з експертною підтримкою / Л.С. Сікора, Н.К. Лиса, Р.С. Марцишин, Ю.Г. Міюшкович // Моделювання та інформаційні технології. - К. ІПМЕ. 2013. – Вип. 68. – С.133-140.
9. *Сікора Л.С., Лиса Н.К., Марцишин Р.С., Міюшкович Ю.Г.* Інформаційно – експертна модель формування факторів забруднення техногенного середовища та аналіз – хімічних ефектів для розробки сенсорів концентрації / Сікора, Н.К. Лиса, Р.С. Марцишин, Ю.Г. Міюшкови // ЗНП, Інститут проблем моделювання в енергетиці. - К. ІПМЕ. 2013. – Вип. 67. – С.129-137.

Поступила 10.04.2017р.

УДК 621.3

О.Б. Полусин [1], аспірант УАД, О.В. Тимченко [1, 2], д.т.н., професор,
В.І. Сабат [1], к.т.н., доцент

СУЧАСНІ МЕТОДИ ЗАХИСТУ МУЛЬТИМЕДІЙНОЇ ІНФОРМАЦІЇ

Анотація. В статті розглянуті методи за допомогою яких здійснюється захист мультимедійних даних та об'єктів авторського права та інтелектуальної власності. Досліджуються елементи методів захисту. Визначається необхідність застосування одиничного чи комплексного методів для здійснення більш надійнішого захисту інформації мультимедіа.

Ключові слова: мультимедійні дані, захист мультимедійної інформації.

Вступ. Комп'ютерна техніка та інформаційні технології з кожним новим днем закріплюється на нових вершинах розвитку. Сюди ми можемо віднести розвиток окремих комплектуючих комп'ютера, до яких входять, процесори, материнські плати, навіть пристрої для зчитування даних, розвиток мереж, які об'єднують домашні і офісні комп'ютери в глобальні мережі, швидкість передачі даних в яких неймовірно збільшується.

Вперше мережа з'явилась для полегшення та прискорення обміном інформації між Стенфордським університетом та університетом штату Юта. Метою даного впровадження був і залишається по сьогоднішній день обмін інформацією.

Звісно нововведення спочатку не набуло досить великих масштабів і нараховувало у своїй мережі всього кілька десятків комп'ютерів, але з часом мережа збільшувалась, кількість користувачів, що прагнули отримати доступ до різноманітної інформації в різних цілях зросла, вони почали під'єднуватись до загального кола користувачів. На даний момент інформаційні потоки в сучасному світі досягли неймовірно великих масштабів, що дозволяє отримати

[1], Українська академія друкарства
[2] Uniwersytet Warmińsko-Mazurski w Olsztynie

 © О.Б. Полусин, О.В. Тимченко, В.І. Сабат

довільну інформацію з мережі, у будь-якому зручному вигляді, з кожної точки планети де є вільний доступ до глобальної мережі Інтернет. Найновіші новини з різних куточків світу, книги, набрані в текстових редакторах чи озвучені як аудіокниги, зображення картин та пейзажів, наукові відкриття та новітні розробки - все це можна зараз отримати безоплатно за лічені хвилини за допомогою пошуку у всесвітній мережі Інтернет.

Поряд із розвитком Інтернету та технологій передавання постало питання щодо захисту як персональних даних, так і захисту даних мультимедіа. Мультимедіа – комбінування різних форм представлення інформації на одному носієві, наприклад текстової, звукової і графічної, або, останнім часом все частіше – анімації і відео [1]. Отже, оскільки в наш час будь-яка інформація може бути перетворена в довільний формат, необхідним стає захистити дані, які можна використати без згоди автора чи власника, чим нанести йому шкоду. Фільми, музика, картини, презентації, статті, наукові роботи та багато інших матеріалів, що являються об'єктами авторського права та інтелектуальною власністю, стають об'єктами посягання людей для отримання вигоди, завдання збитків чи використання у власних цілях.

Захисту мультимедійних даних слід приділити багато уваги, тому що з кожним роком росте шкода, що завдається через ненадійні засоби та методи захисту, що застосовуються, до таких можна віднести як правову так і програмно-апаратну частини.

