УДК 004.9 : 004.056

РОЗЛОМІЙ Інна Олександрівна
к. т. н., старший викладач,
Черкаський національний університет
імені Богдана Хмельницького
ORCID: 0000-0001-5065-9004
e-mail: inna-roz@ukr.net

ЯРМІЛКО Андрій Васильович
к. т. н., доцент, доцент,
Черкаський національний університет
імені Богдана Хмельницького
ORCID: 0000-0003-2062-2694
e-mail: a-ja@ukr.net

ІНТЕГРОВАНИЙ КРИПТОГРАФІЧНО-СТЕГАНОГРАФІЧНИЙ ЗАХИСТ МУЛЬТИМЕДІЙНОГО КОНТЕНТУ І ДАНИХ В СИСТЕМАХ E-LEARNING

У статті розглянуто загальну проблематику безпеки в системах e-learning. Проаналізовано сучасні дослідження та практику застосування інструментарію інформаційної безпеки у таких системах. Встановлено, що у більшості випадків системи e-learning надають користувачам засоби автентифікації та ідентифікації учасників сеансів навчання, забезпечують конфіденційність та адресність інформаційних процесів, захищеність навчальних матеріалів при використанні відкритих каналів зв'язку та інші функції захисту. Проте комплексний підхід до захисту систем e-learning залишається малодослідженим. З огляду на це було запропоновано підсилити захист даних та мультимедійного контенту в системах електронного навчання шляхом застосування інтегрованого криптографічно-стеганографічного підходу. Він застосовує алгоритм побудови цифрового водяного знаку, який базується на операціях матричного криптографічного перетворення. Комплексне застосування двох методів захисту має на меті підвищення стеганографічної стійкості алгоритму вбудовування міток цифрового водяного знаку за рахунок ускладнення завдання вибору параметру інверсії бітів у байтах, призначених для вбудовування ідентифікаційних ознак. Додатковий захисний ефект забезпечується неочевидністю вибору байтів у файлі-контейнері для вбудовування цифрового водяного знаку та можливістю їхньої ідентифікації лише за допомогою криптографічних процедур уповноваженими користувачами. Такий підхід є продуктивним щодо формування стратегії довіри до он-лайн матеріалів і дистанційної діяльності в освітній галузі, особливо – до мультимедійних ресурсів у системах e-learning. Інкорпорування пропонованих захисних механізмів в існуючі та розроблювані системи електронного навчання пропонується шляхом додавання відповідних фрагментів коду або незалежно скомпільованих програмних модулів-плагінів. Практичне впровадження відповідних програмних інструментів має сприяти підвищенню довіри між учасниками системи електронного навчання за рахунок можливості ідентифікації викрадених або скомпрометованих ідей та інновацій у контенті освітніх ресурсів, фіксації статусу скомпрометованих користувачів як серед здобувачів освіти, так і серед викладачів. Позитивний ефект очікується як у контексті ключових детермінант методів захисту даних в системах електронного навчання, так і щодо підтримки сталого розвитку цифрових індустрій, пов'язаних з книговидавництвом та поширенням мультимедійних творів.

Ключові слова: *захист авторського права, цифровий водяний знак, електронне навчання, шифрування, стеганографія, криптографія.*

Постановка проблеми. Цифрова інформаційна революція змінила комерційну та академічну поведінку, а Інтернет відіграв важливу роль у глобалізації цих процесів. Як зазначено L. Shahmoradi, V. Changizi, E. Mehraeen, A. Bashiri, B. Jannat та M. Hosseini,

переваги від трансляції даних, легке редагування будь-якого цифрового вмісту та можливість його відтворення без будь-яких втрат якості зробили цифрову технологію набагато кращою за старі аналогові системи [1]. Це породило нові можливості для інновацій. Розвиток інформаційних технологій стимулював перехід до нових форм організації діяльності в освітній сфері. Її швидкий розвиток стимулюється впровадження електронного навчання, яке є прямим результатом інтеграції освіти та технологій і стало потужним засобом, орієнтованим, зокрема, на використання Інтернет-технологій.

Електронне навчання – це інтерактивний процес, у якому навчальний контент доступний в режимі он-лайн і забезпечує автоматичний зворотний зв'язок із навчальною діяльністю студента, а отже, використання Інтернету для покращення електронного навчання стало трендом сучасних закладів освіти (M. A. H. Masud, X. Huang, [2]). Електронне навчання швидко розширилося завдяки різноманітним технологіям і пристроям для доступу до навчальних ресурсів, таких як ноутбуки, комп'ютери, смартфони та планшети. Технології суттєво вплинули на освіту, навчання та методи викладання.

Беззаперечне значення електронного навчання в освіті призвело до масового зростання кількості курсів електронного навчання та систем, які пропонують різні види послуг. Сьогодні велика кількість навчальних ресурсів доступні через Інтернет в різних форматах (текст, зображення, аудіо, відео), що сприяє самостійному навчанню та виходу за межі географічних кордонів. Курси, призначені для електронного навчання, містять нові типи навчальних матеріалів, які використовують переваги мережевих, мультимедійних та інших інформаційних технологій. Крім того, відбулося розширення можливостей для співпраці із залученням інтерактивних функцій спілкування – форумів, чатів тощо.

