ЕЛЕКТРОНІКА

УДК 004.056.55:791.44.075
DOI https://doi.org/10.32838/2663-5941/2019.4-2/25

Очеретько О.Я.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Розорінов Г.М.
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

ТЕХНОЛОГІЇ РОЗПОВСЮДЖЕННЯ ТА ЗАХИСТУ ЦИФРОВИХ КІНОФІЛЬМІВ

Досліджено передумови та тенденцію розвитку цифрового кіно. Виявлено тенденції розвитку захисту цифрового кіно. Проаналізовано шлях проходження сигналу від сервера до проектора. Розглянуто основні принципи цифрового кіно. Детально розглянута система керування екраном, освітленням у кінотеатрі, звуковідтворювальною апаратурою кінотеатру. Виявлено та синтезовано необхідні передумови створення стандартів цифрового кіно. Розглядається робота консорціуму світових кіностудій, робочої групи з розробки інтернет-технологій і товариства інженерів кінематографії та телебачення та прийняті ними стандарти пов'язані з цифровим кіно. Розглядаються технології зберігання і поширення цифрових копій фільмів із використанням цифрових кінопакетів. Розкриваються структура цифрового кінопакету, особливості наповнення і можливості взаємодії між ними. Пояснюються поняття композиції, файлів доріжок і цифрових бобін. Розглядається структура композиції та функції кожної складової частини. Описується список композицій та її складники. Досліджено, які дії виконуються для захисту цифрових кінофільмів. Особлива увага приділяється проблемі запобігання несанкціонованому доступу та копіюванню фільмів. Пояснюються метод кодування Ключ-Довжина-Значення, який використовується в файлах, які містять сутність та метадані. Розглядається тип повідомлення «ключове повідомлення доставки» який використовується для передачі зашифрованих ключів. Аналізуються способи симетричного і асиметричного шифрування, їх застосування для забезпечення захисту кіноконтенту. Описується призначення повідомлення про отримання ключа та медіаблоку як елементів системи безпеки. Розглядається модель довіри та ключові аспекти її функціонування. Описано список довірених пристроїв, який входить до складу ключового повідомлення доставки. Розглядається коло довіри цифрового кіно як виявлення на якому етапі було порушено питання захисту.

Ключові слова: *захист, ключ, медіаблок, несанкціонований доступ, цифровий кінофільм, шифрування.*

Постановка проблеми. Кінематограф із моменту свого зародження використовував плівку для зберігання і демонстрації зображення. З плином часу її склад і структура змінювалася, на неї стали також записувати звук. Більше століття саме бобіни з кілометрами кіноплівки були носіями кінофільмів.

Але на початку XXI ст. технологічний прогрес дав змогу створити кінопроектор, здатний демонструвати зображення без використання плівки. Так настала епоха цифрового кіно. І хоч досі зйомка може здійснюватися як на плівку, так і цифрові камери, цифрові кінопроектори повністю витіснили своїх попередників. Це сталося з багатьох об'єктивних причин: цифрові фільмокопії не схильні до зносу, для їх демонстрації не потрібно кілька проекційних постів, набагато легше і дешевше виробляти цифрові копії фільмів і доставляти їх у кінотеатри по всьому світі.

Повністю змінилося обладнання кінотеатрів. Тепер десятки фільмів зберігаються на порівняно невеликих серверах замість величезних складів із бобінами, зображення на екрані формується мікродзеркальними або рідкокристалічними матрицями, а нові фільми поширюють на жорстких дисках або за допомогою захищеного супутникового каналу, або по мережі Інтернет.

Нові технології скасовували необхідність у старих стандартах плівкового кінематографу. Тому 20 липня 2005 р. консорціум провідних світових кіностудій Digital Cinema Initiatives (DCI) розробив нові стандарти, які встановлюють вимоги до всього кінообладнання, якості та формату зображення та звуку, способів їх збереження, поширення та захисту. Така стандартизація дає змогу студіям, виробникам обладнання, дистриб'юторам та кінотеатрам бути впевненими в повній сумісності всіх систем кінопоказу. Однією з задач DCI було обрати метод збереження фільмокопії. Таким методом стали цифрові кінопакети Digital Cinema Package (DCP). Цей пакет має відповідати суворим стандартам DCI для безболісного показу в усіх цифрових кінотеатрах.

