denuvo – це назва, яку багато хто знає і багато хто зневажає. Ця система DRM звинувачувалася у зменшенні продуктивності та збільшенні часу завантаження. Її критикують як гравці, так і ті, хто зламує ігри, і навіть розробники самих ігор. Тому не дивно, що гравці миттєво звертаються до розробників з проханням прибрати Denuvo, як тільки гра була зламана. Проте кількість розробників, які прислухалися до таких прохань, невелика. Прикладами можуть бути DOOM, INSIDE та RiME.

Є три основні причини, чому розробники не видаляють Denuvo зі своїх ігор після їх злomu:

- Надійність крака.
- Надійність кракнутої версії.
- Майбутній завантажуваний контент (DLC)

Однією з головних причин, чому розробники залишають Denuvo в своїх іграх після їх злomu, є ненадійність краку. Навіть якщо на початку все здається стабільним і безпроблемним, можуть виникнути серйозні проблеми пізніше.

Наприклад, при зламі гри Immortals Fenix Rising від Empress, спочатку крак працював без нарікань. Проте незабаром пірати почали зіткнутися зі значною нестабільністю гри: вона випадала при різних сценаріях. Хоча Empress випустила два виправлення, це не врятувало ситуацію. Крак відмовлявся працювати після певної дати, і гравцям доводилося змінювати системний годинник, щоб продовжити грати, наслідками такого було безліч незручностей у простому користуванні браузером.

Такі проблеми можуть значно знизити задоволення від гри та підштовхнути гравців до придбання легальної ліцензії. Ні зломщики, ні розробники не можуть стверджувати, що крак працюватиме завжди. Ця ситуація показує, що навіть стабільний крак може стати ненадійним у майбутньому, що стає чинником для збереження Denuvo в грі.

Видалення захисту Denuvo з ігор завжди супроводжується випуском оновленого крака, і це призводить до ряду факторів, які зумовлюють відмову розробників від його видалення. Навіть якщо крак ідеальний, він може бути стабільним на стільки на скільки версія гри яку він зламує. Розробники продовжують працювати над вдосконаленням гри та випускати оновлення, які підвищують стабільність та надають кращі враження гравцям, які придбали ліцензійну версію гри. Ці оновлення зазвичай включають нові версії захисту Denuvo, що унеможлиблює використання старих краків для оновлених ігрових файлів.

Випуск нових версій гри з новими захистами Denuvo призводить до необхідності злому гри знову, як гра, яку ще не зламували, поки не буде стабільного крака стабільної версії гри, пірати завжди будуть мати жахливий досвід гри.

Але навіть якщо у піратів все добре працює, розробники мають третю причину залишити Denuvo - майбутні DLC. Наприклад, варто згадати Anno 1800, одну з найбільших ігор, захищених Denuvo. Після того, як Empress зломала гру, Ubisoft не поспішала прибирати захист, оскільки планувалося випустити кілька значних оновлень та DLC. Ці додатки були випущені разом з оновленим захистом Denuvo, унеможливлюючи їх злом з релізом Empress. Це означає, що групам зломщиків доводиться чекати, поки розробники випустять весь запланований контент, щоб зламати його одним кроком.

Якщо у оновлення немає захисту, то всі оновлення будуть миттєво зламані, начебто гра ніколи не використовувала денуво і пірати матимуть доступ до контенту в той же час, що і ті хто купив гру

Регулярні оновлення показують групам зломщиків, що не варто витрачати час на злом Denuvo, оскільки нове оновлення може вийти в будь-який момент. Якщо нове оновлення не містить захисту, всі оновлення будуть миттєво зламані, начебто гра ніколи не використовувала Denuvo, даруючи піратам доступ до контенту разом з офіційними користувачами. Це стимулює компанії, такі як Ubisoft, прагнути забезпечити привілей доступу до нового контенту для легальних покупців.

Чи є вигода для корпорацій прибирати Denuvo після злому гри? Це залежить від конкретної ситуації та часу, оскільки головною метою компаній є здобуток прибутку. Тому вони можуть вирішити залишити захист або прибрати його залежно від обставин та стратегії розвитку.

Скільки сплачують за Denuvo захист? У зливі в 2020 році договір між Denuvo та Crytek вказує, що для захисту Crysis Remastered заплатили 126 000 євро, і це з урахуванням знижки за те, що випустили гру до 31 березня 2021 року. Якби Crytek випустили гру після цієї дати, то довелося б платити 60 000 євро захисту від злому і 80 000 євро за унікальне шифрування даних, у сумі 140 000 за 12 місяців захисту. Замість оплати Denuvo, ці 126 000 євро можна було б пустити на розробку мультиплеєра в ремастері Crysis. Мультиплеєр складніше зламати, мультиплеєрних краків значно менше ніж краків Denuvo для ігор, які не використовують Steamworks для з'єднання гравців, якого не було в Crysis, оскільки Crysis Remastered був ексклюзивом Epic Store. Говорячи більше про мультиплеєр це функція, яка принесе істотну відмінність і перевагу для тих хто гру купив, але Crytek вирішила інакше. Також, якщо протягом 30 днів з моменту виходу гри вперше активується понад 500 000 копій, Denuvo стягує одноразовий збір у розмірі 60 000 євро.

Денуво надає безліч послуг для розробників, але найпомітніша з них - використання в попередній версії, бета-версії, демо-версії, роздрібній версії, а також включених до неї виправленнях. Це стосувалося і оновлення, яке виправило і завершило Crysis Remastered через кілька тижнів після того, як стара версія була зламана. Crytek вже сплатила захист цих оновлень, що не давало піратам дістатися гри протягом місяців. Чи є якісь причини видаляти Denuvo за такого розкладу справ? Ні! Проте через рік Crytek прибрала Denuvo, коли

випускала гру в Steam. Цьому є пояснення, як пишеться в злитому документі: "Якщо Ліцензіат бажає продовжити захист від несанкціонованого доступу через дванадцять (12) місяців, рахуючи з дати виходу гри, Ліцензіат повинен направити відповідне попереднє письмове повідомлення. Додаткова Плата за захист від несанкціонованого втручання за кожний місяць після дванадцяти (12) місяців, рахуючи з дати укладання права власності, становить дві тисячі євро (2 000 євро)."

Злитий контракт містить ідентичні умови для використання Denuvo у Crysis 2 Remastered, відмінність тільки в тому, що денуво зменшила плату до 112000 євро.

Щомісячна плата через 12 місяців є причиною чому розробники прибирають денуво зі своїх старих проектів.

Декілька розробників, які прибрали Denuvo. DOOM вилучили Denuvo у грудні 2016 року, приблизно через 4 місяці після краха від Conspiracy. Користувач Reddit, який стверджує, що є розробником ігор, заявив, що Denuvo має політику повернення коштів, якщо гра була зламана протягом певного періоду часу (приблизно 3 місяці). Проте Denuvo спростовує ці заяви, стверджуючи, що немає жодних угод, що передбачають повернення коштів у таких випадках, що підтверджується в злитих контрактах з Crytek. Сам Denuvo заявляє, що захист у DOOM був видалений, оскільки DRM виконав своє завдання і захистив гру під час вікна початкових продажів. Крім цього, може бути ще одна причина для вилучення DRM: для DOOM не випускали жодного DLC для одиночної гри, де Denuvo могла б проявити себе, всі DLC для DOOM були виключно мультиплеєрними, тому не потребували захисту від Denuvo, тому у DOOM не було жодної причини залишати Denuvo після злому гри. Вилучення Denuvo було вигідним для гри, оскільки тепер в неї могли грати люди, які не хотіли грати в ігри з Denuvo з принципу. Це стосується практично всіх ігор, з яких видалили Denuvo. Вони роблять це або після того, як всі DLC для одиночної гри були зламані, або коли такі DLC не планувалися спочатку.

Але є пара винятків, таких як Homefront: The Revolution, яка видалила Denuvo раніше, ніж гра була зламана, що призвело до практично миттєвого злому. Те саме стосується Titanfall 2, яку зламали тільки після видалення Denuvo, але

мультиплеєр все ще залишався не зламаним, що змушувало людей купувати гру, оскільки вона на 90% базується на боях проти інших гравців.

Інші ігри, які прибдали Denuvo перед зламанням або під час підготовки до випуску нових DLC та оновлень:

- Life is Strange. Розробники прибдали захист Denuvo з першого епізоду перед виходом наступних частин. Це призвело до злomu всіх епізодів, причина точно невідома.

- Hitman. Denuvo був видалений через проблеми з продуктивністю гри. Розробники заявили, що їхня першочергова мета - забезпечити найкращий досвід для гравців, і Denuvo не повинен впливати на продуктивність гри.

- Monster Hunter Stories 2. Видалення Denuvo перед випуском гри також залишається невідомою причиною, але після цього розмір exe-файлів гри зменшився на 414 Мб.

