УДК 004

М.Скрипка, магістр гр. КН-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОГО КЕРУВАННЯ ЦИФРОВИМИ ПРАВАМИ НА ОСНОВІ DRM

У статті розроблено програмне забезпечення, яке призначено для системи інтелектуального керування цифровими правами на основі DRM. Метою розробки є дослідження та принципи побудови системи інтелектуального керування цифровими правами на основі DRM. Об'єктом дослідження є процес інтелектуального керування цифровими правами на основі DRM. Предметом дослідження є методи інтелектуального керування цифровими правами на основі DRM. Методи дослідження базуються на методах захисту інтелектуальної власності, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи інтелектуального керування цифровими правами на основі DRM. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

інтелектуальне керування цифровими правами, DRM

Постановка проблеми. Управління цифровими правами (DRM) стосується алгоритмів та процесів, створених для забезпечення дотримання авторських прав під час споживання цифрового контенту. Без DRM кінцевий користувач може легко скопіювати ваш контент. Цей процес зазвичай називають піратством. Таким чином, це необхідно в архітектурі онлайн-розповсюдження відео, але споживач не бачить цього.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-10] було виявлено певні прогалини у забезпеченні системи інтелектуального керування цифровими правами на основі DRM.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи інтелектуального керування цифровими правами на основі DRM.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем інтелектуального керування цифровими правами на основі DRM.

– Дослідження системи інтелектуального керування цифровими правами на основі DRM.

– Програмна реалізація системи інтелектуального керування цифровими правами на основі DRM.

Об'єктом дослідження є процес інтелектуального керування цифровими правами на основі DRM.

Предметом дослідження є методи інтелектуального керування цифровими правами на основі DRM.

Методи дослідження базуються на методах захисту інтелектуальної власності, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Розмір ринку управління цифровими правами стрімко зростав останніми роками. Він зросте з 6,66 млрд доларів у 2025 році до 7,94 млрд доларів у 2026 році зі сукупним річним темпом зростання (CAGR) 19,2%. Зростання за історичний період можна пояснити розширенням споживання цифрових медіа, зростанням розповсюдження онлайн-контенту, збільшенням випадків цифрового піратства,

впровадженням моделей ліцензування програмного забезпечення, розвитком потокових сервісів.

Очікується, що ринок управління цифровими правами швидко зростатиме протягом наступних кількох років. У 2030 році він зросте до 15,95 мільярда доларів США зі складним річним темпом зростання (CAGR) 19%. Зростання в прогнозований період можна пояснити зростанням попиту на безпечне цифрове розповсюдження, зростаючим впровадженням управління правами на основі блокчейну, розширенням платформ іммерсивного цифрового контенту, зростанням інвестицій у передові технології шифрування, посиленням регуляторної уваги до захисту інтелектуальної власності. Основні тенденції в прогнозований період включають зростання впровадження хмарних рішень DRM, зростання попиту на технології захисту контенту, зростаючу інтеграцію DRM зі потоковими платформами, розширення моделей контенту на основі підписки, посилену увагу до боротьби з піратством.

Ринок управління цифровими правами зростає через зростання проблем безпеки. Широке використання ПК та ноутбуків приваблює хакерів, які шукають несанкціонованого доступу до корпоративних та урядових мереж, прагнучи викрасти критично важливу інформацію для фінансової та бізнес-вигоди. Корпорації все частіше застосовують підходи до управління бізнес-даними в режимі реального часу, включаючи передачу та зберігання на мобільних пристроях, хмарі, USB-накопичувачах та дисках. Як повідомляє InfoSecurity, прогнозується, що глобальні збитки від програм-вимагачів у 2023 році перевищать 30 мільярдів доларів, що підкреслює зростаючу загрозу. Складність та витонченість кібератак посилюють труднощі виявлення. Управління цифровими правами також застосовується організаціями охорони здоров'я та фінансових послуг для забезпечення дотримання стандартів конфіденційності та захисту даних, таких як HIPAA та Закон Гремма-Ліча-Блайлі. Очікується, що ця зростаюча стурбованість безпекою стимулюватиме зростання ринку в секторі управління цифровими правами.