Дослідження, що проводились в останні роки, які пов'язані з захистом мультимедійних даних, спрямовані на впровадження методів, що дозволять захистити об'єкти авторського права та інтелектуальної власності і до яких на даний час можна віднести присвоєння ідентифікаційних кодів типу ISBN чи DOI, електронно-цифрового підпису, криптографічне шифрування, web-дипозитарії та найпоширеніший метод, що досліджується і має досить велику актуальність - цифровий водяний знак (ЦВЗ).

Постановка проблеми. У зв'язку з широким поширенням глобальної мережі та надшвидким розвитком інформаційних технологій, будь-яка особа, що володіє відповідними знаннями та програмно-апаратними елементами, може безперешкодно заволодіти мультимедійними даними у власних цілях. Зазвичай дані дії здійснюються з метою розповсюдження та отримання винагороди методами копіювання, використання та розповсюдження продукції авторського права. Великі зусилля, що здійснюються для запобігання несанкціонованого використання мультимедійних даних не являються марними, оскільки впровадження все новіших та вдосконалених методів захисту показує позитивні результати, які на жаль все ще являються не достатньо універсальними та не достатньо надійними.

Метою статті є дослідження існуючих методів захисту мультимедійних даних та захисту від копіювання мультимедійної інформації.

Виклад основного матеріалу. У сьогоденні, щоб отримати певну електронну інформацію з корпоративної чи глобальної мереж потрібно виконати ряд маніпуляцій за допомогою програмних елементів. Саме на

першому етапі використання необхідного програмного забезпечення, найпоширенішого компанії Microsoft, Microsoft Windows, часто є порушенням авторських прав та права інтелектуальної власності. Причина полягає в простій ліцензійній угоді, в більшості випадків використання даного програмного продукту ліцензія відсутня. Сама компанія бореться з так званим комп'ютерним піратством різноманітними шляхами [2]. Якщо брати ринок розповсюдження інформаційних технологій лише в Україні станом на 2015 рік частка неліцензійного програмного забезпечення лише компанії Microsoft досягла 82% [3]. Поряд з тим є велика кількість програмного забезпечення, що використовується без ліцензійної угоди і порушує авторські права.

Розглянемо які саме методи використовуються найчастіше для запобігання несанкціонованого використання даних мультимедіа, піратства та збереженні авторських прав та прав інтелектуальної власності.

Засоби та методи шифрування чи кодування відомі з давніх часів і призначення їх аналогічне, тобто захист інформації від зовнішнього втручання чи несанкціонованого використання. Поряд з тим різні методи мають різну мету. Наприклад, метод криптографії, являється найпоширенішим методом шифрування інформації кодуванням для забезпечення безпеки інформації. Протилежним за метою до криптографії можна віднести метод стенографії, завдання якої це приховати факт існування шифрованої чи кодованої інформації. Поряд з тим, використання комбінації цих двох методів дозволить підвищити ефективність захисту даних мультимедіа чи будь-якого об'єкта авторського права.

На першому етапі необхідно зрозуміти, який саме метод чи комбінацію методів захисту необхідно обрати для мультимедійних даних, що потребують забезпечення авторського права. Кількість методів є незначною, але за призначенням вони поділяються на певні категорії:

Ідентифікаційний код ISBN (міжнародний стандартний номер книги) – це універсальний ідентифікаційний номер, що присвоюється книзі або брошурі з метою їх класифікації. Тобто, даний метод, присвоєння коду книзі чи брошурі, використовується для забезпечення авторського права друкованих видань і дозволяє визначити певні дані з присвоєного коду. Сам код складається з 10 або 13 цифр (ISBN 5-02-013850-9). Десятизначний номер поділяється на чотири частини, в той час тринадцятизначний на п'ять, шляхом додавання префіксу 978. Перша цифра – це ідентифікатор мовної групи чи країни. Даний ідентифікатор встановлюється Міжнародним агентством ISBN, наприклад, для англомовних країн ідентифікатор рівний 0 або 1. Для України та країн групи СНД присвоєно ідентифікатор 5. Окрім цього Україна має свої окремі ідентифікатори 966 та 617. Цифри у другій частині - це ідентифікатор видавництва, що призначає національне агентство ISBN, для визначення яким видавництвом було здійснено тираж. Ідентифікатор книги, що знаходиться в третій частині коду, вказується з метою регулювання кількості книг чи брошур. Останню частину в даному коді можна вважати ключовою, оскільки тут знаходиться контрольна цифра,

завдяки якій можна перевірити правильність присвоєного коду.