- Humankind. Розробники видалили захист через його вплив на продуктивність. В їх заяві було сказано: "Нашим пріоритетом завжди є найкращий можливий досвід для гравців, які купують наші ігри та підтримують нас. Denuvo не повинен впливати на продуктивність гравців, і ми не хочемо жертвувати якістю для вас. Ми вважаємо, що це можливо з правильною інтеграцією, і саме це ми хотіли перевірити під час закритого бета-тесту. Однак ми виявили, що поточна інтеграція не є достатньою, і це не щось, що ми можемо виправити до релізу. Тому ми його видалили."

Атаки на системи DRM у відеоігровій індустрії відображають глибокі фактори та мотивації, що підштовхують групи до злomu ігрових захистів. Розглянуті типи та організаційна структура таких груп свідчать про складний ландшафт відмінностей інтересів і методів, які вони використовують для здійснення атак. Реакція розробників на злам гри - усунення чи збереження Denuvo - відображає неоднозначність цього питання. Деякі розробники прибирають захист після злomu, намагаючись зберегти відкритість для гравців і уникнути проблем продуктивності, тоді як інші воліють залишити захист незалежно від інцидентів злomu, дотримуючись стратегій оновлення та доповнень. Варіативність реакцій свідчить про складний баланс між захистом від піратства і забезпеченням задоволення від ігор для всіх гравців.

### **3 ПРАКТИЧНЕ ДОСЛІДЖЕННЯ ВПЛИВУ DRM ЗАХИСТУ НА ПРОДУКТИВНІСТЬ ВІДЕОІГОР**

#### **3.1 Вибір ігор та розробка методології тестування**

Для практичного завдання було вирішено провести детальний аналіз продуктивності відеоігор, захищених системами DRM, та їх піратських версій, де цей захист відсутній. Найпопулярнішою та найефективнішою DRM-системою на даний момент є Denuvo.

Для кращого розуміння предмету дослідження та його параметрів, наведено пояснення ключових термінів:

- FPS (Кадри в секунду) - одиниця виміру, яка показує кількість кадрів, що відображаються на екрані протягом однієї секунди. Це важливий показник для вимірювання плавності відтворення гри або відео.

- Бенчмарк. Тестовий захід, спрямований на вимірювання продуктивності комп'ютерних компонентів, таких як процесори, відеокарти, або програмного забезпечення.

- Бенчмаркінг. Процес виконання бенчмарків для оцінки продуктивності апаратних або програмних компонентів.

- Відеопам'ять. Пам'ять, призначена для зберігання графічної інформації, необхідної для відображення зображень та відео на екрані.

- Середній FPS. Середня кількість кадрів в секунду, що відображаються на екрані протягом певного періоду часу.

- Low 1%. Це показник, який вказує на середню кількість кадрів в секунду, які відображаються на екрані в найбільш навантажених або інтенсивних моментах гри. Цей показник вимірюється відсотком найнижчих значень кадрів у порівнянні з загальною кількістю кадрів за певний період часу.

- Low 0,1%. Це ще більш ретельний показник, який вказує на середню кількість кадрів в секунду в найменш стабільних або найменш продуктивних

моментах гри. Цей показник вимірюється відсотком найнижчих 0,1% значень кадрів у порівнянні з загальною кількістю кадрів за певний період часу.

Для тестування були обрані чотири гри:

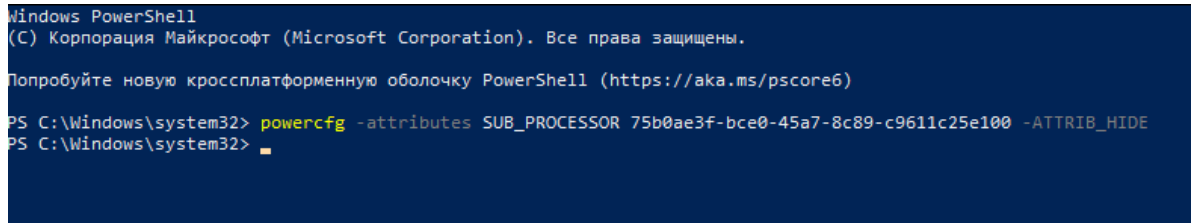
- Far Cry 5 (захист: Steam, Ubisoft Connect launcher, Denuvo)
- Battlefield (захист: Steam, EA on-line activation, Origin client software, Denuvo)
- STAR WARS Battlefront II (захист: Epic Games Store, EA on-line activation, Origin client software, Denuvo)
- Marvel's Guardians of the Galaxy (захист: Epic Games Store, Denuvo)

Тестування буде проводитися на трьох різних, в залежності від бюджету, конфігураціях ПК, що дозволить отримати більш повне уявлення про вплив DRM на продуктивність ігор:

- Конфігурація 1: відеокарта RTX 4070 Super, процесор Ryzen 7 5800x (8 ядер, максимальна частота 4800 МГц), оперативна пам'ять 32 Гб частотою 3200 МГц.
- Конфігурація 2: відеокарта RTX 3060 (найпопулярніша ігрова відеокарта за статистикою Steam), процесор Ryzen 7 5800x з відключеними 2 ядрами та лімітом максимальної частоти у 4200 МГц (орієнтовано на найпопулярніший процесор AMD- Ryzen 5 5500), оперативна пам'ять 16 Гб частотою 3200 МГц.
- Конфігурація 3: відеокарта GTX 1050 ti, процесор Ryzen 7 5800x з відключеними 4 ядрами та лімітом на максимальну частоту у 4300 МГц (орієнтовано на найпопулярніший процесор бюджетного сегменту Intel Core i3-12100F), оперативна пам'ять 16 Гб частотою 3200 МГц.

Для встановлення цих конфігурацій відключення ядер процесора відбувалося у налаштуваннях BIOS, а для встановлення ліміту частоти процесора використовувалась команда PowerShell "powercfg -attributes SUB\_PROCESSOR 75b0ae3f-bce0-45a7-8c89-c9611c25e100 -ATTRIB\_HIDE". Ця команда розблокувала налаштування максимальної частоти. У Windows 10 для доступу до цих налаштувань необхідно було в панелі управління обрати "електроживлення", далі "налаштування схеми електроживлення", потім

"змінити додаткові параметри живлення". У категорії "управління живленням процесора" з'являлася опція "максимальна частота процесора", де можна було встановити потрібні значення у МГц.



```
Windows PowerShell
(C) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

Попробуйте новую кроссплатформенную оболочку PowerShell (https://aka.ms/powershell)

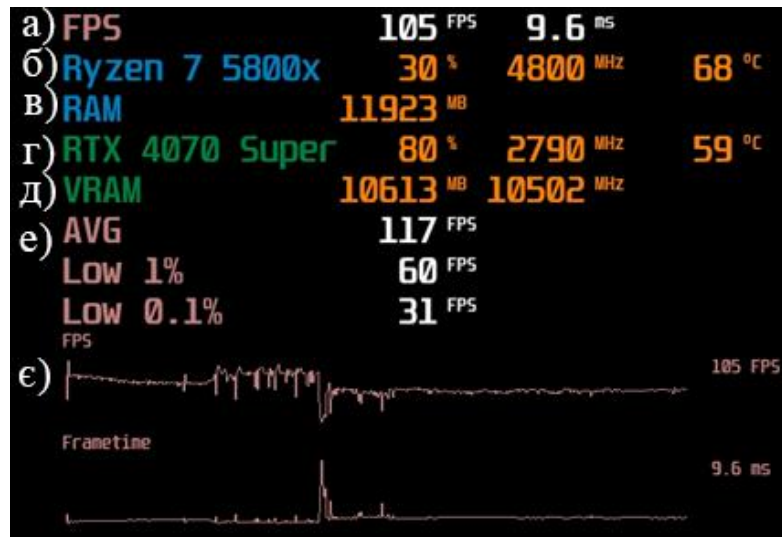
PS C:\Windows\system32> powercfg -attributes SUB_PROCESSOR 75b0ae3f-bce0-45a7-8c89-c9611c25e100 -ATTRIB_HIDE
PS C:\Windows\system32>
```

Рисунок 3.1– Приклад виконання команди у PowerShell

Всі ігри були встановлені одночасно на один SSD накопичувач об'ємом 1 ТБ, що забезпечує рівні умови для всіх ігор на всіх конфігураціях. Метою дослідження не є досягнення точного співпадіння результатів з конфігураціями «процесорів-орієнтирів» через різницю в архітектурі кристалу процесора. Основною метою є порівняння однакових показників в однакових умовах тестування для ліцензійних ігор з працюючими DRM системами та піратських версій, де ці системи обходяться та не працюють під час ігрового процесу.

Показники, що будуть порівнюватися:

- FPS (середній, Low 1%, Low 0,1%)
- Рівність графіку часу кадру
- Ступінь завантаження процесора (у відсотковому вираженні)
- Об'єм використовуваної оперативної пам'яті
- Об'єм та частота використання відеопам'яті відеокарти
- Час, потрібний для першого запуску гри
- Час, потрібний для другого запуску гри



а— показники кількості FPS та час кадру в даний час; б— завантаженість, частота, температура ЦП; в— об'єм використовуваної оперативної пам'яті (ОЗУ); г— завантаженість, частота, температура графічного процесора (ГП); д— об'єм та частота використовуваної відеопам'яті; е— середній FPS, Low 1%, Low 0,1% на протязі бенчмаркінгу; є— графіки FPS та часу кадру.