Великі компанії на ринку управління цифровими правами зосереджуються на розробці інноваційних рішень, таких як послуги з управління цифровими правами, для встановлення авторства та контролю прав використання. Служба управління цифровими правами (DRM) – це технологія, призначена для захисту та регулювання розповсюдження та використання цифрового контенту, запобігання несанкціонованому доступу, копіюванню або обміну медіафайлами, такими як музика, відео або електронні книги. Наприклад, у липні 2024 року Wacom Co., Ltd., японська компанія-розробник програмного забезпечення, яка виробляє графічні планшети та пов'язані з ними продукти, запустила нову послугу управління цифровими правами. Ця послуга DRM від Wacom Co., Ltd. забезпечує покращений захист цифрового контенту, особливо корисна для творчих професіоналів, забезпечуючи безпечний доступ і контроль використання художніх творів і дизайнів. Вона включає безперебійну інтеграцію з пристроями Wacom, що спрощує обмін контентом і співпрацю, а також захищає інтелектуальну власність за допомогою надійних інструментів шифрування та керування дозволами.

У квітні 2024 року американська компанія-розробник програмного забезпечення Agora, Inc., що спеціалізується на комунікаційних програмних рішеннях, співпрацювала з EZDRM для впровадження рішень для управління цифровими правами (DRM), призначених для захисту контенту в прямому ефірі. Це партнерство має на меті підвищити безпеку контенту в прямому ефірі, забезпечуючи захист у режимі реального часу для прямих трансляцій шляхом безперешкодної інтеграції інтерактивної платформи мовлення Agora з надійною технологією DRM EZDRM. Ця інтеграція забезпечує безпечну доставку контенту, запобігаючи несанкціонованому доступу або піратству під час прямих трансляцій. EZDRM – це американська компанія, яка надає послуги з управління цифровими правами як послугою (DRMaaS).

Північна Америка була найбільшим регіоном на ринку управління цифровими правами у 2025 році. Очікується, що Азіатсько-Тихоокеанський регіон буде найшвидше зростаючим регіоном у прогнозований період. Ринок управління цифровими правами

включає доходи, отримані суб'єктами господарювання від надання таких послуг, як ліцензії на програмне забезпечення та ключі, протоколи автентифікації користувачів та IP-автентифікації, проксі-сервери, віртуальні приватні мережі (VPN), регіональні обмеження або геоблокування. Ринкова вартість включає вартість пов'язаних товарів, що продаються постачальником послуг або включені до пропозиції послуг. Враховуються лише товари та послуги, що продаються між суб'єктами господарювання або кінцевим споживачам.

Ринкова вартість визначається як доходи, які підприємства отримують від продажу товарів та/або послуг на визначеному ринку та в певній географічній зоні через продажі, гранти або пожертви у валюті (у доларах США, якщо не зазначено інше).

Доходи для певної географічної області – це споживчі значення, що представляють собою доходи, отримані організаціями у певній географічній області на ринку, незалежно від того, де вони виробляються. Вони не включають доходи від перепродажу вздовж ланцюга постачання, як далі вздовж ланцюга постачання, так і як частину інших продуктів.

Музика в Інтернеті

Крім стандартних підходів DRM, деякі магазини пропонують DRM-схему підписки. Наприклад, сервіс Sony Music Unlimited або онлайн музичний магазин Napster. Користувачі можуть завантажувати і прослуховувати необмежену кількість музики доти, поки діє підписка. Однак із закінченням підписки всі файли перестають відтворюватися.