Виклад основного матеріалу дослідження. DCP пакет являє собою складну впорядковану структуру, яка завдяки своїй гнучкості дає змогу зберігати в собі різні види інформації. Це «пакувальний ящик» для файлів, який може містити або не містити повний фільм. З іншого боку, цифровий кінофільм складається зі структурованого набору файлів, які називаються композицією. Композиція являє собою кінцевий продукт, який може складатися не тільки з кінофільму, але також трейлерів і рекламних оголошень.

Архітектуру композиції запропонували наприкінці 2001 р. Вона була відмінною від будь-якого формату засобів масової інформації, що використовувалася при поширенні в той час. Характерною рисою кінобізнесу є поширення кінофільмів у багатьох індивідуальних версіях, таких як версії з певним звуковим форматом, титрами, конкретним форматом зображення, однією або кількома мовами. Це зумовлено обмеженнями обладнання та необхідністю демонстрації фільмів у різних країнах. Архітектура композиції була розроблена для ефективного вирішення проблеми необхідності доставляти кілька версій фільму в кінотеатри, надаючи механізм для обміну файлами між ними.

DCP може містити одну або кілька композицій, або тільки часткову композицію. Якщо він складається з однієї або кількох композицій DCP називається композиційним пакетом (Composition Package). Якщо він складається з елементів композиції DCP, то він називається пакетом ресурсів (Asset Package). Крім того, в пакеті завжди присутній список (Packing List), в якому описані всі елементи, що містяться в цьому DCP [1].

Композиція складається з кількох файлів, а саме списку відтворення і файлів доріжок (Track Files). Для гнучкості і розширюваності кожен такий файл містить тільки один тип сутності (Essence), такий як зображення, звук або субтитри. Спосіб та послідовність відтворення файлів вказано у списку відтворення, який називається композиційним списком відтворення або CPL.

SMPTE визначає поняття «контент» як метадані та сутність. Сутність у цифровому кіно − це термін, який застосовується до однієї форми вираження, такої як зображення, звук або субтитри. Типи сутності є унікальними за своєю природою, тобто може бути тільки файл зображення з частотою 24 кадрів на секунду, тільки файл зображення з 48 кадрами на секунду, тільки файл із 3D-зображенням, тільки звукова доріжка у форматі 5.1, тільки звукова доріжка у форматі 7.1 і т.д. Використовуючи ці визначення, файл доріжки несе в собі один тип сутності плюс необхідні метадані, щоб полегшити його використання [2].

Незалежність сутнісних типів у композиції забезпечує високу ступінь розширюваності, даючи змогу в майбутньому вводити нові типи сутностей без порушення структури композиції. Наприклад, коли поняття «композиція» та «цифровий кіно пакет» були вперше введені у цифрове кіно, стереоскопічного 3D не було в планах. Але розширюваність композиції дала змогу швидко додати файл доріжки стереоскопічного зображення, коли з'явився цифровий 3D [3].

Файли доріжок запаковані у спеціальній версії формату обміну даними або MXF. MXF надає структурований метод для перенесення різних типів сутностей із метаданими. Хоча MXF здатний нести більш як один тип сутності в одному файлі, необхідно підкреслити, що для цифрового кіно прийнято використовувати тільки один тип сутності для кожного файлу. Обмеження, що застосовуються до MXF для упаковки цифрового кінозображення і звуку, визначені в SMPTE ST429-3 (файли доріжок звукового супроводу і зображення) [4].

Файли доріжок MXF складаються із заголовка, контейнера сутності і нижнього колонтитула. Заголовок містить метадані, що описують файл доріжки. Контейнер сутності несе саму сутність. Нижній колонтитул містить таблицю індексів сутностей [5].

Сутність зображення і звуку запакована з використанням технології KLV (Key-Length-Value) (рис. 1).