Рисунок 3.2— Розміщення та назви показників моніторингу

Всі показники будуть порівнюватися на однакових сценах для кожної пари ігор, що дозволить отримати об'єктивні дані про вплив DRM на продуктивність відеоігор.

### 3.2 Порівняльний аналіз результатів тестування

Аналіз результати тестування, що були проведені на трьох різних конфігураціях ПК. Дослідження охоплює порівняльний аналіз різноманітних параметрів між ліцензійними версіями ігор з захистом DRM та їх піратськими аналогами. Результати будуть розділені та відсортовані, відповідно до кожної конфігурації.

У рамках першої конфігурації, яка відноситься до високобюджетного сегменту, використовуються компоненти з характеристиками, що визначені у Таблиці 3.1.

Таблиця 3.1– Параметри першої тестової конфігурації.

|                              |                                                                     |
|------------------------------|---------------------------------------------------------------------|
| ЦП                           | AMD Ryzen 7 5800x, 8 ядер 16 потоків, максимальна частота- 4800 мГц |
| ГП                           | Nvidia Geforce RTX 4070 super                                       |
| ОЗУ                          | 32 Гб DDR4 з частотою 3200 мГц                                      |
| Сховище                      | SSD M.2 (PCI-E 4.0 x4) на 1 ТБ                                      |
| Налаштування графіки в іграх | Максимальні налаштування з увімкненим DirectX12                     |
| Роздільна здатність          | Full HD 1920×1080                                                   |

Для першої конфігурації, були виміряні часи завантаження ліцензійних і піратських версій ігор. Результати наведені у табл. 3.2.

Таблиця 3.2– Час завантаження ігор для першої конфігурації (у секундах)

| Гра                              | Ліцензійна версія - перший запуск | Ліцензійна версія - другий запуск | Зломана версія - перший запуск | Зломана версія - другий запуск |
|----------------------------------|-----------------------------------|-----------------------------------|--------------------------------|--------------------------------|
| Battlefield V                    | 106                               | 58,1                              | 56                             | 45,6                           |
| STAR WARS Battlefront II         | 85,6                              | 22,9                              | 83,9                           | 83,7                           |
| Marvel's Guardians of the Galaxy | 41,7                              | 36,4                              | 52,3                           | 52                             |
| Far Cry 5                        | 71                                | 39                                | 30,7                           | 23,9                           |

Результати тестування показують, що піратські версії ігор у більшості випадків завантажуються швидше у порівнянні з ліцензійними версіями.

- Battlefield V. Зломана версія значно швидше завантажується як під час першого запуску з різницею у 47.17%, так і під час другого запуску з різницею у 21.51%.

- STAR WARS Battlefront II. Тут різниця в часі завантаження між ліцензійною і піратською версіями незначна для першого запуску, але для другого запуску зломана версія завантажується значно повільніше з різницею у 261.14%.

- Marvel's Guardians of the Galaxy. Ліцензійна версія має швидший час завантаження як під час першого запуску на 25.42%, так і під час другого запуску на 42.86%.

- Far Cry 5. Зломана версія показала значно кращі результати як під час першого запуску з різницею у 131.27%, так і під час другого запуску 63.18%.

Загалом, піратські версії ігор зазвичай демонструють швидший час завантаження у порівнянні з ліцензійними версіями, що можна пояснити кількома причинами:

- Додаткове навантаження DRM. DRM-захист, такий як Denuvo, часто додає додаткове навантаження на систему під час запуску гри. Це може включати перевірки ліцензій, шифрування та інші процеси, які можуть значно уповільнити час завантаження.

- Оптимізація піратських версій. Піратські версії можуть бути оптимізовані хакерами для кращої продуктивності, що включає видалення DRM-захисту та інших непотрібних процесів, що прискорює завантаження гри.

- Запуск лаунчерів. Для ліцензійних версій ігор часто потрібно запускати один, а інколи і два лаунчери (наприклад, Steam, Origin або Epic Games Store), що також додає час до загального часу завантаження. Це пояснює велику різницю між першим та другим запуском гри, оскільки у другий раз всі лаунчери запуснені та готові до роботи.

Таким чином, основним фактором, що впливає на швидкість завантаження ліцензійних версій ігор, є наявність DRM-захисту та необхідність запуску додаткових лаунчерів, які можуть створювати додаткове навантаження на систему. Це важливий аспект для розробників, які повинні збалансувати між

захистом своїх продуктів і забезпеченням оптимальної продуктивності для користувачів.

Першим на черзі буде Battlefield V. Важливо зазначити, що під час тестування ліцензійної версії при першій спробі були виявлені нестабільності роботи. На рис. 3.3 та рис. 3.4 зображено два випадки різких стрибків на графіку часу кадру, так званих "статтерів". Вони спостерігалися протягом усього тестування. Через ці нерівності на графіку сам ігровий процес відчувався "рвано", що можна побачити на моніторингу FPS. Хоча середній FPS був більше 150, значення Low 1% та Low 0,1% не перевищували 10 кадрів.

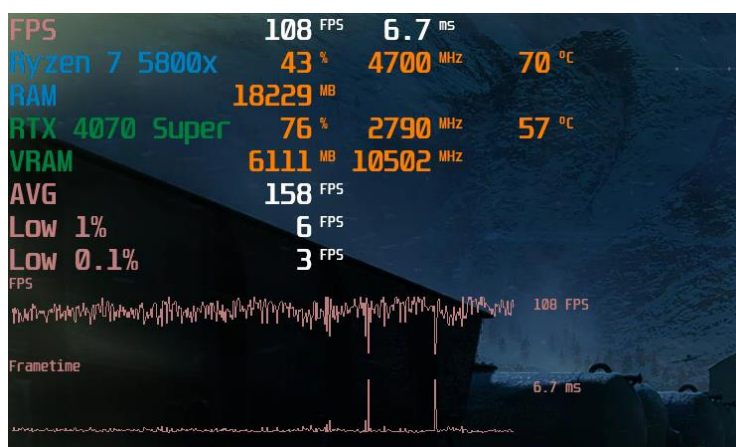


Рисунок 3.3— Один з випадків статерів (конфігурація 1)



Рисунок 3.4— Другий з випадків статерів (конфігурація 1)

Подібна поведінка зазвичай виникає під час завантаження чи провантаження локації. В даному випадку ніяких завантажень чи переходів не було – персонаж біг по прямій лінії на провантаженій локації. Проблема вирішилася після повного перезапуску гри, що під час реального онлайн матчу виконати не так легко і зручно. Точні причини цього явища визначити не вдалося, у інших іграх та конфігураціях такої критичної ситуації не виникало.

На рисунку 3.4 можна чітко побачити залежність двох графіків. FPS одразу падав, як підіймався час кадру. У відрізку з трьома стрибками видно, наскільки нерівний графік під час статтерів і як він стабілізувався після них.

Переходимо до безпосереднього порівняння коректних тестів. Тестовою сценою слугувала перша місія одиночної кампанії. Результати знімалися на однаковому моменті у кінці місії.

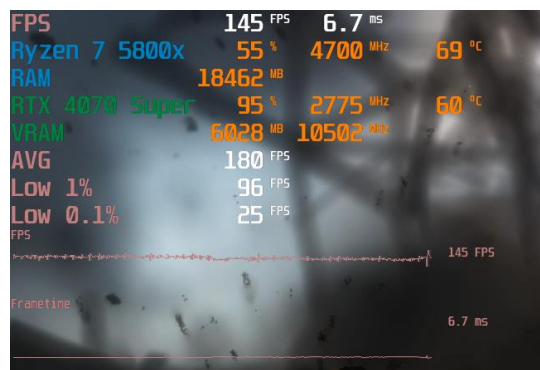


Рисунок 3.5– Результат тестування ліцензійної версії Battlefield V (конфігурація 1)



Рисунок 3.6– Результат тестування зломаної версії Battlefield V (конфігурація 1)

За результатами тестування можна зробити такі висновки:

- FPS у обох версіях майже однаковий, проте значення Low 1% та Low 0.1% на зломаній версії вище, що означає, що гра працювала плавніше.

- Важливою відмінністю є інші показники, такі як завантаження оперативної пам'яті ОЗУ та відеопам'яті. У ліцензійній версії використовується майже на 3 Гб більше ОЗУ та на 200 Мб більше відеопам'яті.

У STAR WARS Battlefront II виникла дивна ситуація. Тестовою сценою слугував рівень зі "Сценарії битв". Дивність ситуації полягає в тому, що ліцензійна версія дуже нестабільно працювала у відкритих яскравих локаціях. В той час як зламана версія використовувала лише половину можливостей відеокарти, хоча зазвичай ігри використовують всі 100% можливостей відеочіпу. Перезапуск не змінив ситуацію в обох випадках.