У зв'язку з тим, що схеми DRM у різних виробників відрізняються між собою, іноді стає неможливим програвати музику від різних виробників на одному пристрої (пристрій може просто не підтримуватися DRM-схемою). Рішенням подібних проблем займаються, наприклад, в Англії. Так Ендрю Гауерс склав список пропозицій по поліпшенню політики захисту авторських прав (англ. Gowers Review of Intellectual Property), що містить 54 пункту. Цей список перебуває у відкритому доступі, і ознайомитися з ним може будь-який бажаючий. Серед всіх інших виправлень пункти з 8 по 12 містять пропозиції по створенню деяких виключень для сумлінного використання авторських прав, наприклад, бібліотеками (розглядається можливість переходити від однієї схеми DRM до іншої). Згодом планувалося ввести подібні виключення й для звичайних користувачів. Взагалі проблема з різними DRM у програвачах стояла досить гостро, наприклад, Apple відмовилися від DRM-захисту в музиці повністю, завдяки чому музика з iTunes програється спокійно на будь-якому пристрої, що підтримує формат AAC. Деякі магазини, наприклад, німецький Musicload, також оголосили про відмову від DRM, тому що з'ясувалося, що 3 з 4 дзвінків у їхню службу підтримки надходило від незадоволених DRM-користувачів. [17]

Телевізійні програми

Ця концепція була розроблена компанією Fox Broadcasting в 2001 році й була підтримана MPAA і Федеральним Агентством по зв'язку (ФАС) США. Однак у травні 2005 року Апеляційний Суд США ухвалив, що ФАС не має достатню владу для накладення подібних обмежень на телеіндустрію в США.

Куди більшого успіху ця система домоглася, коли була прийнята Проектом Цифрового Відео Віщання – консорціумом, що включає більше 250 вещателів, виробників, операторів мережі, розроблювачів програмного забезпечення й керуючих органів більше 35 країн. Цей консорціум намагався розробити нові цифрові стандарти для DRM у телемовленні. Одним з найбільш перспективних стандартів є варіант із поліпшеним прапором передачі, розроблений для європейського телебачення DVB-CPCM (DVB Content Protection and Copy Management, укр. захист умісту й керування копіюванням). Цей стандарт був наданий на розгляд європейським урядам в 2007 році. Всі нормативні частини на даний момент уже схвалені для публікації Керівною Радою DVB і будуть опублікований ETSI як офіційний європейський стандарт ETSI TS 102 825-X (X – номер підрозділу). На сьогоднішній день ще ніхто не взяв на себе забезпечення Сумісності й Надійності (англ. Compliance and Robustness) для даного стандарту (однак розробки в даному напрямку ведуться багатьма компаніями), що не дозволяє сьогодні впровадити цю систему повсюдно. [1]

У США постачальниками кабельного телебачення використовується стандарт CableCard, що обмежує доступ користувача тільки тими послугами, на які він підписаний.

Текст, документи, електронні книги

Керування цифровими правами на підприємстві – це застосування технологій DRM для керування доступом до корпоративних документів (файли Microsoft Word, PDF, AutoCAD, електронні листи, сторінки внутрішньої мережі інтранет). Ці технології, більше відомі як Керування Інформаційними Правами (англ. Information Rights Management), в основному використовуються для запобігання несанкціонованого використання документів, що є інтелектуальною власністю підприємства (наприклад, з метою промислового шпигунства або випадкового витоку інформації). Звичайно ця система убудована в програмне забезпечення системи керування вмістом, однак деякі корпорації (наприклад, Samsung Electronics) розробляють свої власні системи DRM.

Електронні книги, призначені для читання на ПК, мобільних пристроях або спеціальних «читалок», звичайно використовують DRM з метою обмежити копіювання, печатка або викладання книг у загальний доступ. Звичайно такі книги обмежені кількістю пристроїв, на яких їх можна прочитати, а деякі видавці взагалі забороняють будь-яке копіювання або печатку. Деякі компанії й оглядачі вважають, що наявність DRM створює безліч проблем для видання книг. [3]

Цикл шифрування

Щоб розпочати цикл «безпеки», зв’язок між програмним забезпеченням для кодування, що запитує, та сервером ліцензій шифрується.

Кожен сегмент шифрується відповідно до специфікації MPEG Common Encryption (CENC) для ISO-BMFF.

Що таке ISO-BMFF?

ISO-BMFF – це стандартизований формат файлів, який служить контейнером для аудіо- та відеоконтенту. Відомою реалізацією ISO-BMFF (і часто використовується як його синонім) є формат файлів MP4 або фрагментований MP4 (fMP4). У робочому процесі DRM мультимедійний контент шифрується, а контейнер ISO-BMFF покращується за допомогою метаданих та алгоритмів шифрування, специфічних для DRM.