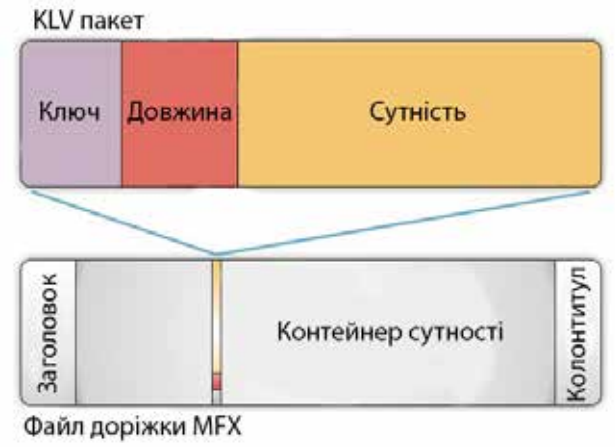

Рис. 1. Структура KLVпакета

Ключ (Key) визначає природу присутньої сутності. Довжина (Length) описує довжину поля з сутністю (Value). Саме поле сутності містить один кадр зображення або звук.

За визначенням, композиція повинна мати як мінімум три файли: композиційний список відтворення (CompositionPlayList), файл доріжки зображення і файл звукової доріжки [6]. Крім того, ці доріжки можна розділити на кілька файлів, що складаються з фрагментів цих доріжок, названих бобін (Reels). Назва «Бобіни» походить із часів плівкового кінопрокату, де фільм поставлявся у вигляді частин (кінострічки на бобінах). Це полегшувало фізичну доставку фільму. Також це давало змогу вносити зміни, замінюючи тільки одну бобіну, замість усього фільму, що могло знадобитися під час виправлення титрів або варіювання рекламних роликів. Аналогічним чином, у цифровому поширенні і виробництві можна домогтися високої ефективності в розбитті цифрового контенту на частини, а саме в організації композицій у вигляді набору «цифрових бобін».

На рис. 2 показана композиція, що складається з композиційного списку відтворення і чотирьох типів файлів доріжок (зображення, звук, субтитри і приховані субтитри), які організовані у вигляді двох цифрових бобін.

На практиці, композиція може містити до 100 файлів або більше. Кількість файлів доріжок може бути обмежена правилами шифрування. Часто існує кілька версій фільму. Для 3D-контенту, різних субтитрів, додаткових мовних звукових доріжок або фрагментів фільму з цензурою можуть знадобитися різні версії фільму. Для кожної має бути створена своя композиція. У композиції може бути лише по одній доріжці зображення, звуку, звичайних і прихованих субтитрів. Але при цьому дозволено обмінюватися файлами доріжок між композиціями. Наприклад, різні композиції, що представляють собою різні версії фільму, які призначені для поширення в різних країнах, можуть мати різні файли звукової доріжки, але один і той самий файл доріжки зображення (рис. 3).

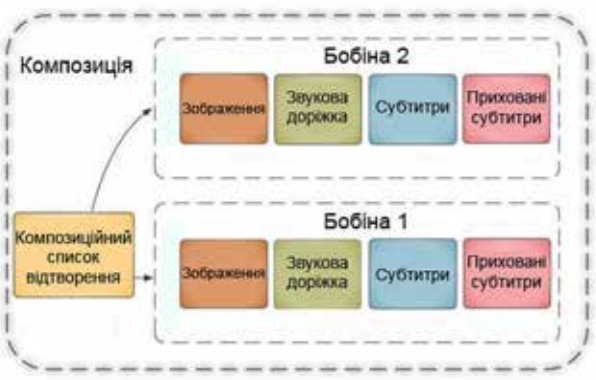

Рис. 2. Структура композиції

Рис. 3. Композиції для фільмів зі спільним зображенням, але з різними звуковими доріжками

Аналогічно, можна мати дві композиції з однаковою звуковою доріжкою і різними доріжками 3D- і 2D-зображення. Таким чином, можна поширювати багато версій фільму без необхідності відправки дублікатів файлів доріжок.