Проте легкість та доступність методів і засобів виготовлення ідеальних цифрових копій та пов'язане з цим масштабне незаконне копіювання електронного контенту є значним викликом для нормального розвитку цифрових індустрій, пов'язаних з книговидавництвом, аудіовізуальними творами та навіть науковими публікаціями. Не оминає ця проблема і сферу електронного навчання.

Виникнення та розвиток систем e-learning безпосередньо пов'язані з поширення комп'ютерно-опосередкованої комунікації та розвитком нових інформаційно-комунікаційних технологій (ІКТ). Спілкування в комп'ютерному форматі впливає на багато різних аспектів притаманної освітньому процесу міжособистісної та групової комунікації. Серед них вартими пильної уваги є, зокрема, механізми формування вражень, групова динаміка та етичні питання, пов'язані з довірою до джерела і, власне, до самої інформації. Недоліки цього формату, які особливо проявляються при відсутності відеотрансляції, пов'язують з втратою значимої для правильної інтерпретації повідомлень невербальної інформації: тону, міміки та жестів. Таким чином, хоча комунікація за допомогою комп'ютера надає чимало переваг, технологічне посередництво може також гальмувати процес спілкування та відбиватися на його якості. Додаткові труднощі виникають також із захистом інформаційних ресурсів та персональних даних, що збираються та обробляються під час процедур електронного навчання.

Практичний досвід переходу до електронного навчання з використанням його дистанційних форм переконливо показав, що використання Інтернет-технологій в організації навчання призводить до значного підвищення доступності та якості навчання і, як наслідок, сприяє підвищенню рентабельності системи навчання. Система електронного навчання забезпечує кожного студента інформаційними та освітніми можливостями в будь-який момент часу незалежно від їх місцезнаходження. Іншими

словами, Інтернет-орієнтована модель освіти характеризується повнотою свободи від просторово-часових обмежень, що є її незаперечною перевагою. Водночас, розроблені комунікаційні рішення систем електронного навчання не забезпечують можливості абсолютного контролю над каналами спілкування. Переваги надання знань у цифровій формі можуть бути знівельовані можливістю їх незаконного копіювання, модифікації та розповсюдження без урахування авторських прав. Тому надання навчальних матеріалів через відкриті канали зв'язку, захист переданого мультимедійного вмісту навчальних курсів, так само як і пов’язаних з освітнім процесом даних, автентифікації та ідентифікації його учасників, конфіденційності та адресності сеансів навчання, питання захисту авторських прав, інтелектуальної власності, академічної доброчесності стають особливо актуальними.

Аналіз останніх досліджень і публікацій. Електронне навчання стало основним напрямком в освітньому секторі та було масово впроваджено у вищій освіті. Воно охоплює широкий набір програм і процесів, таких як веб-навчання, комп’ютерне навчання, віртуальні класи та цифрова співпраця. Причому, як показує практика, бурхливому зростанню попиту на такі інновації та, зокрема, на дистанційні освітні послуги, сприяє не лише технологічний прогрес, але й трансформація освітнього простору внаслідок глобальних і локальних катаклізмів, таких як епідемії, стихійні лиха та війни. Якість систем електронного навчання привертає значну увагу дослідників, котрі намагаються визначити фактори їхнього ефективного функціонування, щоб максимізувати ефективність цих систем. Одним з важливих показників їхньої якості є вирішення питань інформаційної безпеки і, зокрема, конфіденційності та безпеки користування.

Інформаційна безпека визначається, як комплекс заходів щодо виявлення та запобігання неавторизованому доступу користувачів, здійсненому за допомогою відповідного набору інструментів (V. I. Zuev, [3]). На важливості інформаційної безпеки для систем електронного навчання наголошує S. Aljawarneh у [4]. У дослідженні [5] S. H. Hasan, D. M. Alghazzawi та A. Zafar найважливіші вимоги щодо конфіденційності та безпеки, пов’язані з електронним навчанням, розділяють на три основні групи:

– конфіденційність користувача (визначення мети збору даних, знання політики конфіденційності, необхідності видалення даних після використання тощо);

– конфіденційність мережі (всі ресурси вразливі до мережевих атак);

– механізми безпеки (автентифікація, створення профілю користувача, захист навчальних матеріалів, сертифікація, біометрична ідентифікація, ідентифікація за допомогою смарт-карт тощо).

Найчастіші випадки, пов’язані із заподіянням шкоди в контексті електронного навчання, підсумовано G. Riahi в [6] таким чином:

1) пошкоджені або втрачені повідомлення, оцінки, дані чи роботи;
2) ідентифікація скомпрометованих учнів або викладачів;
3) викрадені або скомпрометовані ідеї або інновації студентів;
4) порушена цілісність соціальних або технічних систем.