Системи DRM використовують ISO-BMFF для зберігання та транспортування зашифрованих медіаданих і забезпечують пов'язання з ліцензією DRM. Коли користувачі намагаються отримати доступ до захищених медіаданих, система DRM перевіряє, чи має користувач на це право, залежно від пов'язаної ліцензії.

Коротше кажучи, це забезпечує безпечне зберігання, доставку та контроль цифрових медіафайлів у рамках DRM.

Сегменти можуть бути повністю зашифровані або частково зашифровані, коли шифруються лише деякі кадри або навіть лише частини кадрів.

Стандарт MPEG-CENC визначає, як шифрується сегмент, і відображає, який ключ дешифрування потрібно використовувати для якого сегмента (або його частин), пов'язуючи з ним ідентифікатор ключа. MPEG-CENC використовується для потоків DASH та HLS, якщо сегменти мають формат контейнера fMP4.

Стандартне шифрування контенту виконується за допомогою алгоритму Advanced Encryption Standard (AES) з використанням 128-бітних ключів. Залежно від використовуваної системи DRM, вона використовується або в режимі лічильника (CTR), або в режимі ланцюжка блоків шифрування (CBC).

Ці два режими відрізняються тим, як шифрується корисне навантаження.

Важливо зазначити, що шифруються лише необроблені аудіо- та відеодані в сегменті, а метадані, додані в контейнер, – ні.

Існує три основні постачальники DRM: Google Widevine, Apple FairPlay та Microsoft Playready.

Їхнє застосування може значно відрізнятися залежно від багатьох унікальних факторів – необхідність вибору постачальника, який відповідає потребам дистриб'ютора

контенту щодо доставки та відтворення (залежно від того, які пристрої підтримуються), може значно ускладнити процес впровадження DRM.

Для підвищення безпеки та зменшення ризику зворотного проектування систем DRM зазвичай немає чітких повідомлень журналу.

Фактично, частини процесу розглядаються як чорна скринька, і в результаті налагодження може бути ще складнішим на пристроях (наприклад, SmartTV або телеприставках) зі старими версіями програмного забезпечення DRM.

У браузері або операційній системі контент потім буде розшифровано модулем розшифрування контенту (CDM), який розшифровує кожен зашифрований аудіо- та відеосегмент.

Цикл дешифрування

Коли веб-плеєр ідентифікує контент, захищений DRM, він викликає процеси та інтерфейси, визначені розширеннями зашифрованого медіа (EME), які використовуються в браузерах для ініціювання процесу запиту ліцензії.

EME використовується для взаємодії з модулем розшифрування контенту (CDM), який реалізований у браузері та може покладатися або не покладатися на функції операційної системи, такі як HDCP.

Під час відтворення контенту, захищеного DRM, запити на ліцензію генеруються CDM та передаються програвачу через EME.

Всю роботу з розшифрування виконує CDM. Найголовніше, що розшифрований контент залишається в CDM – він не є і не повинен бути доступним для програмного забезпечення для відтворення, оскільки інакше можна було б створити розшифровані копії контенту.

Для відтворення захищеного контенту, після виявлення того, що контент захищений, програвач або програмне забезпечення для відтворення надсилає запит на ліцензію на сервер ліцензування.

Якщо ліцензія кешується локально, цей запит можна пропустити, і замість нього можна використовувати кешовану ліцензію.

Запит на ліцензію, що надсилається програвачем програмного забезпечення для відтворення, завжди містить метадані, які однозначно ідентифікують відтворюваний контент, а формат цих метаданих залежить від використовуваного DRM-рішення.

Ці метадані DRM можуть міститися або в маніфесті (наприклад, MPEG-DASH або вбудовані в HLS), або в конфігурації програвача, або в окремих сегментах.

Хоча це не є обов'язковою вимогою, запит зазвичай містить додаткові дані із пристрою, що запитує, такі як ідентифікатор, який можна використовувати для його унікальної ідентифікації.

Якщо надана вся обов'язкова інформація, сервер може надати ліцензію програвачу або програмному забезпеченню для відтворення з ключами розшифрування, необхідними для безпечного відтворення запитуваного контенту на клієнті.

