УДК 681.3, 004.62

Карабась Ю. О., Морозов Ю. В.
Національний університет "Львівська політехніка"
кафедра електронних обчислювальних машин

Кіберфізична система захищеної передачі мультимедійних даних через Інтернет

Розглянуто проблеми захисту мультимедійних даних від сторонніх осіб під час передачі відкритим каналом зв'язку. Проаналізовано існуючі технічні рішення, їх переваги та недоліки. Запропоновано структуру та наведено опис власного рішення.

Ключові слова: захист мультимедійних даних, система захисту інформації

Problem with protection of multimedia data from the third side during transmission via communication channel was analysed. Existing solutions with their advantages and disadvantages were analysed. Structure and description of own solution were proposed.

Keywords: protection of multimedia data, information protection system

Вступ. Зараз світ переживає процес активного розвитку інформаційних технологій. У зв'язку з цим цінність галузей, що займаються виробництвом мультимедійних продуктів та інтелектуального контенту, суттєво збільшується з кожним роком. Через це гостро постало питання захисту авторського права [1-4].

Наразі проблема захисту мультимедійних даних від несанкціонованого розповсюдження, як правило, вирішуються за допомогою заходів юридичного характеру. Але комплексного рішення, яке могло б вирішити проблему захищеної передачі мультимедійного контенту через мережу Інтернет на даний момент не існує.

У цій доповіді наведено детальний опис згаданої вище науково-технічної проблеми. Було проведено детальний аналіз останніх досліджень та досягнень у галузі захисту мультимедійних даних. Розглянуто аналоги та існуючи способи вирішення проблеми.

На основі проведеного аналізу було розроблено власне рішення, що враховує проблеми існуючих способів захисту мультимедійної інформації та вирішує їх.

Стан проблеми. Використання сучасних інформаційних системи для розповсюдження, запису, збереження та обробки мультимедійної інформації суттєво збільшило прибуток компаній, що займаються виготовленням інтелектуальної власності. Але при цьому виникає маса питань технологічного характеру, що пов'язані з дотриманням інтересів власників авторських прав та захистом медіа контенту від сторонніх осіб. Протягом останніх десяти років ці питання активно вирішуються інженерами з усього світу.

Одне з популярних рішень це так звані DRM (з англ. DRM - Digital rights management — керування цифровими правами) [4-8]. DRM - це поняття, що використовується для посилання на технології авторизації, які використовуються видавцями, приватними особами, власниками авторських прав з метою обмеження використання цифрової інформації. Основна мета технологій керування цифровими правами – унеможливити неавторизований доступ до даних, копіювання інформації.

DRM включає у себе як програмні, так і програмно-апаратні засоби. DRM доволі часто критикуються звичайними користувачами. Адже системи керування цифровими правами часто створюють додаткові труднощі для покупців (наприклад, аудіозаписи, що були куплені через систему Apple iTunes можна прослуховувати лише на плеєрах цієї компанії).

DRM включає у себе як програмні, так і програмно-апаратні засоби. DRM доволі часто критикуються звичайними користувачами. Адже системи керування цифровими правами часто

створюють додаткові труднощі для покупців (наприклад, аудіозаписи, що були куплені через систему Apple iTunes можна прослуховувати лише на плеєрах цієї компанії).

Ще одне рішення, що дозволяє однозначно ідентифікувати власника оригінального медіа контенту — цифрові водяні знаки. Це спосіб захисту авторських прав, що базується на досягненнях стеганографії.

Стеганографія (з грецьк. steganos – секрет, таємниця; graphy – запис) – спосіб передачі або зберігання інформації, суть якого полягає у приховуванні факту наявності секретних даних. Тобто якщо криптографія захищає вміст повідомлення від сторонніх осіб, то стенографія захищає сам факт наявності прихованого повідомлення.

Хоч цифрові водяні знаки і дозволяють захистити авторські права, але цей спосіб не є комплексним. Використання описаного вище методу ніяк не зашкодить зловмиснику отримати медіа контент. Цифрові водяні знаки лише допоможуть власнику авторських прав довести свою позицію під час заходів організаційно-юридичного характеру.