На рисунку 3.7 можна побачити найвиразніший момент нестабільності, про рівність графіків тут не може йтися.



Рисунок 3.7– Результат тестування ліцензійної версії STAR WARS Battlefront II (конфігурація 1)



Рисунок 3.8– Результат тестування зламаної версії  
STAR WARS Battlefront II (конфігурація 1)

Підбиваючи підсумки тестування цієї пари можна виділити наступні моменти:

- Ліцензійна версія по всім параметрам поступається зламаній версії. Через нестабільну роботу виникає велика різниця у FPS, до 60 кадрів.
- Піратська версія використовує на 3,5 Гб менше ОЗУ.
- Відеочіп у зламаній версії працює тільки на половину своїх можливостей. Однак, оскільки це не викликало ніяких проблем з продуктивністю, цей факт можна вважати скоріше особливістю роботи гри, а не проблемою.
- Використання відеопам'яті в зламаній версії становить менше ніж третину від ліцензійної версії.

Причинами такої нестабільності можуть бути проблеми серверної частини зі сторони EA або самої Denuvo. Відомо багато випадків проблем стабільності гри або навіть запуску гри через збої роботи серверів Denuvo.

У грі Marvel's Guardians of the Galaxy присутній вбудований бенчмарк, який спеціально розроблено для тестування продуктивності системи. Результати оцінювалися як з вбудованого бенчмарку, так і з тестової сцени в самій грі.

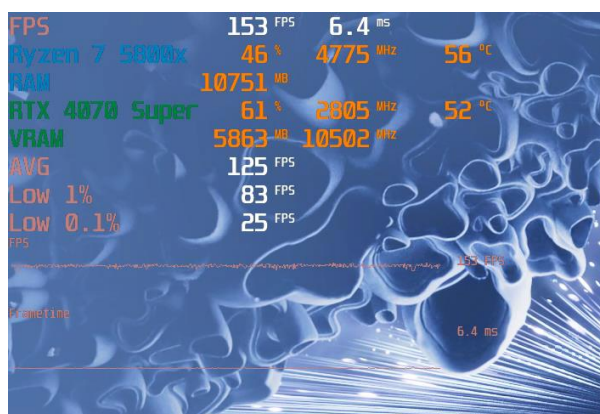


Рисунок 3.9— Результат вбудованого бенчмарку ліцензійної версії  
Marvel's Guardians of the Galaxy (конфігурація 1)

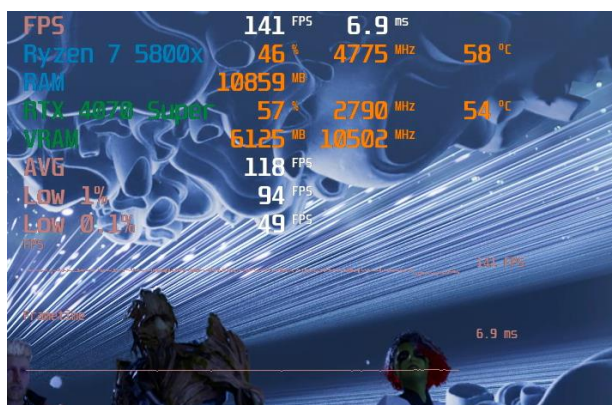


Рисунок 3.10— Результат вбудованого бенчмарку зламаної версії  
Marvel's Guardians of the Galaxy (конфігурація 1)

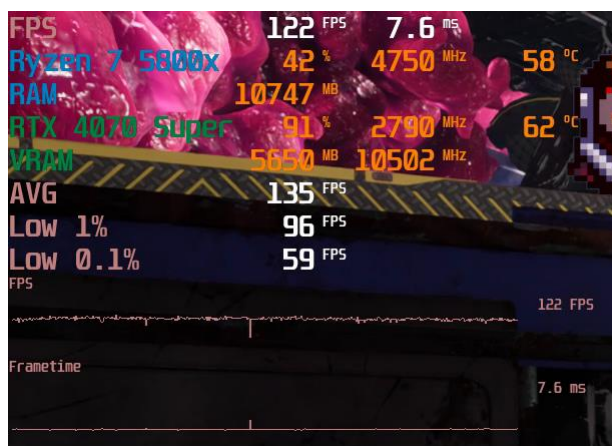


Рисунок 3.11— Результат тестування ліцензійної версії  
Marvel's Guardians of the Galaxy (конфігурація 1)



Рисунок 3.12– Результат тестування зламаної версії  
Marvel's Guardians of the Galaxy (конфігурація 1)

Ліцензійна версія гри виграє у порівнянні з піратською. У результатах вбудованого бенчмарку середній FPS у ліцензійній версії трохи вищий, і цю різницю не можна вважати помилкою через людський фактор, оскільки у вбудованому тесті використовуються ідентичні сцени. Проте показники Low 1% та Low 0.1% залишаються нижчими, що може бути пов'язано з використанням внутрішньоігрових подій, описаними у першому розділі.

Під час безпосереднього ігрового процесу лідерство повністю переходить до ліцензійної версії, яка має вищі показники FPS та однакове використання ресурсів ПК. Це легко пояснюється хорошою оптимізацією гри, коли гра виходила не було ніяких скарг на порану роботу чи ще якісь проблеми, що зараз, нажаль, велика рідкість.

У наступній грі, Far Cry 5, також є вбудований бенчмарк, результати якого використовувалися разом з тестом ігрового процесу, а саме тестуванням прологу гри.



Рисунок 3.13— Результат вбудованого бенчмарку ліцензійної версії Far Cry 5 (конфігурація 1)

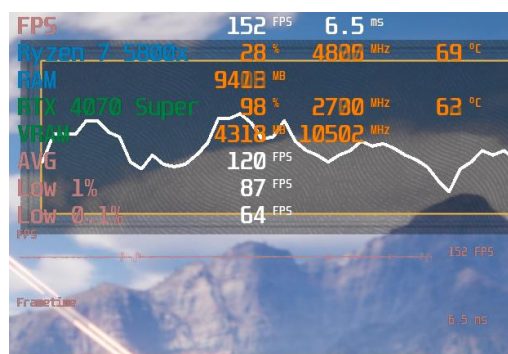


Рисунок 3.14— Результат вбудованого бенчмарку зламаної версії Far Cry 5 (конфігурація 1)

В бенчмарку помітний незначний пріоритет ліцензійної версії у FPS. Однак, ліцензійна версія використовує на 2 Гб більше ОЗУ та на 3 Гб більше відеопам'яті.

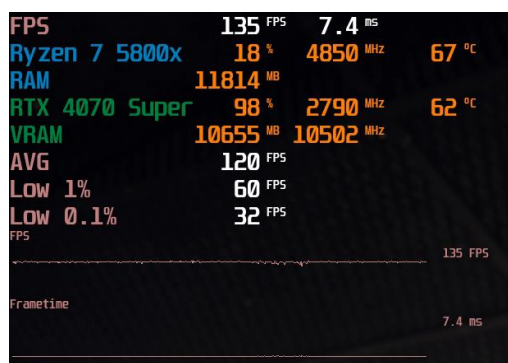


Рисунок 3.15— Результат тестування ліцензійної версії Far Cry 5 (конфігурація 1)

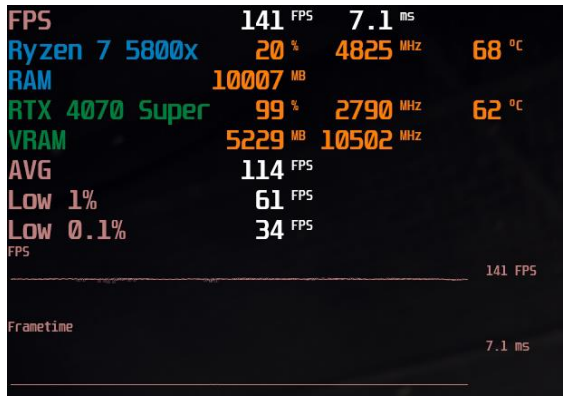


Рисунок 3.16– Результат тестування зламаної версії Far Cry 5 (конфігурація 1)

У тесті прологу результати були зафіксовані у самому кінці, і вони досить схожі з тими, що були у синтетичному тесті. Різниця у FPS становила близько 5 одиниць на користь ліцензії. Відмінність у використанні ОЗУ залишилась приблизно 2 Гб, тоді як різниця у використанні відеопам'яті зросла до 5 Гб.

У рамках другої конфігурації, яка відноситься до середньобюджетного сегменту, використовуються компоненти з характеристиками, що визначені у Таблиці 3.3.