Повернена ліцензійна угода може містити інформацію про необхідний рівень безпеки розшифрування контенту, наприклад: розшифрування контенту за допомогою програмного забезпечення значно менш безпечне, ніж розшифрування за допомогою апаратного забезпечення.

З точки зору гравця, отримання ліцензії за допомогою EME починається зі створення клієнтом відтворення так званого ключового сеансу. Використовуючи цей ключовий сеанс та метадані DRM, взяті з сегментів, маніфесту або інших джерел, гравець запускає процес запиту ліцензії за допомогою EME.

Потім CDM генерує підписане ключове повідомлення, яке програвач або програмне забезпечення для повернення коштів надсилає на сервер ліцензій.

Сервер ліцензій повертає запитувану ліцензію, а також приймає рішення про те, чи надано клієнту права на відтворення запитуваного контенту; якщо ні, відтворення зупиняється та відображається помилка.

Або ж сервер ліцензій може визначити, що, наприклад, програвач може відтворювати лише SD-версії контенту.

Якщо запит ліцензії був успішним, клієнт оновлює ключовий сеанс повернутою ліцензією.

Потім розшифрування контенту повністю обробляється CDM.

За деяких обставин ліцензія кешується на певний час і може бути використана для відтворення захищеного контенту офлайн (наприклад, Netflix).

Робочий процес дуже схожий для невеб-платформ, таких як нативні додатки для Android, iOS або tvOS. Кожна платформа має власний набір API, подібних до EME on Web, для взаємодії з базовою інтегрованою CDM.

Ліцензія та розшифровані дані не повинні бути доступні клієнтам, окрім користувача ліцензованого контенту.

Таким чином, закриті ключі та розшифровані дані зберігаються в безпечному середовищі в браузері, операційній системі або навіть на обладнанні (якщо підтримується), як-от у надійних середовищах виконання.

Використання різних форматів контейнерів, таких як fMP4 та MPEG-2 TS, ускладнювало розповсюдження однакового контенту на всіх платформах.

Однак швидке впровадження CMAF та стандартизація CENC серед виробників обладнання та розробників програмного забезпечення зменшують складність впровадження для галузі.

Хоча CMAF та CENC все ще дозволяють використання AES CTR та AES CBC, постачальники DRM поступово переходять до використання AES CBC.

Запобігання копіюванню контенту, захищеного авторським правом, у інших правовласників

Припустімо, ви розміщуєте онлайн-платформу відео на вимогу, яку можна використовувати для перегляду всіляких голлівудських фільмів. Власник прав на контент, який ви розповсюджуєте, не хоче, щоб ваші користувачі могли просто створювати копії цього контенту.

Таким чином, постачальник платформи може бути зобов'язаний за контрактом використовувати певну форму захисту контенту для дотримання прав власника прав на контент.

Це часто трапляється з мовниками, які не лише розміщують власний контент, але й, наприклад, транслюють прямі трансляції телепередач чи інші фільми чи серіали. Системи DRM можуть використовуватися для захисту контенту від незаконного копіювання користувачами цього сервісу.

Вибір найкращих DRM-сервісів

Існує кілька варіантів контролю доступу до вашого цифрового контенту, обмежуючи його лише авторизованими користувачами. Постачальники DRM пропонують рішення та послуги творцям контенту, видавцям та дистриб'юторам.

Вони спеціалізуються на розробці та впровадженні технологій, інструментів і систем, що забезпечують захист, розповсюдження та управління вашим цифровим контентом. Вони також забезпечують дотримання умов ліцензування та законів про авторське право.

Такі рішення, як шифрування, контроль доступу, управління ліцензіями, захист контенту та моніторинг, можуть бути надані хорошим партнером з DRM.

Набір послуг розробляємої системи інтелектуального керування цифровими правами на основі DRM виглядає так:

– Інтеграція системи DRM: Постачальники DRM інтегрують свої технології в існуючі платформи розповсюдження контенту, веб-сайти або потокові платформи, забезпечуючи безперебійну функціональність DRM та захист цифрового контенту.