Оскільки один DCP пакет може містити кілька композицій, а самі композиції можуть спільно використовувати одну і ту саму сутність, ми можемо мати кілька різних версій фільму в одному пакеті (рис. 4).

Але бажано, щоб різні версії фільму поширювалися як окремі DCP пакети. У таких випадках батьківська композиція буде містити повну версію фільму і буде створена одна або кілька дочірніх версій композиції, які будуть спільно використовувати певні файли доріжок батьківської композиції. Коли всі композиційні списки відтворення та сутності присутні в загальному сховищі даних,

система відтворення матиме все необхідне для відтворення кожної з версій фільму. Але при цьому у DCP пакеті з дочірньою композицією будуть присутні не всі файли, які необхідні для відтворення. Для правильного управління розподілом батьківських і дочірніх композицій необхідний механізм.

Рис. 4. Дві версії фільму в спільному DCP пакеті

На практиці батьківській композиції присвоюється ярлик «Оригінальної версії» (Original Version), який переноситься у власний DCP пакет (рис. 5).

Кожній дочірній композиції присвоюється ярлик «Файл версії» (Version File), і він також переноситься у власний DCP пакет. Коли батьківський пакет ОВ і пов'язані дочірні пакети ФВ завантажуються до сервера цифрового кіно, всі файли, необхідні для відтворення різних композицій, будуть присутні і готові до відтворення.

Обидва способи розподілу призводять до однакового результату, даючи змогу відтворювати різні композиції, а отже, різні версії фільму.

Ще однією важливою задачею DCI було обрати метод захисту фільмів від несанкціонованого доступу і копіювання. Для цього використовуються два методи шифрування: симетричне і асиметричне.

Згідно з симетричним методом, дані шифруються і розшифровуються одним і тим самим ключем. Уявімо тепер, що фільм у форматі DCP зашифрований саме таким способом, і необхідно показати його в кінотеатрі. Фільм відправляється в кінозал, і навіть якщо його перехоплять пірати, то відкрити ніяк не зможуть, адже він зашифрований. Але відразу виникає проблема передавання ключа. Адже його можуть перехопити так само, як і фільм. Ключ можна передавати при особистій зустрічі. Але тоді для кожного з тисяч кінотеатрів світу доведеться особисто привозити ключ. Це абсолютно не зручно. У цьому і полягає головна проблема симетричного шифрування.

Асиметричний метод передбачає використання пари ключів − публічного і приватного. Основний сенс алгоритму полягає в тому, що отримувач генерує цю пару ключів. Відправник отримає публічний ключ, на його основі шифрує інформацію, після чого розшифрування можливе тільки отримувачем і тільки його приватним ключем, який зберігається в секреті. Обидва ключі пов'язані між собою складною односторонньою математичною функцією, і на основі відкритого ключа ніяк не можна отримати приватний. Для кращого розуміння асиметричного алгоритму можна навести дуже простий приклад, який відобразить всю суть цього методу. Уявімо, що в нас є фільм, який треба передати в кінотеатр. Працівники кінотеатру над-