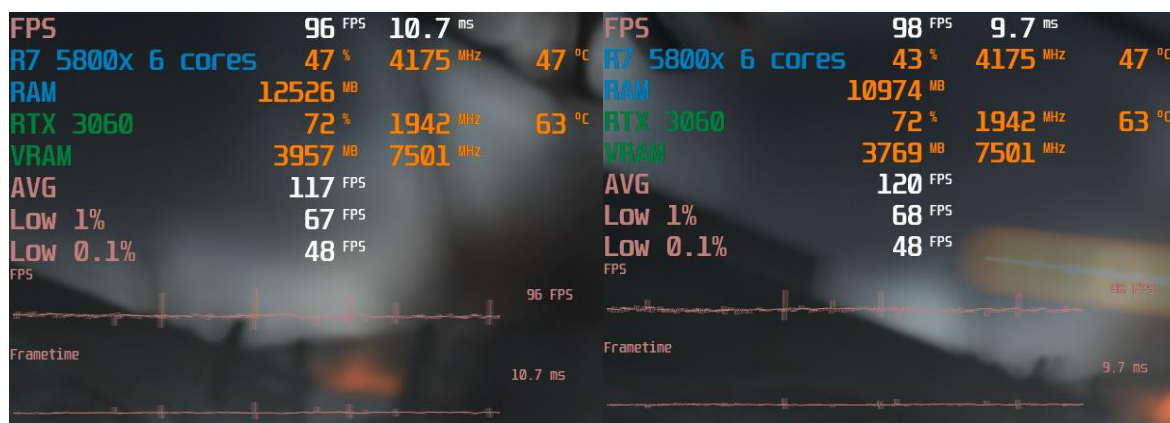
Таблиця 3.3– Параметри другої тестової конфігурації.

|                              |                                                                     |
|------------------------------|---------------------------------------------------------------------|
| ЦП                           | AMD Ryzen 7 5800x, 6 ядер 12 потоків, максимальна частота- 4200 мГц |
| ГП                           | Nvidia Geforce RTX 3060                                             |
| ОЗУ                          | 16Гб DDR4 з частотою 3200 мГц                                       |
| Сховище                      | SSD M.2 (PCI-E 4.0 x4) на 1 ТБ                                      |
| Налаштування графіки в іграх | Високі налаштування з вимкненим DirectX 12                          |
| Роздільна здатність          | Full HD 1920×1080                                                   |

Таблиця 3.4– Час завантаження ігор для другої конфігурації (у секундах)

| Гра                                    | Ліцензійна<br>версія -<br>перший запуск | Ліцензійна<br>версія -<br>другий запуск | Зломана версія<br>- перший<br>запуск | Зломана<br>версія -<br>другий запуск |
|----------------------------------------|-----------------------------------------|-----------------------------------------|--------------------------------------|--------------------------------------|
| Battlefield V                          | 105,1                                   | 60                                      | 46,9                                 | 44,3                                 |
| STAR WARS<br>Battlefront II            | 126,5                                   | 47,8                                    | 108,4                                | 83,7                                 |
| Marvel's<br>Guardians of<br>the Galaxy | 59,1                                    | 44,7                                    | 60                                   | 62,3                                 |
| Far Cry 5                              | 71,5                                    | 43,1                                    | 40,1                                 | 26                                   |

У другій конфігурації зберігається та сама закономірність. Ліцензійні версії, окрім Marvel's Guardians of the Galaxy, завантажуються повільніше, ніж їхні зломані версії.



а)

б)

а– ліцензійна версія; б– зламана версія

Рисунок 3.17– Результати тестування обох версій Battlefield V (конфігурація 2)

Результати тестування не показали значної різниці в продуктивності між ліцензійними та зломаними версіями ігор. Показники FPS відрізнялися на рівні

похибки, що робить цю різницю непомітною для користувача. Однак, як і в попередніх тестах, ліцензійні версії споживають більше ресурсів ПК: на 1,5 Гб більше ОЗУ та на 200 Мб більше відеопам'яті.



а)

б)

а— ліцензійна версія; б— зламана версія

Рисунок 3.18— Результати тестування обох версій STAR WARS Battlefront II (конфігурація 2)

Для даної конфігурації було вже задіяно всі 100% ресурсів ПК, на відміну від високобюджетної. Різниця у FPS не досягає і 10 кадрів, що можна вважати також на рівні похибки, оскільки точні на 100% події неможливо відтворити у двох різних матчах. Вже стандартною ситуацією є і різниця у використанні пам'яті, а саме: ліцензійна версія використовує на 1 Гб більше ОЗУ та на 700 Мб більше відеопам'яті.

Під час тестування за допомогою вбудованого бенчмарку Marvel's Guardians of the Galaxy було виявлено статери у конкретних відрізках як для ліцензійної, так і для зламаної версії. Стрибки графіку часу кадра відбувались на одних і тих самих моментах в обох версіях, але інтенсивність цих стрибків у ліцензійній версії була значно вищою. Оскільки це відбувалось в обох версіях, провину на внутрішньоігрові події перекладати не можна — проблема криється в особливостях роботи самої гри.

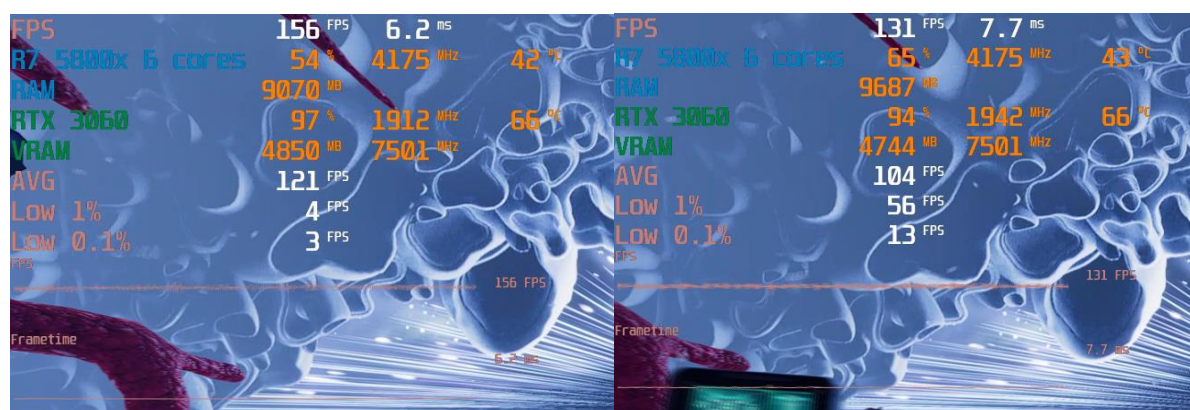


а)

б)

а– ліцензійна версія; б– зламана версія

Рисунок 3.19– Статери під час тестування вбудованого бенчмарку обох версій Marvel's Guardians of the Galaxy (конфігурація 2)



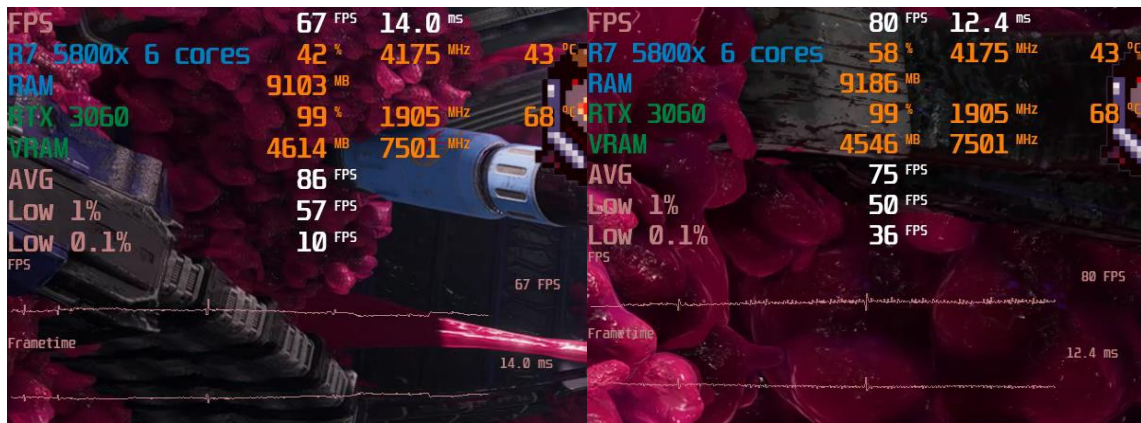
а)

б)

а– ліцензійна версія; б– зламана версія

Рисунок 3.20– Результати тестування вбудованого бенчмарку обох версій Marvel's Guardians of the Galaxy (конфігурація 2)

Через різну інтенсивність статерів, у фінальному результаті тестування видно, що хоч у ліцензійної версії середній FPS вищий, показники Low 1% та Low 0,1% кардинально відрізняються. Дуже цікавим є факт, що зламана версія потребує більшого об'єму ОЗУ, що зберегло закономірність з попереднього тестування.