– Шифрування контенту: Рішення для шифрування захищають цифровий контент від неавторизованих користувачів та онлайн-піратства. Гарний партнер застосує надійні

алгоритми шифрування для захисту вашого контенту під час зберігання, передачі та відтворення.

– Керування ліцензіями: Системи керування ліцензіями займаються створенням, видачею та керуванням ліцензіями DRM. Ці системи гарантують, що користувачі мають необхідні дозволи та права для доступу до вашого захищеного контенту.

– Забезпечення дотримання прав: ці механізми забезпечують дотримання прав використання, визначених ліцензіями DRM. Це може включати обмеження кількості пристроїв, на яких можна отримати доступ до вашого контенту, забезпечення обмеженого за часом доступу або контроль можливості копіювання чи обміну контентом.

– Аналітика та моніторинг: Постачальники DRM пропонують інструменти аналітики та моніторингу для відстеження використання контенту, виявлення потенційних порушень та збору інформації про поведінку користувачів.

Зрозуміло, що управління цифровими правами – це складна тема, до якої не існує універсального підходу. Але це невід'ємна частина відеороботу для кожного, хто хоче захистити або монетизувати свій цифровий відеоконтент. Це сфера постійного розвитку, оскільки ті, хто має намір займатися піратством, шукають нові способи обійти захист вашого контенту заради власної вигоди. У даній роботі система керування цифровими правами на основі DRM реалізується за рахунок використання методів стеганографії. Структурна схема розробленого програмного забезпечення представлена на рисунку 1. В якості даних, що вбудовуються може використовуватися будь-яка інформація: текст, повідомлення, невелике зображення тощо, які дозволяють підтверджувати та захищати авторські права. Роль контейнеру буде відігравати будь-яке кольорове цифрове зображення, яке потребує захисту у рамках забезпечення авторських прав, що задовольняє стандартним вимогам до контейнерів для стегоповідомлень.

