ДОСЛІДЖЕННЯ ВБУДОВАНИХ МЕТОДІВ ЗАХИСТУ МУЛЬТИМЕДІЙНОГО КОНТЕНТУ ЕЛЕКТРОННИХ ВИДАНЬ

***Нерода Т.В.**, к.т.н., професор, кафедра АКТ, УАД*
***Фіялка Д.**, студент, кафедра АКТ, УАД*

Важливість захисту цілісності та автентичності мультимедійного контенту освітніх електронних видань виявляється в численних аспектах. Захист цілісності дозволяє уникнути неправомірних змін чи втрат даних, що може виникнути через віруси, зловмисне програмне забезпечення або несанкціоновані втручання та академічну недоброчесність, гарантуючи стабільність та надійність освітніх послуг та забезпечуючи користувачам достовірний та правдивий контент в університетській он-лайн бібліотеці [1]. На сьогодні цілісність та автентичність мультимедійного контенту електронних видань стають критичними факторами у попередженні плагіату та забезпеченні точності даних, особливо при відновлення друкованих видань в електронному виді [2]. Тому актуальним є дослідження шляхів збереження цілісності та автентичності мультимедійного контенту електронних видань, що визначається потребою у вірогідності та коректності інформації в різних контекстах.

Окремі засоби захисту мультимедійного контенту є наперед вбудованими у певні формати електронних видань. **EPUB** (Electronic Publication), будучи одним з популярних форматів електронних книг, підтримує захист авторських прав за допомогою технології DRM (Digital Rights Management). Це дозволяє обмежувати доступ і використання контенту, наприклад, копіювання або друку, в залежності від прав власника. У для цього формату передбачена технологія Readium LCP (Licensed Content Protection) для захисту від крадіжки та незаконного копіювання для електронних книг. Також IDPF (International Digital Publishing Forum) розробляє стандарти для електронних книг EPUB, що зокрема включають засоби захисту та безпеки.

Формат **PDF** (Portable Document Format) підтримує вбудовані засоби безпеки, такі як шифрування та паролі для обмеження доступу до вмісту. Деякі версії PDF також підтримують технології DRM для захисту авторських прав. Розширений **Interactive PDF** може включати вбудовані мультимедійні елементи та функції захисту, такі як цифрові підписи. Формат **AZW** (Amazon Kindle Format) підтримує технології захисту DRM, які використовуються Amazon для контролю за доступом до електронних книг. Удосконалений AZW3 для читачів Amazon Kindle також підтримує технології DRM для контролю за доступом та використанням контенту. Формат **Topaz**, який використовується в продуктах Amazon, таких як Kindle, підтримує захист авторських прав.

Формат, який використовується для електронних книг у програмі **iBooks** (Apple iBooks Format) на пристроях Apple, також може включати захист авторських прав. **PDB** (PalmDOC), використовуваний для електронних книг на пристроях Palm, та **LIT** (Microsoft Reader eBook Format), використовуваний Microsoft Reader, також підтримує технології DRM і інші заходи для контролю за використанням контенту.

MOBI (Mobipocket eBook Format) використовується для електронних книг і підтримує технології захисту власності, такі як DRM. Це дозволяє контролювати використання електронних книг, забезпечуючи авторські права. Відкритий формат для електронних книг **Fb2** (FictionBook) не має вбудованих засобів DRM, але може бути захищений відокремленими засобами DRM під час розповсюдження. **Hpub** (HTML5 Publication) є форматом для електронних видань, який використовує HTML5. Він надає механізми включення засобів захисту, такі як обмеження доступу, авторизацію та шифрування. Виходячи зі стандартів ePUB3, деякі інтерактивні та мультимедійні електронні книги можуть використовувати покращені можливості захисту, такі як шифрування та управління правами, що розширює захист контенту.

Деякі спеціалізовані формати електронних видань також цільово оснащувались загальними і пропрієтарними алгоритмами захисту контенту. Так, формат **Folio Infobase** (Folio Views) використовується для створення електронних довідкових систем та баз даних. Він може включати засоби захисту, такі як обмеження доступу до конкретних розділів, шифрування та інші засоби безпеки. Формати **CBZ**, **CBR, CBL** (Comic Book Archive) для електронних коміксів, можуть включати вбудовані засоби захисту, наприклад, обмеження та контроль доступу або шифрування. Формати **CBT** (Computer-Based Training), спрямовані на навчання та тренування, можуть включати засоби захисту для контролю доступу до навчального матеріалу.

Деякі електронні книги реалізовані у форматі виконуваних файлів (**EXE**) із вбудованими методами захисту, такі як шифрування або обмеження доступу. Додаткові заходи безпеки можуть включати використання захищених програмних середовищ для читання електронних книг, які контролюють доступ і використання контенту. Формат **DNL** (Desktop Author) теж призначений для роботи на комп'ютерах і не обмежений конкретними платформами. Його можна використовувати на різних системах, таких як настільні та ноутбуки, що працюють під керуванням різних операційних систем, таких як Windows або macOS. Він застосовується для електронних книг та підтримує певний рівень безпеки для контенту, щоб обмежити несанкціонований доступ і використання. Використання шифрування для захисту вмісту від несанкціонованого доступу.

Розглянуті методи захисту можуть комбінуватися в залежності від конкретної реалізації програмного забезпечення, яке використовується для компіляції цифрових підручників. Результати виконаного дослідження рекомендуються застосовувати при захисті конфіденційності, цілісності та автентичності мультимедійного контенту електронних освітніх видань у хмарному сховищі вузівської бібліотеки, збережених у розглянутих форматах.

Список літератури

1. Фіялка, Д., & Сербан, В. (2023). Інтеграція системи управління контентом в університетський інформаційний простір. Сучасні інформаційні системи та технології, (6), 54-57.

2. Коханівський, О.П. (2015). Мультимедійні технології відновлення друкованих видань в електронному виді : навч. посіб. Київ: НТУУ «КПІ».