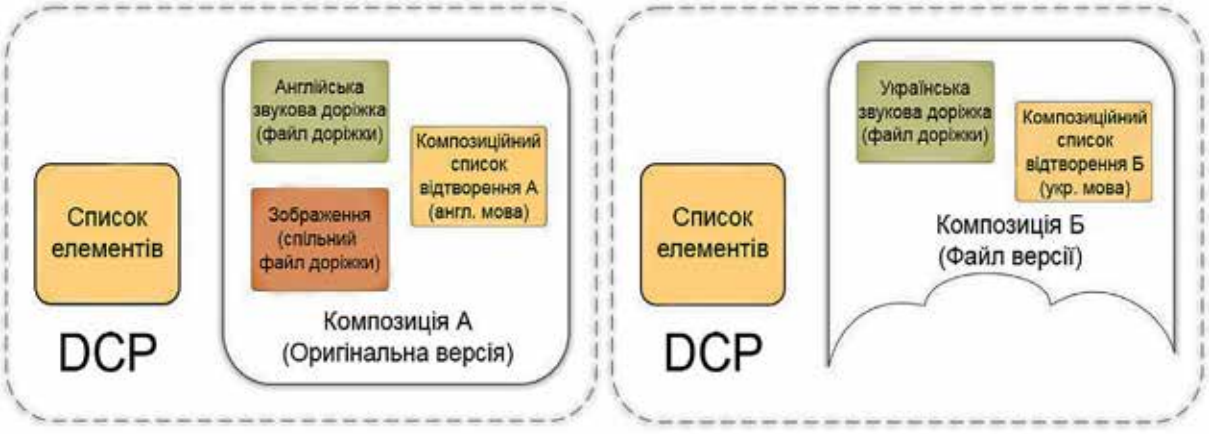

Рис. 5. Дві версії фільму в окремих DCP пакетах

силають нам звичайний замок, ключ від якого є тільки у них. Ми кладемо носій із нашим фільмом у кейс і замикаємо його цим замком. Тепер ніхто, крім співробітників кінотеатру, не зможуть відімкнути кейс, адже ключ є тільки в них. Замок у цьому випадку − публічний ключ, а ключ від нього – приватний [7].

Тож стандарт DCI передбачає захист контенту за допомогою обох способів шифрування. Кожен виробник медіаблоків або серверів для кожної конкретної моделі генерує 2 сертифікати за стандартом X.509, публічний і приватний, і маркує їх серійним номером. Приватний сертифікат вшивається глибоко в надра системи, де дістати його неможливо, а публічний можна отримати, надіславши запит до виробника. Розширення таких сертифікатів .pem або .crt.

Спочатку DCP шифрується звичайним симетричним ключем, а вже сам цей ключ зашифровується асиметричним алгоритмом на основі публічного сертифіката необхідного нам сервера або медіаблоку. Симетричний ключ від нашого DCP, який зашифрований таким асиметричним алгоритмом, називається Key Delivery Message (KDM). Далі цей KDM відсилається в кінотеатр електронною поштою і завантажується до сервера, де він уже на основі приватного сертифіката медіаблоку або сервера розшифровує симетричний ключ від нашого фільму [8].

Під час генерації KDM також вказується часовий період, протягом якого можна розшифровувати DCP пакет. Після закінчення цього часу показ буде неможливий до завантаження нового KDM, із новими датами. Це робиться спеціально для того, щоб творці фільму могли регулювати показ у кінотеатрах. Також існує Distribution KDM − технічно звичайний KDM, тільки згенерований для обладнання по мастерингу DCP. Призначений він для того, щоб дистриб'ютори могли розшифровувати на своєму обладнанні фільм і вносити будь-які правки.

У процесі шифрування композицій зашифровуються тільки файли доріжок. Вони можуть бути вибірково зашифровані, коли деякі файли доріжок шифруються, а інші − ні. На практиці рішення, що стосуються шифрування, залишаються на вибір власника контенту. Наприклад, власник контенту може зашифровувати тільки зображення і не чіпати звукові або текстові файли. Коли файл доріжки зашифрований, вся сутність у файлі зашифрована, вона не може бути частково зашифрованою. Композиційний список відтворення (CPL) не зашифровується.

Алгоритм шифрування, який використовується в цифровому кіно, − це відомий симетричний алгоритм розширеного шифрування (Advanced Encryption Algorithm, AES). У цифровому кіно використовується 128-бітний ключ. У процесі шифрування сутність у кожному файлі доріжки зашифрована за допомогою унікального ключа. Кожен із файлів доріжок не може використовувати один і той самий ключ. KDM містить зашифровану версію кожного ключа для кожного з файлів доріжок.