Постановка задачі. Запропонувати унікальне та ефективне рішення проблеми з захистом мультимедійних даних під час передачі через мережу Інтернет. Розробити кіберфізичну систему, що дозволить користувачам отримати безпечний доступ до мультимедійних даних. Розрбити структурну схему кіберфізичної системи, описати принцип її роботи.

Розв'язання задачі. Для вирішення поставленої задачі було вирішено розробити клієнт-серверну систему, що буде складатися з трьох основних частин: сховище даних, сервер та клієнт. Структурну схему системи захищеної передачі мультимедійних даних наведено на рис. 1.

Рис. 1. Структурна схема системи захищеної передачі мультимедійних даних

Сховище даних використовується з метою збереження мультимедійного контенту. Уся інформація у сховищі зберігається у закодованому вигляді.

Основне призначення серверної частини — безпечна доставка медіа даних до клієнтів. Використовуючи сервер, клієнт може отримати доступ до даних інших користувачів. Серверна частина при цьому забезпечує безпечну передачу інформації і гарантує, що дані не будуть доступні стороннім особами. Окрім цього користувач має можливість поширювати власні медіа дані іншим клієнтам.

Клієнтська частина призначена для передачі інформації на сторону сервера, отримання та відтворення закодованих даних від серверної частини.

Закодовані дані між сервером та клієнтом передаються згідно до алгоритму Діффі-Хеллмана. Це один із способів безпечного обміну криптографічними ключами. Він забезпечує захищену передачу даних між двома сторонами з використанням загальнодоступного інформаційного каналу.

Метод Діффі-Хеллмана служить базою для багатьох протоколів захисту інформації, що використовують автентифікацію [9-10]. У якості прикладу можна навести протокол TLS (з англ. Transport Layer Security — захист на транспортному рівні). Принцип роботи алгоритму Діффі-Хеллмана зображено на рис. 2.

