УДК 004.056.5:347.77

Пуздрановський І.В.
Салієва О.В.

АНАЛІЗ СУЧАСНИХ DRM-СИСТЕМ КЕРУВАННЯ ЦИФРОВИМИ ПРАВАМИ

Вінницький Національний Технічний Університет

Анотація

В даній статті розглянуто сучасні системи управління цифровими правами. Наведено їх особливості, переваги та недоліки. Здійснено порівняння проаналізованих систем управління цифровими правами.

Ключові слова: Захист, інформація, цифрові активи

Abstract

This article discusses modern digital rights management systems. Their features, advantages and disadvantages are given. A comparison of the analyzed digital rights management systems was made.

Key words: Protection, information, digital assets.

Вступ

У зв'язку із розширенням кількості медіа інформації в мережі Інтернет зростає актуальність проблеми захисту авторських прав медіа файлів. Кількість джерел медіа інформації постійно збільшується, але не всі дотримуються правил авторського права, таким чином виникає проблема захисту авторами свого медіа контенту. Для вирішення цієї проблеми було розроблено спеціальні системи, які дозволять захисти авторську власність. В даній статті розглядаються сучасні DRM-системи керування цифровими правами, їх особливості, переваги та недоліки.

Дослідження

Цифровий актив – це, як правило, все, що створюється та зберігається в цифровому вигляді, що можна ідентифікувати та виявити, і має або надає цінність. Цифрові активи стають більш популярними та цінними, оскільки технологічний прогрес є частиною нашого особистого та професійного життя. Дані, зображення, відео, письмовий вміст тощо давно вважаються цифровими активами з правами власності [1].

Управління цифровими правами (DRM) – це спосіб захисту авторських прав для цифрових медіа, різними засобами для контролю або запобігання поширенню цифрових копій через комп'ютерні або телекомунікаційні мережі. Цей підхід передбачає використання технологій, які обмежують копіювання та використання захищених авторським правом творів і патентованого програмного забезпечення [2].

У певному сенсі, керування цифровими правами дозволяє видавцям або авторам контролювати дії користувачів відносно їх творів. Для компаній запровадження керування цифровими правами або процесів може допомогти запобігти доступу користувачів або використанню певних активів, дозволяючи організації уникнути юридичних проблем, які виникають через несанкціоноване використання. Сьогодні DRM відіграє все більшу роль у безпеці даних.

З розвитком однорангових служб обміну файлами, таких як торрент-сайти, онлайн-піратство стало вагомою проблемою для матеріалів, які захищені авторським правом. Технології DRM не відслідковують тих, хто займається піратством. Натомість вони взагалі унеможливлюють крадіжку або поширення вмісту даних.

У більшості випадків керування цифровими правами містить коди, які забороняють копіювання, чи коди, які обмежують час або кількість пристроїв, на яких можна отримати доступ до певного продукту.

Видавці, автори та інші творці вмісту використовують програмні засоби або системи, які шифрують медіа, дані, електронну книгу, вміст, програмне забезпечення чи будь-який інший матеріал, захищений авторським правом. Тільки ті, хто має ключі розшифрування, можуть отримати доступ до матеріалу.

Існує багато способів захисту вмісту, програмного забезпечення чи продукту. DRM може використовувати такі види захисту:

– Обмеження або заборона користувачам редагувати або зберігати вміст матеріалів.

– Обмеження або заборона користувачам ділитися або пересилати продукт або вміст матеріалів.

– Обмеження або заборона користувачам друкувати вміст матеріалів. Деякі документи або ілюстрації можна надрукувати лише обмежену кількість разів.

– Заборона користувачам створювати знімки екрана вмісту матеріалів.

– Встановлення для документа чи носія терміну дії, після якого користувач більше не матиме до нього доступу. Це також можна зробити, обмеживши кількість використань, які має користувач.

– Блокування доступу лише до певних IP-адрес, місць або пристроїв.

– Водяні знаки на творах мистецтва та документах, щоб встановити право власності та особу.

Керування цифровими правами також дозволяє видавцям і авторам отримувати доступ до журналу людей і часу, коли використовувався певний медіа, контент або програмне забезпечення.

Традиційні засоби керування цифровими правами можуть спричинити певні труднощі. Деякі з них обмежені типами файлів, які вони підтримують (наприклад, захист лише файлів Office і PDF). Інші мають негнучку структуру, яка потребує постійного клієнта, що ускладнює впровадження та діє як перешкода для співпраці [3].

Widevine DRM – це технологія ліцензування та шифрування DRM надана Alphabet, яка широко використовується Google Chrome, Brave, Firefox та багатьма іншими як система захисту вмісту. Окрім комп'ютерів, вона також захищає вміст даних на пристроях Android, Android TV і Chromecast.

Особливості Widevine DRM:

– Захист вмісту: ширше охоплення споживчих пристроїв і попередньо інтегровані платформи захисту вмісту.

– Відтворення відео: вдосконалений відеопрогравач HTML5 із високоякісним потоковим передаванням, QoS і доступністю на кількох пристроях.

– Одноразове шифрування: вміст зашифрується один раз за допомогою Widevine DRM і передається через надійні відеоконтейнери галузі, такі як MP4 і WebM.

Seclore – це розробка рішень для керування корпоративними цифровими правами (EDRM). Її архітектура DRM розроблена для керування системами безпеки вмісту корпоративного рівня. EDRM від Seclore автоматично додає мікро-цифрові права на файли та вміст під час їх завантаження, спільного користування або використання в іншому місці.