Шифрується тільки сутність пакета KLV. Метадані, пов'язані з сутністю, відкриті, щоб їх можна прочитати при пошуку в файлі. Це також дає змогу оператору відтворювати файл доріжки з будь-якого кадру, тобто робити перемотку. Пакет KLV із зашифрованою сутністю запаковується в інший «спеціальний» пакет KLV разом із пов'язаними з ним криптографічними метаданими. «Спеціальний» пакет KLV просто містить зашифрований контент, не знаючи характеру його вмісту. Далі він запаковується в файл доріжки MXF так само, якби шифрування не проводилося зовсім [9] (рис. 6).

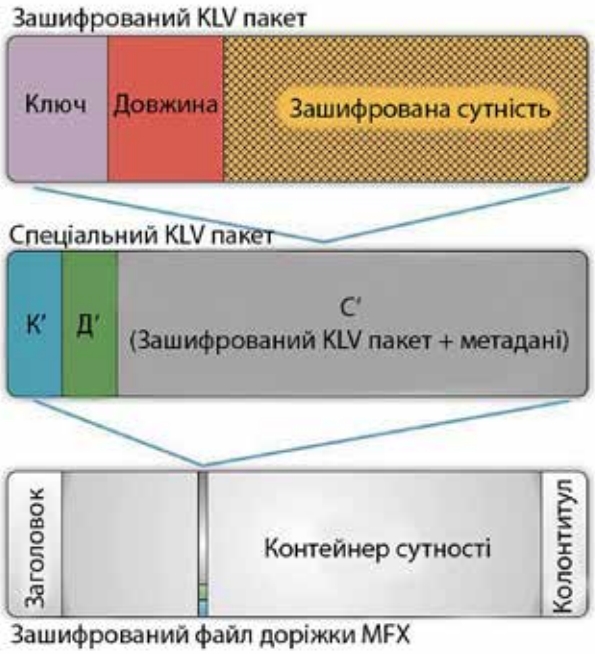

Рис. 6. Структура зашифрованого KLV пакета

Для надійного захисту використовують так звану модель довіри. Метою моделі довіри є мінімізація кількості суб'єктів, яким варто довіряти, щоб зберегти бізнес інтереси. Модель довіри дає змогу високо цінувати вміст, що поширюється по всьому світу без обтяжень у виконанні та показах.

На ранніх етапах виробництва кінематографа керують власники прав, де є довіра. Однак

розподіл кінофільмів, як правило, здійснюється поза межами права власника прав. Тому для забезпечення надійного середовища в дистрибуції потрібний особливий розгляд. Типова модель робочого процесу високого рівня для кінофільмів наведена нижче. Цікавим є питання поділу сфер впливу дистрибуції та показу.

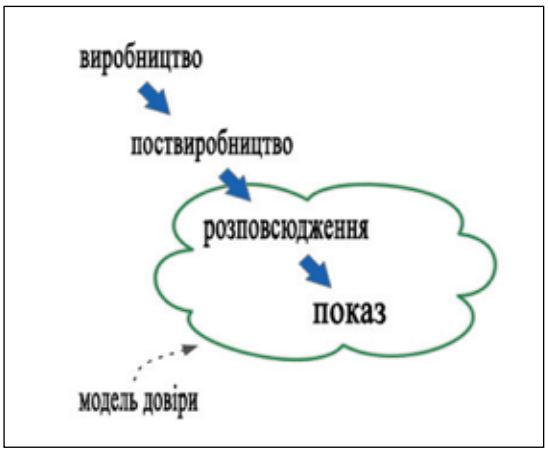

Рис. 7. Область, у якій працює модель довіри

Довіра забезпечується шляхом шифрування вмісту цифрового кінематографа та керування ключами безпеки, які дають змогу відтворювати вміст. З практичних причин корисно шифрувати один раз та поширювати для багатьох користувачів. Але також бажано обмежити, де відтворюється зашифрований вміст, даючи змогу відтворювати в кожному окремому місці або на екрані за принципом «бізнес-вимоги власника прав».

Модель довіри до цифрового кіно дає змогу закрити цей відкритий цикл довіри через журнал безпеки цифрового кіно. Журнал створює модель робочого процесу «Коло довіри», як показано нижче.