а)

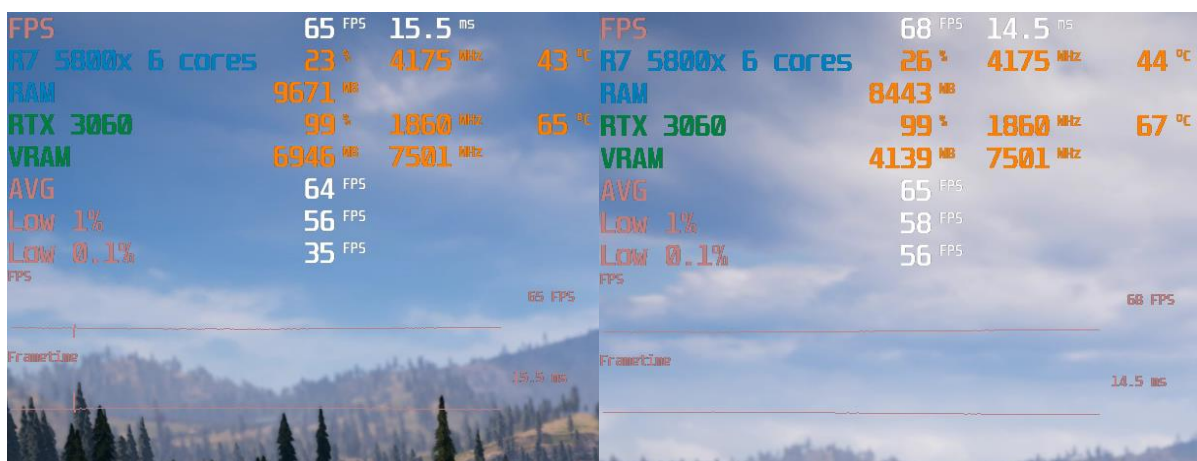
б)

а– ліцензійна версія; б– зламана версія

Рисунок 3.21– Результати тестування обох версій  
Marvel's Guardians of the Galaxy (конфігурація 2)

За результатами тестування самого ігрового процесу видно, що при приблизно однаковому використанні ресурсів ліцензійна версія випереджає зламану за двома з трьох показників FPS, поступаючись лише у показнику Low 0,1% через значно сильніші стрибки часу кадра.

За результатами тестування вбудованого бенчмарку Far Cry 5 можна зазначити, що FPS відрізняється тільки у Low 0,1%, через один статер, який є в обох версіях, але, як і у попередній грі, відрізнялась сила та інтенсивність статеру. Серед інших показників можна помітити різницю у використанні пам'яті: ліцензійна версія використовує на 1 Гб більше ОЗУ та на 3 Гб більше відеопам'яті.

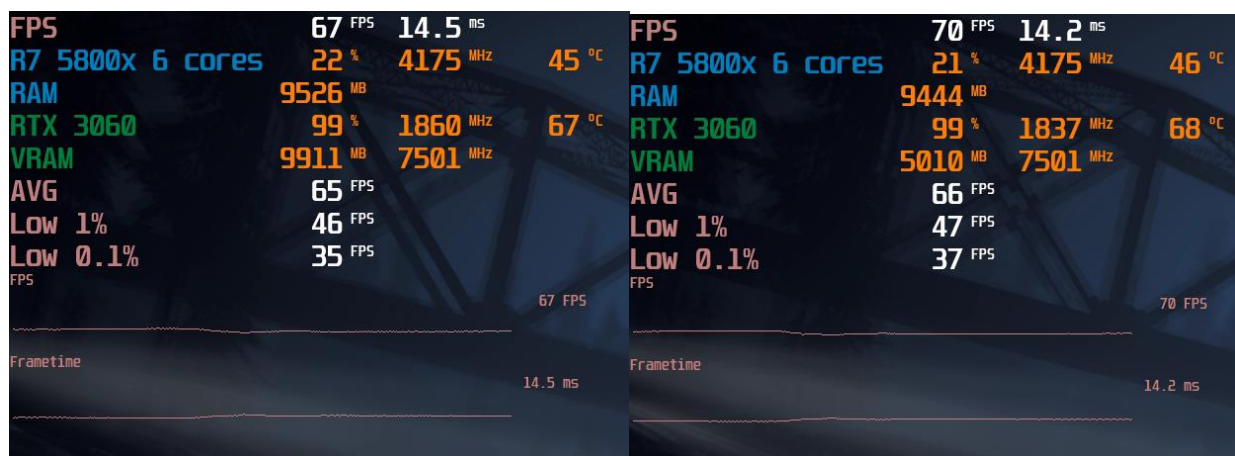


а)

б)

а– ліцензійна версія; б– зламана версія

Рисунок 3.22– Результати тестування вбудованого бенчмарку обох версій Far Cry 5 (конфігурація 2)



а)

б)

а– ліцензійна версія; б– зламана версія

Рисунок 3.23– Результати тестування обох версій Far Cry 5 (конфігурація 2)

На відміну від синтетичного тесту, під час ігрового процесу всі показники FPS відрізнялись у рамках похибки. На подив, об'єм використовуваної ОЗУ також не відрізняється, проте різниця у використанні відеопам'яті сягає двократної.

У рамках третьої конфігурації, яка відноситься до низькобюджетного сегменту, використовуються компоненти з характеристиками, що визначені у Таблиці 3.5.

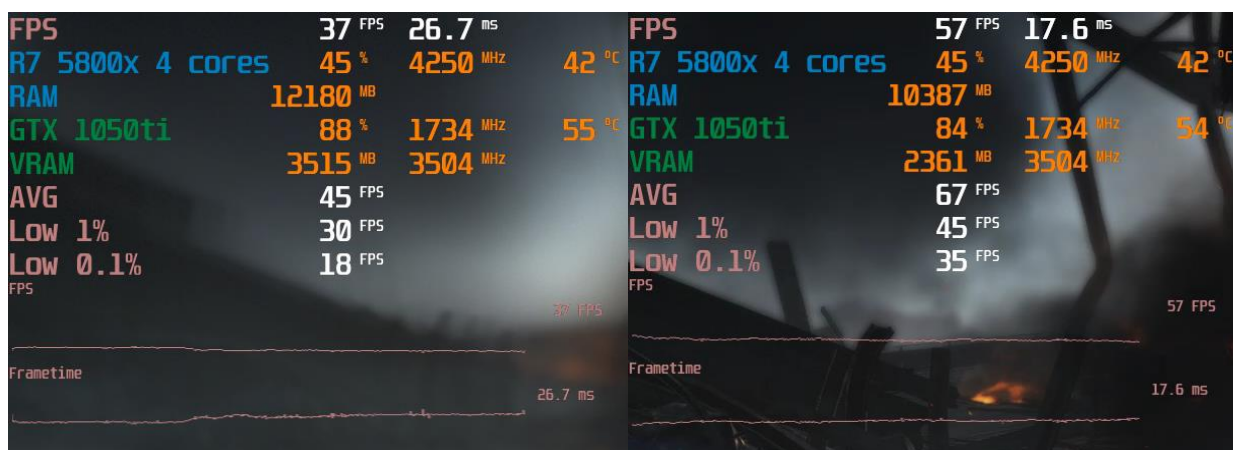
Таблиця 3.5– Параметри третьої тестової конфігурації.

|                              |                                                                       |
|------------------------------|-----------------------------------------------------------------------|
| ЦП                           | AMD Ryzen 7 5800x, 4 ядра 8 потоків,<br>максимальна частота- 4300 мГц |
| ГП                           | Nvidia Geforce GTX 1050ti                                             |
| ОЗУ                          | 16Гб DDR4 з частотою 3200 мГц                                         |
| Сховище                      | SSD M.2 (PCI-E 4.0 x4) на 1 ТБ                                        |
| Налаштування графіки в іграх | Мінімальні налаштування з вимкненим<br>DirectX 12                     |
| Роздільна здатність          | Full HD 1920×1080                                                     |

Таблиця 3.6– Час завантаження ігор для третьої конфігурації (у секундах)

| Гра                                    | Ліцензійна<br>версія -<br>перший запуск | Ліцензійна<br>версія -<br>другий запуск | Зломана версія<br>- перший<br>запуск | Зломана<br>версія -<br>другий запуск |
|----------------------------------------|-----------------------------------------|-----------------------------------------|--------------------------------------|--------------------------------------|
| Battlefield V                          | 85,6                                    | 62                                      | 47,3                                 | 44                                   |
| STAR WARS<br>Battlefront II            | 223                                     | 47                                      | 94                                   | 68                                   |
| Marvel's<br>Guardians of<br>the Galaxy | 77,5                                    | 36,4                                    | 54,6                                 | 52                                   |
| Far Cry 5                              | 91,5                                    | 51,8                                    | 30,3                                 | 20,5                                 |

Для третьої конфігурації ситуація з часом запуску дещо змінилась. Під час першого запуску STAR WARS Battlefront II в обох версіях проводилась оптимізація шейдерів, але, як можна побачити у таблиці 3.6, у ліцензійної версії це відбувалось більш ніж на 2 хвилини довше. Проте, як і у попередніх конфігураціях, другий запуск був швидшим, ніж у зламаній версії. Також, це вперше, коли ліцензійна версія Marvel's Guardians of the Galaxy поступилася у швидкості зламаній версії.