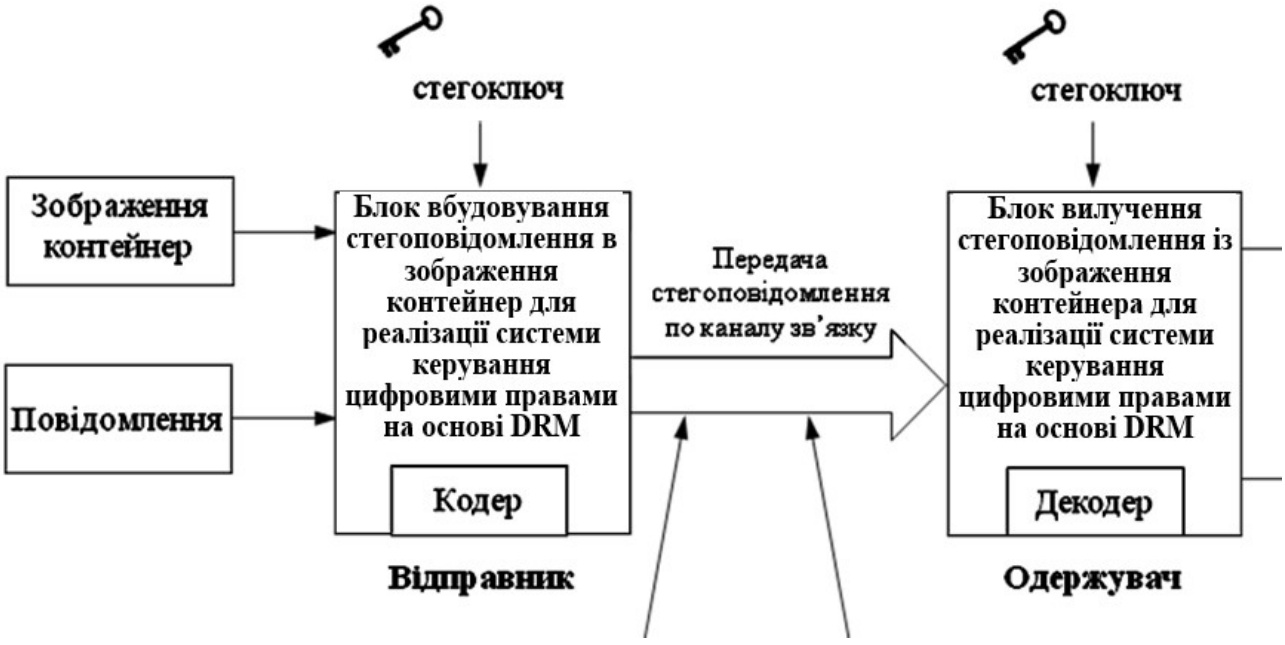

Рисунок 1 – Структурна схема системи

Стегоключ – секретний ключ, необхідний для приховування інформації. Залежно від кількості рівнів захисту (наприклад, вбудовування заздалегідь зашифрованого повідомлення) в стегосистемі може бути один або декілька стегоключів. Вбудовування повідомлення в зображення контейнер відбувається за допомогою стегокодера, який крім приховування інформації здійснює також і перешкодостійке кодування. Після цього зображення з прихованим повідомленням передається по каналу зв'язку, де може зазнавати атак зловмисників, а також викривлень інформації в наслідок перешкод у каналі зв'язку або застосувань алгоритмів стиснення з втратами. Вилучення повідомлення із зображення

контейнера здійснюється за допомогою стегодетектора. Стегодекодер перевіряє наявність прихованого повідомлення і в разі його існування, вилучає інформацію.

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів інтелектуального керування цифровими правами на основі DRM. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем інтелектуального керування цифровими правами на основі DRM.

– Досліджена система інтелектуального керування цифровими правами на основі DRM.

– На основі отриманих результатів досліджень створена програмна реалізація системи інтелектуального керування цифровими правами на основі DRM.

Розроблені алгоритми дозволяють успішно вирішувати завдання інтелектуального керування цифровими правами на основі DRM. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Kuznetsov, O., Smirnov, O., Akhmetov, B., Alimseitova, Z., Imoize, A.L. «Deep Learning Frontiers in Copy-Move Forgery Detection: Advances, Challenges, and Future Directions». Advancements in Cybersecurity Next Generation Systems and Applications, 2025. 202-229.
2. Lakhno, V., Malyukov, V., Smirnov, O., Bebeshko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». 8th International Symposium on Intelligent Informatics, ISI 2023, 2025. vol 389. pp 377-389. Springer, Singapore.
3. Kuznetsov, O., Smirnov, O., Mormul, M., Kotukh, Y., Zvieriev, V. «Comparative Research on Cryptocurrency Efficiency: An Objective Analysis of Key Metrics». International Journal of Computing 23(4), 2024. pp. 563-573.
4. Kuznetsov O., Frontoni E., Kuznetsova K., Smirnov O., Kostenko V. «Blockchain applications in metaverse environments: new horizons». Advanced Metaverse Wireless Communication Systems. pp. 255-293. 2024.
5. Kuznetsov, O., Frontoni, E., Chevardin, V., Smirnov, O., Imoize, A.L. «Advancing metaverse security with cryptographic innovations». Advanced Metaverse Wireless Communication Systems. pp 351-386. 2024.
6. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». CEUR Workshop Proceedings, 2024, 3909, pp. 227–241.
7. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 379–402.
8. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 403–447.
9. Ткаченко, О., Ільєнко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 2(26), С. 170–188.
10. Смірнова Т.В., Конопліцька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». Кібербезпека: освіта, наука, техніка. 2024. №4(24), С. 6-27.
11. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
12. Kuznetsov, O., Frontoni, E., Kandiy, S., Smirnova, T., Prokopov, S., Bilanovych, A. «New Cost Function for S-boxes Generation by Simulated Annealing Algorithm». Lecture Notes on Data Engineering and Communications Technologies, 2023. vol 180. pp. 310-320. Springer, Cham.
13. Kuznetsov, O., Frontoni, E., Kandiy, S., Smirnov, O., Ulianovska, Y., Kobylianska, O. «Heuristic Search for Nonlinear Substitutions for Cryptographic Applications». Lecture Notes on Data Engineering and Communications Technologies, 2023. vol 180. Springer, Cham. pp. 288-298.
14. Kuznetsov, O., Kuznetsova, Y., Smirnov, O., Kostenko, O., Zvieriev, V. «Evaluating Hashing Algorithms in the Age of ASIC Resistance». CEUR Workshop Proceedings, 2023, 3628, pp. 93-105.
15. Kuznetsov O., Frontoni E., Kuznetsova Ye., Smirnov O., Chevardin V. «Achieving Enhanced Security in