Рис. 8. Структурна схема кола довіри цифрового кіно

Захист фільмів у кінотеатрі забезпечує медіаблок. Він містить всі необхідні елементи обробки в межах захищеної зони для формування зображення і звуку, а також елементів інтерфейсу за межами захищеної зони. Структура медіаблоку показана на рис. 9.

Медіаблок складається з таких елементів [10]:

– система керування показом (SMS). Система керування показом забезпечує керування медіаблоком, як за допомогою призначеного для користувача інтерфейсу, так і машинного управління;

– безпечна зона обробки (SPB). Для обробки зображення і звуку SPB має відповідати Федеральним Стандартами Обробки Інформації США

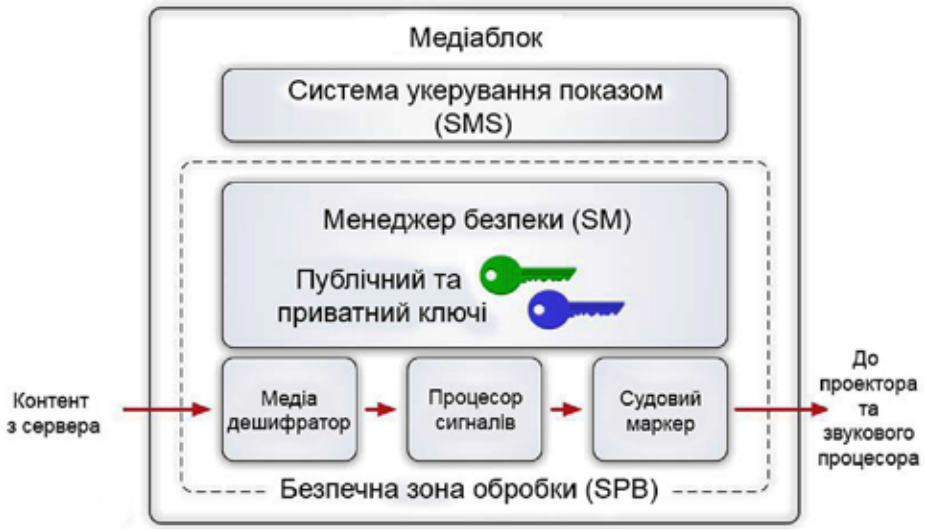

Рис. 9. Структура медіаблоку

(FIPS) 140-2 Level 3, а також відповідати вимогам DCI. Згідно зі специфікацією, для обробки зображення і звуку SPB має бути захищена від несанкціонованого доступу. Наприклад, фізичне втручання повністю зітре всі ключі;

– менеджер безпеки (SM). Елемент медіаблоку, який відповідальний за дані системи безпеки і політики безпеки. Це автономна підсистема, що має власний процесор і захищену операційну систему;

– медіа-дешифратор. Медіа-дешифратор розшифровує зашифровану сутність файлу доріжки, використовуючи публічний ключ медіа блоку;

– процесор сигналів. Обробка зображень, що включає декомпресію JPEG 2000 і обробку звуку в разі використання системи зі складним багатоканальним звуком;

– судовий маркер. Специфікація DCI вимагає використовувати судове маркування, але його використання не є обов'язковим для власників контенту. Інформація визначається DCI і включає в себе інформацію про місцезнаходження і час доби;

– захищений годинник. Він захищений від несанкціонованого доступу і має резервне живлення. Він потрібен для визначення поточної дати/часу.

– Коли була вперше представлена концепція медіаблоку, передбачалося, що існуватимуть кілька типів медіаблоків, такі як окремі мультимедійні блоки для зображення і звуку. Наприклад, DCI часто посилається на медіаблок для зображення (IMB) в його специфікації. Однак на практиці виробники воліють обробляти якомога більше типів сутностей в одному медіаблоці. У результаті IMB, як правило, є єдиним медіаблоком, який можна знайти в більшості цифрових систем кіно.

Вміст може бути зашифрований під час входу в медіаблок, а на його виході бути вже розшифрованим. Така схема можлива лише тоді, коли медіаблок встановлений всередині проектора (Integrated Media Block) і піддається процесу сполучення з проектором. Якщо створення пари між IMB і проектором підроблено з метою отримати доступ до незашифрованого зображення, це викличе процес захисту від несанкціонованого доступу в межах медіаблоку.