Особливості Seclore:

– Просте керування. Центр управління дозволяє легко керувати політиками використання, дозволами користувачів, захищеними файлами та журналами активності на одній інформаційній панелі.

– Захист одним клацанням миші: встановлюються автоматичні або ручні методи захисту для файлів одним клацанням миші.

– Легка автентифікація: інтегрована система федерації ідентифікації дозволяє користувачам швидко автентифікуватися за допомогою SSO, соціальних мереж і веб-каталогів.

– Системи DLP: попередньо інтегровані системи запобігання втраті даних для автоматичного захисту файлів, виявлених DLP.

LockLizard – це система, що забезпечує надійний захист документів від копіювання, яка використовує надійне шифрування та технологію відкритих ключів для захисту документів.

Особливості LockLizard:

– Підтвердження копіювання: захист документів від копіювання автоматично вимикає функції редагування та спільного використання на пристроях користувача, щоб запобігти несанкціонованому доступу до документа.

– Механізм самознищення: автоматичне закінчення терміну дії доступу до документа на основі конкретних переглядів, відбитків, днів або фіксованої дати.

– Динамічні водяні знаки: друк водяних знаків на документі за для запобігання його зміні навіть під час доступу неавторизованих користувачів.

– Блокування розташування: контроль BYOD і місця, де використовуються документи, за допомогою регіонального блокування розташування LockLizard.

CaseLabs – це система, яка надає хмарні послуги ліцензування DRM для всесвітнього цифрового відеовмісту. Сервіс DRM, відомий як DRMToday, надає мільярди ліцензій щомісяця, охоплюючи мільйони пристроїв щодня [4].

Особливості CaseLabs:

– Глобальне охоплення: міжрегіональні сервери AWS, які мають високу масштабованість і низьку затримку.

– Швидке ліцензування: швидкісна мережа DRMtoday дозволяє мінімізувати стандартний час доставки ліцензії для клієнтів у будь-якій точці світу.

– Онлайн-панель інструментів: проста для розуміння інтерфейсна панель інструментів, яка дозволяє керувати діями ліцензування та відстежувати їх.

– Зручність VideoPlayer: попередньо інтегрована з діапазоном інтелектуальних SDK для відтворення PRESTOplay від CastLabs; також працює зі сторонніми рішеннями.

У таблиці 1 здійснено порівняння проаналізованих DRM.

Таблиця 1 – Порівняння досліджуваних DRM

DRM	Widevine DRM	Seclore	LockLizard	CaseLabs
Сфера	Для всіх користувачів	Корпративна		
Платформи	– PC – Android – Android TV – Chromecast	– PC – Android – WEB	PC	WEB
Зручність	Немає ніяких інструментів, що забезпечують зручність користування	– Керування дозволами та захистом з одної панелі – Швидка автентифікація за допомогою SSO	– Зручний інтерфейс – Швидкість роботи	– Глобальне охоплення – Швидке ліцензування – Онлайн-панель інструментів – Зручність VideoPlayer
Тип контенту	Відео	Всі дані	Документи	Відео
Види захисту	– Шифрування – Вдосконалений відеопрогравач	– Шифрування – Керування доступом – Система запобігання втрати даних	– Регіональне блокування – Захист від копіювання – Водяні знаки – Захист від знімків екрану	– Шифрування – Вдосконалений відеопрогравач – SDK – Контроль використання
Вид зберігання	Пристрій користувача	Сервера компанії	Пристрій користувача	Хмара

Усі проаналізовані DRM охоплюють власну сферу і забезпечують захист різними методами, тобто кожна система призначена під конкретну задачу і під потреби користувачів.

Висновок

Підводячи підсумки даного дослідження, можна однозначно стверджувати, що в наш час захист авторських прав на цифрові активи є надзвичайно важливим і для реалізації даного захисту існує безліч методів та засобів. DRM-системи управління цифровими правами об’єднують в собі ці методи та засоби, щоб максимального захистити дані від порушення авторського права. Використовуючи DRM автори запобігають проблемі розвитку піратства в мережі інтернет, яка призводить до збитків як матеріального, так і репутаційного характеру.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. FRANKENFIELD J. Digital Assets [Електронний ресурс] / JAKE FRANKENFIELD. – 2022. – Режим доступу до ресурсу: https://www.investopedia.com/terms/d/digital-asset-framework.asp.

2. Digital rights management [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://www.britannica.com/topic/digital-rights-management.

3. Conor Roach. What is Digital Rights Management (DRM)? [Електронний ресурс] / Conor Roach. – 2023. – Режим доступу до ресурсу: https://www.digitalguardian.com/blog/what-digital-rights-management.

4. Програмне забезпечення для керування цифровими правами (DRM) у 2022 році [Електронний ресурс] – Режим доступу до ресурсу: https://techukraine.net/12-

%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B5-%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F-%D0%B4%D0%BB%D1%8F-%D0%BA%D0%B5%D1%80%D1%83%D0%B2%D0%B0%D0%BD%D0%BD/.

Пуздрановський Ілля Володимирович – студент групи КІТС-19б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: ilia.puzdranovskuy@gmail.com

Науковий керівник: ***Салієва Ольга Володимирівна*** – доктор філософії (PhD) за спеціальністю 125 «Кібербезпека», старший викладач кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: salieva8257@gmail.com

Puzdranovskyi Illia V. – student of KITS-19b group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail ilia.puzdranovskuy@gmail.com

Supervisor: ***Saliieva Olha V.*** – Doctor of Philosophy (PhD) in 125 "Cybersecurity", Senior Lecturer, Department of Management and Security of Information Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: salieva8257@gmail.com