а)

б)

а– ліцензійна версія; б– зламана версія

Рисунок 3.24– Результати тестування обох версій Battlefield V  
(конфігурація 3)

Результати тестування Battlefield V показують критичну різницю у показниках FPS між ліцензійною та зламаною версіями. У зламаній версії середній FPS вище 60 кадрів, що дуже важливо для плавного геймплею, а також значення Low 1% та Low 0.1% перевищують 30 кадрів, що свідчить про стабільність і плавність гри. Ліцензійна версія використовує на 2 Гб більше ОЗУ та 2 Гб більше відеопам'яті порівняно з зламаною версією.



а)

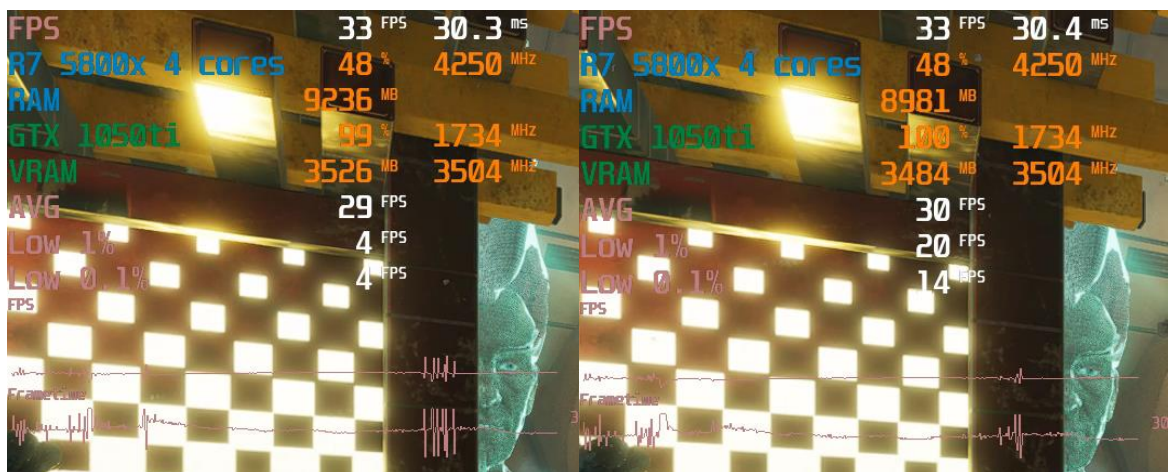
б)

а– ліцензійна версія; б– зламана версія

Рисунок 3.25– Результати тестування обох версій STAR WARS Battlefront II  
(конфігурація 3)

У STAR WARS Battlefront II спостерігається схожа ситуація з тестом попередньої конфігурації. Хоча різниця у показниках FPS становить приблизно 10 кадрів, на користь зламаної версії, це не так помітно через загально високі показники. Ліцензійна версія використовує на 1,5 Гб більше ОЗУ та на 500 Мб більше відеопам'яті порівняно з зламаною версією.

Під час тестування Marvel's Guardians of the Galaxy на третій конфігурації також були виявлені статери у вбудованому бенчмарку, але цього разу вони виникали у трохи інших місцях, ніж на попередній конфігурації. Інтенсивність статерів знову була більшою у ліцензійній версії. Наслідки цього можна побачити на графіку FPS на рис. 3.26а, де чітко видно сильні різкі стрибки, тоді як на зламаний версії (рис. 3.26б) графік FPS залишається майже рівним.

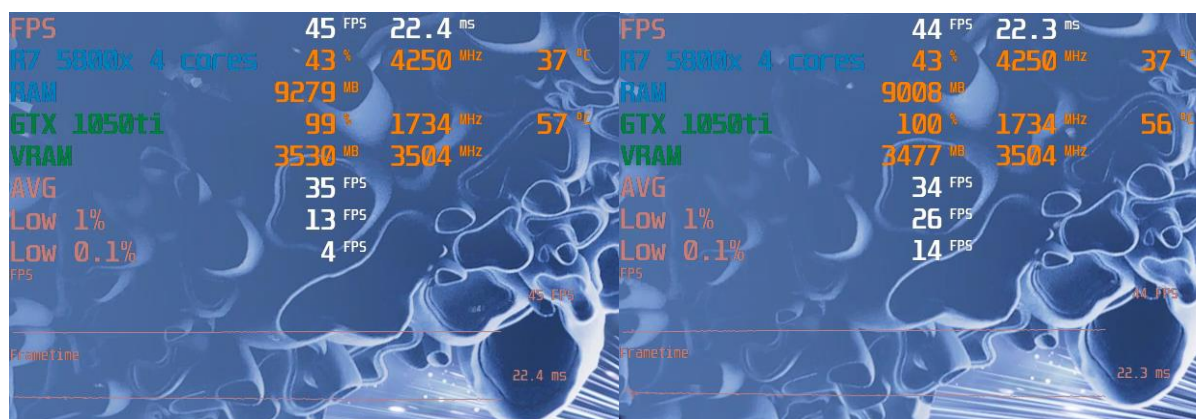


а)

б)

а— ліцензійна версія; б— зламана версія

Рисунок 3.26— Статери під час тестування вбудованого бенчмарку обох версій Marvel's Guardians of the Galaxy (конфігурація 3)



а)

б)

а– ліцензійна версія; б– зламана версія

Рисунок 3.27– Результати тестування вбудованого бенчмарку обох версій  
Marvel's Guardians of the Galaxy (конфігурація 3)

Фінальні результати тестування бенчмарку показують незначну різницю у середньому FPS, але суттєву різницю у Low 1% та Low 0.1%. У споживанні ресурсів ПК спостерігається незначна різниця у використанні ОЗУ. За результатами тестування безпосередньо ігрового процесу не було виявлено значних відмінностей у продуктивності. Споживання ОЗУ у ліцензійній версії було більшим на 400 Мб, ніж у зламаної версії.



а)

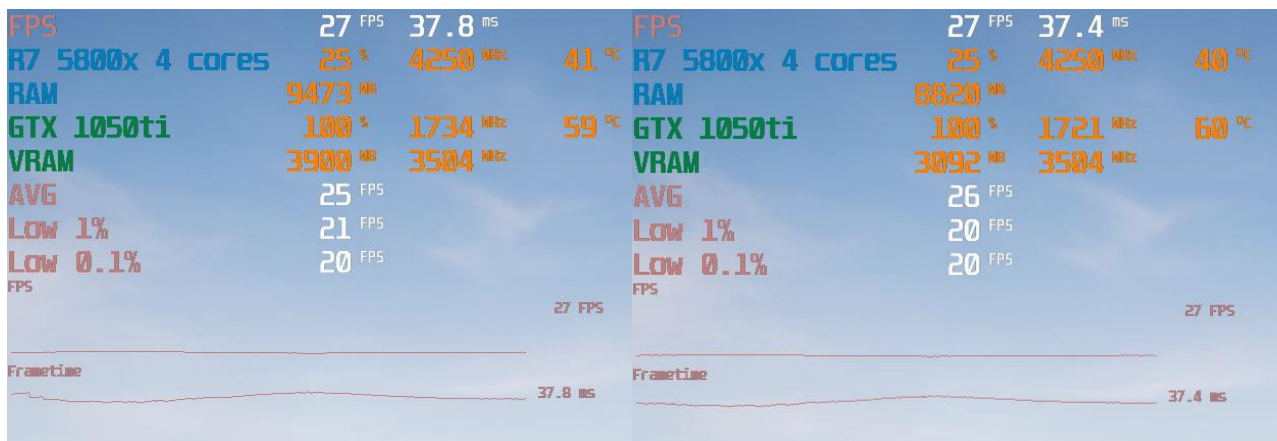
б)

а– ліцензійна версія; б– зламана версія

Рисунок 3.28– Результати тестування обох версій  
Marvel's Guardians of the Galaxy (конфігурація 3)

У даному випадку ситуація протилежна до тієї, що була на першій конфігурації: загальна продуктивність обох версій була настільки малою, що різниця між ними не відчувалася.

За результатами тестування бенчмарку Far Cry 5 не було виявлено відмінностей у FPS. Однак ліцензійна версія використовувала на 600 Мб більше ОЗУ та на 800 Мб більше відеопам'яті при загальному об'ємі відеопам'яті у 4 Гб.