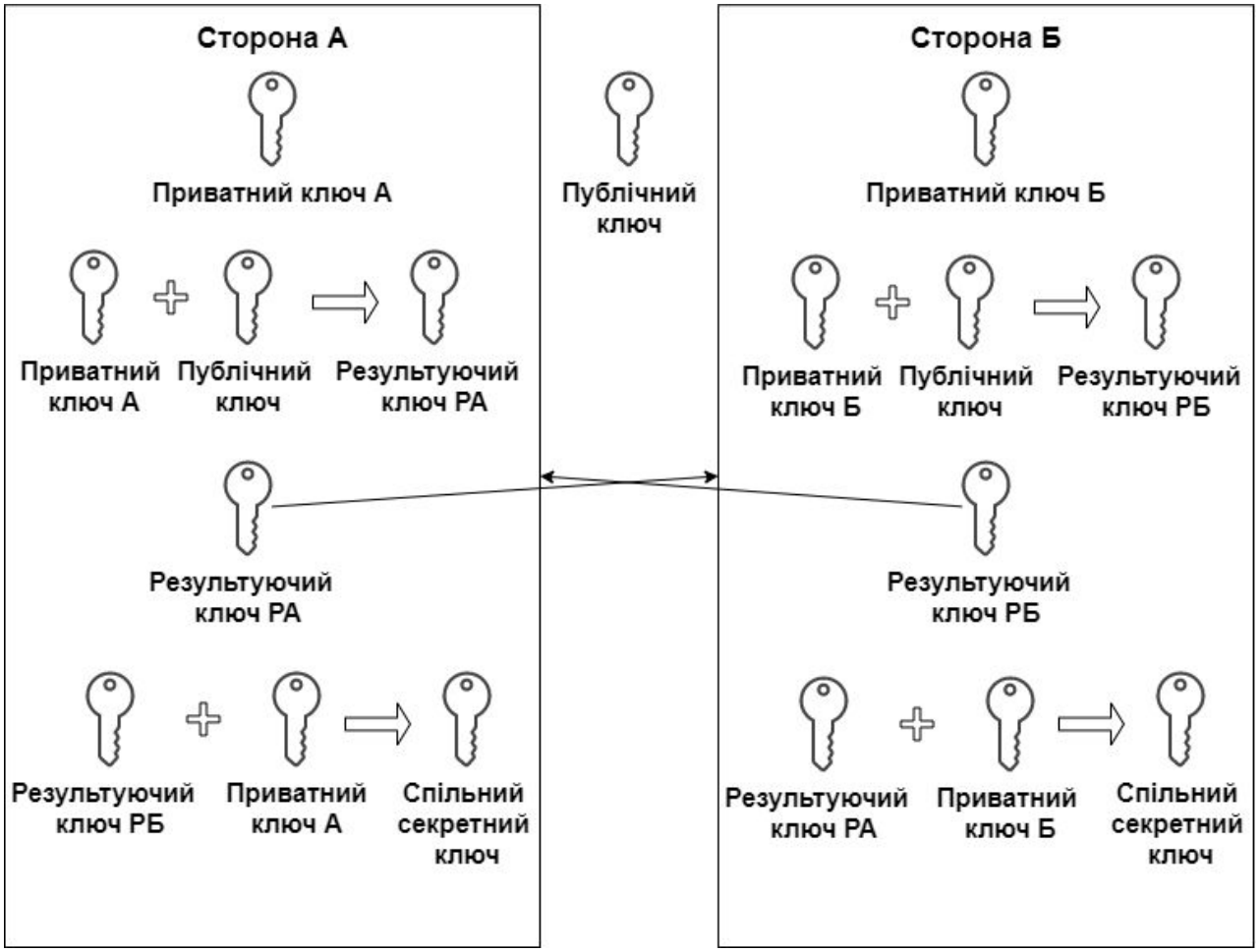

Рис. 2. Принцип роботи алгоритму узгодження ключів Діффі-Хеллмана

Метод Діффі-Хеллмана служить базою для багатьох протоколів захисту інформації, що використовують автентифікацію. У якості прикладу можна навести протокол TLS (з англ. Transport Layer Security — захист на транспортному рівні). Принцип роботи алгоритму Діффі-Хеллмана зображено на рис. 2.

Процес обміну ключами з використанням методу Діффі-Хеллмана відбувається наступним чином:

1. Дві сторони узгоджують ключ, який є доступним для всіх.
2. Кожна зі сторін обирає секретний ключ, який зберігає на свої стороні.
3. Сторони шифрують секретний ключ за допомогою узгодженого публічного ключа. В результаті кожна зі сторін тепер має власний результуючий ключ.
4. Між сторонами відбувається обмін результуючими ключами.
5. Кожна зі сторін шифрує отриманий результуючий ключ своїм приватним ключем. В результаті у кожного з учасників обміну тепер є спільний секретний ключ.

Алгоритм широко використовується для передачі даних через відкритий інформаційний канал. Але він не позбавлений недоліків. Мінусом розглянутого алгоритму є вразливість перед атаками типу MITM (з англ. Man in the middle – людина посередині). Жодна із сторін не має можливості достовірно визначити хто насправді її співрозмовником.

Висновки. У даній роботі було запропоновано спосіб вирішення проблеми з безпечною передачею мультимедійний даних через мережу Інтернет. Було розроблено структуру клієнт-серверної кіберфізичної системи, що буде забезпечувати захист чутливої інформації від сторонніх осіб. Було розроблено та описано структурну схему системи.

Література

1. Paul Stanton, William Yurick, Larry Brumbaugh. Protecting Multimedia Data in Storage: A Survey of Techniques Emphasizing Encryption, 2005
2. Simon Singh. The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2000
3. Stuart McClure, Joel Scambray, George Kurtz. Hacking Exposed 7: Network Security Secrets and Solutions, 2012
4. Adam Shostack. Threat Modeling: Designing for Security, 2014
5. Bill Rosenblatt. Digital Rights Management: Business and Technology, 2001
6. Eberhard Becker, Willms Buhse, Dirk Günnewig, Niels Rump. Digital Rights Management: Technological, Economic, Legal and Political Aspects, 2003
7. Joan Van Tassel. Digital Rights Management: Protecting and Monetizing Content, 2006
8. Christopher May. Digital Rights Management: The Problem of Expanding Ownership Rights, 2007
9. Uyless D. Black. Internet Security Protocols: Protecting IP Traffic, 2000
10. Colin Boyd. Protocols for Authentication and Key Establishment, 2003