ISAN – номер розроблений на Міжнародній конференції товариств авторів і композиторів, що дозволяє ефективно захистити фільми та інші аудіовізуальні твори. Саме цей ідентифікатор слід використовувати для більшої надійності в комбінації з іншими методами, найчастіше для боротьби з відео та аудіо піратством. Відмінність ідентифікатора ISAN від ISBN, що застосовується лише для друкованих видань, полягає в тому, що перший застосовується зазвичай для аудіовізуальних творів чи баз даних і застосовується за допомогою комп'ютерних програм. До можливих застосувань відносять: аудіовізуальну каталогізацію, допомога при зборі товариств в управлінні правами, скоротити несанкціоноване використання захищеного контенту. Номер ISAN має вигляд 0000-0000-3A8D-0000-Z-0000-0000-6, та дозволяє ідентифікувати лише роботу, тобто кінофільм, серіал, окремі епізоди чи трейлери, але він не ідентифікує публікацій чи правовласників.

Цифровий ідентифікатор DOI – серійний номер, що використовується для постійної і унікальної ідентифікації об'єктів будь-якого типу. Саме цей ідентифікатор можна назвати унікальним, через його можливості відслідковувати об'єкт авторського права, навіть коли зміниться його URL адреса та застосування його з різними об'єктами мультимедійних даних. Ідентифікатор DOI складається з трьох елементів, де перший елемент це сама директорія doi (наприклад http://dx.doi.org/), другий елемент префікс, що має вигляд 10.XXXX(X) та за допомогою якого можна ідентифікувати видавця, а третій - суфікс bc.000027, що дозволяє ідентифікувати публікацію і являється індивідуальним для кожної публікації.

Електронно-цифровий підпис (ЕЦП) - це блок інформації, який додається до файлу даних автором та захищає файл від несанкціонованої модифікації і вказує на власника підпису. Для роботи цифрового підпису, необхідно два ключі захисту: 1) особистий ключ, який зберігається у автора; 2) відкритий ключ, який знаходиться у загальному доступі. Сам ЕЦП може використовуватись як фізичними, так і юридичними особами з метою ідентифікації власника і підтвердження цілісності даних, що зберігаються в електронній формі. Використання електронно-цифрового підпису являється ефективним методом забезпечення безпеки інформації на різних рівнях використання: від персональних даних певної особи до інформаційної безпеки держави в цілому. Як було вказано, ЕЦП складається з двох ключів. Особистий ключ формується унікальною послідовністю випадкових чисел довжиною 264 біти. Другий ключ, відкритий, обчислюється вже з відомого особистого ключа і служить лише для перевірки ЕЦП документів, що отримані. У відкритому ключі також вказується персональна інформація про власника, реєстраційний номер, термін дії сертифікату відкритого ключа.

Найпоширенішим, в наш час, способом захистити мультимедійні дані та об'єкти авторського права, це *застосування цифрового водяного знаку*. Вирізняється він своєю універсальністю і методом захисту. Перевага полягає

в простому ефекті невидимки. Тобто, при звичайному візуальному розгляді чи звичайному прослуховуванні користувач не помітить будь-яких закодованих чи шифрованих позначень. Значок копірайта, ім'я автора, рік видання, місце видання, запис чи інша додаткова інформація, являються тими позначеннями, що є частиною цифрового водяного знаку і без застосування певного програмного засобу вони є невидимі при звичному використанні. На даний момент існують фірми, що займаються розробкою програмного забезпечення та удосконаленням методу вставлення цифрового водяного знаку в мультимедійний контент для більш надійного захисту. Серед таких програм найбільшої популярності у використанні набули Digimarc MyPictureMarc та EIKONAmark. Найчастіше цифрові водяні знаки використовують для захисту зображень, хоча за останні роки дослідження було наведено приклади, коли даний метод захисту можливо ефективно застосувати у аудіо та відеопотоках.