Висновки. З огляду на вищезазначене, Digital Cinema Initiatives має досить складну, але водночас структуровану систему збереження, захисту і поширення цифрового кіноконтенту. Концепція DCP пакетів є досить універсальною і гнучкою, що дає змогу без великих зусиль використовувати нові типи сутностей та з легкістю маніпулювати ними задля створення різноманітних версій фільмів.

Система захисту DCP пакетів демонструє велику надійність, що підтверджується відсутністю випадків крадіжок оригінальних файлів кіноконтенту ані під час поширення, ані з серверів кінотеатрів. Водночас зловмисники іноді крадуть фільми із серверів кінокомпаній та дистриб'юторів, що вказує на незначну потужність системи захисту кіноконтенту на етапі постпродукції. Існують і так звані CamRip версії фільмів, що є наслідком слабкого контролю за глядачами в деяких кінотеатрах.

Список літератури:

1. SMPTE ST429-2 DCP Operational Constraints. URL: http://ieeexplore.ieee.org/document/7290915/
2. SMPTE ST 390-2011 MXF Pattern "OP-Atom". URL: http://ieeexplore.ieee.org/document/7290732/
3. SMPTE ST 429-10 DCP Stereoscopic Picture Track File. URL: http://ieeexplore.ieee.org/document/7292178/
4. SMPTE ST429-3 Sound and Picture Track File. URL: http://ieeexplore.ieee.org/document/7291560/
5. SMPTE ST 377 MXF File Format Specification. URL: http://ieeexplore.ieee.org/document/7292073/
6. SMPTE S429-7 Composition Playlist. URL: http://ieeexplore.ieee.org/document/7291923/
7. Современные алгоритмы шифрования. URL: https://www.bytemag.ru/articles/detail.php?ID=6645
8. SMPTE ST430-1 Key Delivery Message (KDM). URL: http://ieeexplore.ieee.org/document/7290381/
9. SMPTE ST429-6 MXF Track File Essence Encryption. URL: http://ieeexplore.ieee.org/document/7291629/
10. Eric Diehl. Securing Digital Video: Techniques for DRM and Content Protection.Springer Science & Business Media, 2012. 266 c.

Ocheretko O.Y., Rozorinov H.M. DIGITAL MOVIE DISTRIBUTION AND PROTECTION TECHNOLOGIES

The preconditions and tendency of digital cinema development has been investigated. The tendencies of development of protection of digital cinema has been revealed. The path of signal passing from the server to the projector has been analyzed. The basic principles of digital cinema has been considered. The screen

control system, lighting in the cinema, sound reproduction equipment of the cinema has been considered in detail. The necessary prerequisites for the creation of digital cinema standards has been identified and synthesized. The work of the consortium of world film studios, the working group on the development of Internet technologies and the society of engineers of cinematography and television and the standards adopted by them related to digital cinema has been considered. The technologies of storage and distribution of digital copies of films using digital cinema packages has been considered. The structure of the digital cinema package, the features of filling and possibilities of interaction between them has been revealed. The notion of composition, track files and digital bobbin has been explained. The composition structure and functions of each component has been considered. The list of songs and its components has been described. Actions that was taken to protect digital movies has been explored. Particular attention to preventing unauthorized access and copying of films has been paid. The key-length-value encoding method used in files containing the essence and metadata has been explained. The type of message "key delivery message" used to transfer encrypted keys has been considered. The methods of symmetric and asymmetric encryption, their application for protection of cinema content has been analyzed. The purpose of the message about the receipt of the key and the Media Block as elements of the security system has been described. A model of trust and key aspects of its functioning has been considered. The list of trusted devices that is part of the key delivery message has been described. The range of digital cinema credibility is considered, as well as revealing at what stage security issues has been raised.

Key words: *defence, key, media-block, unauthorized division, digital movie, encryption.*