УДК 004.056.53 https://doi.org/10.30837/IYF.PCEIP.2024.113

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ЦИФРОВОГО КОНТЕНТУ: DRM І ТЕХНОЛОГІЯ DENUVO

Лісняк Д.С.
Науковий керівник – асист. Гвоздьов Р.Ю.
Харківський національний університет радіоелектроніки, каф. БІТ,
м. Харків, Україна
e-mail: danylo.lisniak@nure.ua

The rapid evolution of the distribution of digital content has led to the need to create reliable mechanisms for protecting intellectual property from unauthorised access and distribution. This article examines two main methods of protecting digital content: Digital Rights Management (DRM) and Denuvo technology. DRM acts like a set of locks and keys, controlling who can access digital content and what they can do with it. Denuvo, on the other hand, serves as a sophisticated defence against unauthorised access and piracy, especially in the gaming industry. This article is dedicated to figuring out how to make sure that digital content remains secure in a world where sharing and copying is easy.

Існує загальновідома думка, що захист авторських прав є надмірно обмежувальним, але з огляду на той факт, що кожного разу, коли хтось завантажує цифровий контент, захищений авторськими правами, замість того, щоб купляти право на використання цифрового продукту, несанкціоновано копіюють, використовують та розповсюджують такі продукти [1]. Не варто забувати і про ігрову та кіноіндустрію, які втрачають мільярди доларів через піратство. Технології управління цифровими правами (DRM) здатні захистити цифровий контент і обмежити його використання.

DRM (Digital Rights Management) – це технологія, яка захищає цифрові авторські права шляхом управління та обмеження доступу до цифрових носіїв, захищених авторським правом [2, 3]. Програмне забезпечення DRM також містить у собі різні заходи проти несанкціонованого копіювання, розповсюдження та зміни зазначених матеріалів, захищених авторським правом. Технологія захисту DRM дає видавцям і творцям повний контроль над тим, хто може отримати доступ до їхнього контенту і що вони можуть з ним робити. DRM захищає IP-адреси і запобігає крадіжці та незаконному розповсюдженню їхніх робіт в Інтернеті. Хоча DRM не бореться і не переслідує тих, хто займається піратством, він насамперед запобігає потраплянню цифрового контенту у відкритий доступ.

Також варто розглянути використання DRM на мобільних пристроях, які є невід’ємною частиною сучасних технологій. Можливість використовувати DRM на мобільних телефонах забезпечує повну безпеку контенту. OMA DRM – це механізм DRM, визначений Open Mobile Appliance. Мобільний DRM

спроектований таким чином, щоб зберігати контроль над медіа-об'єктами. Він може керувати використанням контенту, даючи змогу розробляти нові функції для кінцевих користувачів і різні види послуг мобільного контенту для розробників послуг, постачальників контенту, постачальників послуг і операторів.

DRM захист часто зіштовхується з критикою, наприклад за наступними пунктами. Незручність для користувачів: DRM завдає незручностей законним користувачам. Дана технологія обмежує передачу контенту з одного пристрою на інший, обмін контентом з членами сім'ї та створення резервних копій. Проблеми сумісності: системи DRM можуть спричиняти проблеми сумісності між різними пристроями, програмними платформами та екосистемами. Контент, захищений однією системою DRM, може бути недоступний на пристроях або в програмному забезпеченні, які не підтримують цей формат DRM. Потенційна невдача: якщо компанія, що захищає контент за допомогою DRM, збанкрутує або припинить підтримку системи DRM, користувачі не зможуть отримати доступ до придбаного контенту. Таке вже траплялося в минулому, внаслідок чого споживачі залишалися без доступу до своїх електронних бібліотек.

В якості прикладу системи DRM, можна розглянути Denuvo –програмне забезпечення DRM, крім того, це рішення захисту для ігрової індустрії, яке не дає змоги людям зламувати та розповсюджувати ігри, а також виявляє та блокує шахраїв у багатокористувацьких іграх [4]. Перш за все, Denuvo не є системою захисту від несанкціонованого доступу. Розробники повинні інтегрувати свій код із Denuvo, включно з маркуванням функцій, які не впливають на продуктивність, але є важливими для обфускації Denuvo. Наприклад, це може бути функція, що ініціалізує ядро програми. Її слід запускати тільки один раз, тому її уповільнення не вплине на загальну продуктивність.

На перший погляд, це проміжне програмне забезпечення для захисту від шахрайства, яке аналізує ігрові файли та читерські інструменти, встановлені на комп'ютері. Як і багато інших античит-програм, Denuvo Anti-Cheat використовує драйвери рівня ядра. Іншими словами, коли Denuvo працює, він має найвищий рівень привілеїв, який тільки може мати програмне забезпечення, крім ядра операційної системи.

Список використаних джерел

1. Gvozdov Roman et al. "Method of Biometric Authentication with Digital Watermarks." 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T). IEEE, 2021.

2. «What is Digital Rights Management (DRM)?», Conor Roach, May 2023.

3. «A Publishers Guide to DRM: What Is DRM, How It Works, and When Publishers Need It», Video Technology, April 2023, посилання на джерело: https://target-video.com/what-is-drm/

4. «What Is Denuvo and Why Do Some Gamers Hate It?», Debarshi Das, April 2023, посилання на джерело: https://www.makeuseof.com/what-is-denuvo/