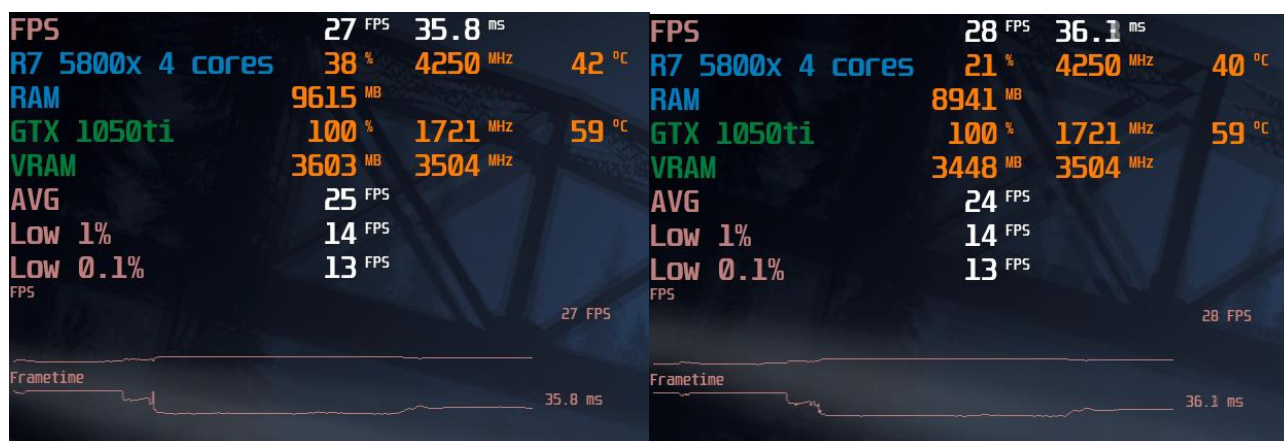
а)

б)

а– Ліцензійна версія; б– зламана версія

Рисунок 3.29– Результати тестування вбудованого бенчмарку обох версій Far Cry 5 (конфігурація 3)

Результати тестування ігрового процесу показали подібну ситуацію, відмінність у використанні відеопам'яті зменшилася, але ліцензійна версія все ще потребує більше ресурсів. У Far Cry 5 спостерігалася подібна ситуація, як і у Marvel's Guardians of the Galaxy, з занадто низькою продуктивністю для помітної різниці.



а)

б)

а– ліцензійна версія; б– зламана версія

Рисунок 3.30– Результати тестування обох версій Far Cry 5 (конфігурація 3)

У Far Cry 5 спостерігалася подібна ситуація, як і у Marvel's Guardians of the Galaxy, з занадто низькою продуктивністю для помітної різниці.

## ВИСНОВКИ

Проведене дослідження охоплює вплив DRM захисту на продуктивність відеоігор, порівняння ліцензійних та зламаних версій ігор на трьох різних конфігураціях ПК. Загальний аналіз показав, що у більшості випадків зламані версії ігор демонструють кращу продуктивність та стабільність у порівнянні з ліцензійними версіями. Всі протестовані ігри, включаючи Battlefield V, STAR WARS Battlefront II, Marvel's Guardians of the Galaxy та Far Cry 5, показали, що ліцензійні версії використовують більше ресурсів ПК. Це було особливо помітно у випадку з Battlefield V та STAR WARS Battlefront II. Marvel's Guardians of the Galaxy, на відміну від інших ігор, у більшості випадків показала кращі результати у ліцензійній версії, ніж у зламаних.

Результати тестування часу завантаження ігор показали, що зламані версії зазвичай завантажуються швидше як під час першого, так і під час другого запуску. Особливо це помітно у випадку з Battlefield V та Far Cry 5, де зламані версії показали значно кращі результати на всіх трьох конфігураціях.

DRM системи не є основним чинником у питанні продуктивності ігор, вони лише ескалюють наявні проблеми в оптимізації, на яку останнім часом розробники закривають очі з багатьох причин. Розумним рішенням проблеми може бути замість впровадження DRM систем зосередитись на розробці мультиплеєрних режимів для високобюджетних AAA проектів, які важче зламати. Це може зацікавити гравців які спробували урізану зламану версію і змотивувати придбати гру. Для інді сектору варто встановлювати DRM системи, оскільки зазвичай в іграх з малим бюджетом максимум буває кооперативна гра яку легко обійти локальною мережею. Проте, знаючи розцінки Denuvo, цей варіант не виглядає можливим, бо в такому випадку бюджет на захист гри буде вище, ніж бюджет самої гри.

## ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Mori R., Tashiro S. The Concept of Software Service System (SSS). *Systems and Computers in Japan*. 1988. Vol. 19, no. 5. P. 38–49. URL: <https://doi.org/10.1002/scj.4690190504>.
2. THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998 : Закон США of 28.10.1998 no. 105-304.
3. Copy protection - Emulation General Wiki. *Emulation General Wiki*. URL: [https://emulation.gametechwiki.com/index.php/Copy\\_protection](https://emulation.gametechwiki.com/index.php/Copy_protection).
4. Steam DRM (Steamworks Documentation). *Steamworks*. URL: <https://partner.steamgames.com/doc/features/drm>.
5. Game Protection on Steam: Steam's Own Methods and 3rd Party DRM. *StarForce*. URL: <https://www.star-force.com/blog/index.php?blog=2683>.
6. Contributors to Wikimedia projects. Ubisoft Connect - Wikipedia. *Wikipedia, the free encyclopedia*. URL: [https://en.wikipedia.org/wiki/Ubisoft\\_Connect](https://en.wikipedia.org/wiki/Ubisoft_Connect).
7. Technique for enabling nominal flow of an executable file : patent EP2998895A1 eu. No. 14003279.8 ; applied on 22.09.2014 ; published on 23.03.2016. 18 p. URL: <https://patentimages.storage.googleapis.com/ee/ce/9a/ebff047200289b/EP2998895A1.pdf>.
8. Colangelo T. Theseus: Digital Rights Management in video games: their impact on performance and the legal structure connected to them. *The URN resolver of The National Library of Finland*. 124th ed. 2020. P. 10–25. URL: <https://urn.fi/URN:NBN:fi:amk-2020090320065>.
9. Contributors to Wikimedia projects. Crack intro - Wikipedia. *Wikipedia, the free encyclopedia*. URL: [https://en.wikipedia.org/wiki/Crack\\_intro](https://en.wikipedia.org/wiki/Crack_intro).
10. Contributors to Wikimedia projects. List of warez groups - Wikipedia. *Wikipedia, the free encyclopedia*. URL: [https://en.wikipedia.org/wiki/List\\_of\\_warez\\_groups](https://en.wikipedia.org/wiki/List_of_warez_groups).

11. Contributors to Wikimedia projects. Nuke (warez) - Wikipedia. Wikipedia, the free encyclopedia. URL: [https://en.wikipedia.org/wiki/Nuke\\_\(warez\)](https://en.wikipedia.org/wiki/Nuke_(warez)).
12. Contributors to Wikimedia projects. Standard (warez) - Wikipedia. Wikipedia, the free encyclopedia. URL: [https://en.wikipedia.org/wiki/Standard\\_\(warez\)](https://en.wikipedia.org/wiki/Standard_(warez)).
13. Contributors to Wikimedia projects. Topsite - Wikipedia. Wikipedia, the free encyclopedia. URL: <https://en.wikipedia.org/wiki/Topsite>.
14. Contributors to Wikimedia projects. Warez scene - Wikipedia. Wikipedia, the free encyclopedia. URL: [https://en.wikipedia.org/wiki/Warez\\_scene](https://en.wikipedia.org/wiki/Warez_scene).
15. Contributors to Wikimedia projects. Warez - Wikipedia. Wikipedia, the free encyclopedia. URL: <https://en.wikipedia.org/wiki/Warez>.
16. Btarunr. Denuvo DRM pricing structure specific to crysis remastered leaked, over \$100k for a year. TechPowerUp. URL: <https://www.techpowerup.com/275158/denuvo-drm-pricing-structure-specific-to-crysis-remastered-leaked-over-usd-100k-for-a-year?cp=1>.
17. Dai W., Berleant D. Benchmarking contemporary deep learning hardware and frameworks: a survey of qualitative metrics. arXiv.org. URL: <https://arxiv.org/abs/1907.03626>.
18. Games market reports and forecasts. Newzoo. URL: <https://newzoo.com/games-market-reports-forecasts>.
19. Hardware survey. Unbiased hardware comparisons. URL: <https://technical.city/en/hardware-survey?tab=cpu>.
20. Machkovech S. Evidence continues to mount about how bad Denuvo is for PC gaming performance. Ars Technica. URL: <https://arstechnica.com/gaming/2018/12/evidence-continues-to-mount-about-how-bad-denuvo-is-for-pc-gaming-performance/>.
21. Papadopoulos J. Denuvo server issues prevented players from playing Batman: Arkham Knight, Mad Max & Shadow of War. DSOGaming. URL: <https://www.dsogaming.com/news/denuvo-server-problems-prevented-players-from-playing-batman-arkham-knight-mad-max/>.

22. Papadopoulos J. Square enix removes denuvo anti-tamper tech from life is strange: before the storm. DSOGaming. URL: <https://www.dsogaming.com/news/square-enix-removes-denuvo-anti-tamper-tech-life-strange-storm/>.

23. Plunkett L. PC game removes denuvo DRM before it even launches. Kotaku. URL: <https://kotaku.com/pc-game-removes-denuvo-drm-before-it-even-launches-1847332999>.