Також одним із надійних методів вважають, *обмеження доступу* до матеріалів, що знаходяться в базах даних комерційних сайтів, деяких електронних бібліотек та архівів доступ до яких надається тільки за попередню плату. На жаль, надати впевненості, що захист буде відбуватись належним чином, також не являється можливим, оскільки, як зазначається статистикою, більшість витоків інформації стається саме через причини, що спричинені персоналом. А також, використання такого методу захисту інколи потребує фінансування.

Використання *методу криптографічного шифрування* дозволяє частково обмежити або повністю виключити можливість копіювання творів. Хоча криптографічне шифрування набрало досить великої популярності у захисті інформації, на жаль для його застосуванню в захисті мультимедійних даних не приділяють достатньої уваги, що зменшує ефективність і стримує розвиток даного методу.

Метод антикопії. Призначення цього методу полягає у встановленні своєрідний технічний бар'єр на CD-ROM, що не дозволяє зробити копії. Даний метод можна назвати ефективним, але оскільки розвиток технологій досягнув нових вершин, встановлення технічного бар'єру можна віднести до застарілих методів.

Створення web-депозитаріїв. Цей метод не набрав досить великої популярності і, на нашу думку, недооцінений. Основне його призначення це зберігати об'єкти авторського права на інтернет-ресурсі і при необхідності підтвердити факт і час розміщення об'єкту [4, 5].

Усі вище наведені методи захисту мультимедійних даних та об'єктів авторського права мають право на своє існування, хоча деякі з них можна вважати неефективними або такими, що втратили свою актуальність. На даний момент актуальні дослідження, спрямовані на досягнення та покращення результатів впровадження цифрового водяного знаку. Оскільки даний метод являється універсальним в своїх можливостях і застосування його можемо спостерігати у різних елементах інформації, можна вважати, що

нові дослідження будуть давати кращі і досконаліші шляхи застосування цифрового водяного знаку, а також покращить захист як персональних так і мультимедійних даних.

Висновки. Порівнявши різноманітні методи захисту мультимедійних даних та об'єктів авторського права та інтелектуальної власності, можемо дійти висновку, що використання комбінованих методів кодування і шифрування надають нові перспективи для досягнення більш надійного захисту даних. Центральним та ключовим елементом завдяки своїй універсальності, на даний момент, залишається цифровий водяний знак. Його властивості в поєднанні з іншими методами захисту нададуть більшого захисту і впевненості власникам мультимедійної інформації, а також авторам, що здійснюють авторську та інтелектуальну діяльність.

1. https://uk.wikipedia.org/wiki
2. https://www.microsoft.com/uk-ua/antipiracy/
3. http://www.epravda.com.ua/news/2016/10/19/608322/
4. Рекомендації щодо вдосконалення механізму регулювання цифрового використання об'єктів авторського права і суміжних прав через мережу Інтернет – [Електронний ресурс] – Режим доступу: http://sips.gov.ua/ua/recomnet.html.
5. http://www.isan.org/about/#what_is_isan

Поступила 20.04.2017р.

УДК 004.9

Р.О. Кульчицький [1], аспірант УАД, О.В. Тимченко [1, 2], д.т.н, професор,
І.М. Лях[3], к.т.н., доцент

ПОРІВНЯННЯ АЛГОРИТМІВ ВИЯВЛЕННЯ КОНТУРУ ЦИФРОВОГО ЗОБРАЖЕННЯ

Анотація. В задачах розробки систем комп'ютерного зору, відновлення тривимірного зображення із серії знімків, моделювання та редагування зображення часто постає завдання виділити контур певної текстури – букви у слові, лиця людини, контуру будинку, тощо. Виділення контурів – доволі складна та нова математична задача. Новизна пов'язана з тим що цифрове фото зародилося на початку 1980-х, а масове застосування - лише в 1990-х роках.

Ключові слова. Контур зображення, цифрове фото.

[1], Українська академія друкарства
[2] Uniwersytet Warmińsko-Mazurski w Olsztynie
[3] ДВНЗ «Ужгородський національний університет»