Biometric Authentication: A Rigorous Analysis of Code-Based Fuzzy Extractor». CEUR Workshop Proceedings, Volume 3624, 2023, pp. 330-339.
16. Smirnov, O., Sydorenko, V., Aleksander, M., Zhyharevych, O., Yenchev, S. «Simulation of the cloud IoT-based monitoring system for critical infrastructures». CEUR Workshop Proceedings, Volume 3530, 2023, pp. 256-265.
17. Kuznetsov, O., Kandiy, S., Frontoni, E., Smirnov, O. «Trade-offs in Post-Quantum Cryptography: A Comparative Assessment of BIKE, HQC, and Classic McEliece». CEUR Workshop Proceedings, Volume 3504, 2023, pp. 1-11.
18. Смірнов О.А. Козлов Я.О., Смірнова Т.В. «Дослідження застосування SIEM-систем для забезпечення кібербезпеки та захисту інформації». ІІ Міжнародна науково-практична Інтернет-конференція «Інновації та перспективні шляхи hозвитку інформаційних технологій (ІПШРІТ-2023)» м.Черкаси 6 грудня 2023 року – Черкаси: ЧДТУ.– 2023. – С.251-252.
19. Козлов Я.О., Смірнова Т.В., Смірнов О.А. «Дослідження SIEM-систем для забезпечення кібербезпеки». VII міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології" до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 26.
20. Козлов Я.О., Козірова Н.Л., Смірнов О.А. «Дослідження структури та принципу роботи SIEM-системи». VII міжнародна науково-практична конференція "Інформаційна безпека та комп'ютерні технології" до 30-ти річчя кафедри кібербезпеки та програмного забезпечення, м. Кропивницький. 1 листопада 2023 р. – Кропивницький: ЦНТУ. – 2023. – С. 59.
21. Вінтенко Б.Ю., Смірнов О.А., Коваленко О.В., Смірнов С.А., Коваленко А.С. «Дослідження нормативних документів та галузевих стандартів розробки програмного забезпечення комп'ютерних систем управління АЕС, важливих для безпеки». Системи управління, навігації та зв'язку, 2023, вип. 2(72), С. 170-178.
22. Смірнова Т.В., Гнатюк С.О., Бердибаєв Р.Ш., Сидоренко В.М., Жигаревич О.К., «Система корелювання подій та управління інцидентами кібербезпеки на об'єктах критичної інфраструктури». Кібербезпека: освіта, наука, техніка, №3(19), 2023, С. 176-196.
23. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,
24. Smirnov, O., Lakhno, V., Akhmetov, B., Chubaievskyi, V., Khorolska, K., Bebeshko, B. «Selection of a Rational Composition of İnformation Protection Means Using a Genetic Algorithm». In: Rajakumar, G., Du, KL., Vuppalapati, C., Beligiannis, G.N. (eds) Intelligent Communication Technologies and Virtual Mobile Networks. Lecture Notes on Data Engineering and Communications Technologies, vol 131. 2023. Springer, Singapore. pp. 21-34.
25. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». Journal of Ambient Intelligence and Humanized Computing Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.
26. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
27. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
28. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
29. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. «Вступ до кібербезпеки»: навчальний посібник – Кропивницький: ЦНТУ – 2022. – 968 с.
30. Теорія та практика сучасного інформаційно-психологічного протиборства: навчальний посібник / [В.М. Петрик, С.О. Гнатюк, М.М. Присяжнюк та ін.]; за заг. ред. С.О. Гнатюка, В.М. Петрика та О.А Смірнова. – Полтава, 2022. – 334 с.
31. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418
32. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260.