Огляд загроз безпеці систем електронного навчання зроблено в [7-9], де описано підхід до створення захищеної системи електронного навчання. Авторами A. R. Ghobadi, A. Boroujerdizadeh, A. H. Yaribakht та A. Abd Manaf описана загальна концепція захисту систем електронного навчання за допомогою цифрових водяних знаків (ЦВЗ) [10]. У праці наведена класифікація методів накладання ЦВЗ для забезпечення цілісності контенту в системах електронного навчання. Інші напрямки досліджень стосувались методу вбудовування ЦВЗ за допомогою генетичних

алгоритмів (H. S. Heniedy, O. M. Ouda, M. O. Khozium, [11]) та методу вейвлет-перетворень (A. Zemtsov, [12]). Загалом, у більшості оглянутих досліджень вивчалися окремі частини ключових детермінант методів захисту даних в системах електронного навчання.

Мета дослідження. Огляд літератури виявив, що малодослідженим залишається комплексний підхід до захисту систем e-learning. Дана обставина вплинула на формування мети цієї статті: захист даних та мультимедійного контенту в системах електронного навчання шляхом застосування інтегрованого криптографічно-стеганографічного підходу. Такий підхід має підвищити довіру між учасниками системи електронного навчання.

Виклад основного матеріалу.

1. Загальні методи захисту мультимедійного контенту і даних у системах e-learning. При всій багатоманітності технічної та технологічної підтримки комп'ютерно-опосередкованої комунікації у системах e-learning, ознакою часу є опора на хмарні технології. Електронне навчання на основі хмарних технологій – це спосіб зменшити вартість і складність доступу до даних, які контролюються сторонніми службами. Традиційні методи електронного навчання поєднуються з технологією хмарних обчислень, щоб надати переваги користувачам.

Хмарні технології та пов'язані з ними сервіси, крім очевидних переваг, мають і об'єктивні недоліки, які випливають з самої архітектури «хмари» як техніко-технологічного рішення і, відповідно, з її здатності гарантувати безпеку даних як таку, тобто принциповою здатністю сервісів гарантувати зберігання та обробку даних згідно з чинними правовими актами. Як показано на рис. 1, загрози безпеці у системах електронного навчання стосуються всіх типів хмарних послуг: дистанційного надання програмного забезпечення (SaaS), платформи (PaaS) чи інфраструктури (IaaS).

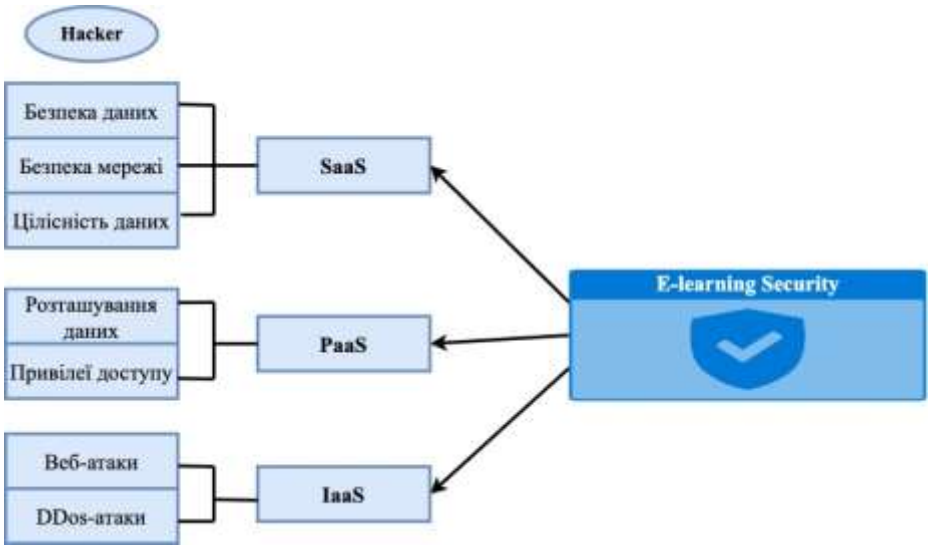

Рисунок 1 – Типи атак на системи e-learning

Дані відіграють важливу роль у хмарних службах, оскільки багато постачальників хмарних послуг зберігають дані клієнтів у великих центрах обробки даних (data centre). Під час перехідних операцій безпека даних клієнтів не гарантується. Коли один користувач синхронізує декілька пристроїв, дані можуть бути пошкоджені.

Безпеку даних можна класифікувати двома способами. По-перше, власник даних має переконатися, що постачальник хмарних послуг оброблятиме дані лише згідно з інструкціями клієнта. По-друге, власник даних повинен бути впевнений, що постачальник хмарних послуг вжив відповідних дій у разі несанкціонованого доступу до даних, модифікації даних, знищення даних зловмисниками.

Постачальникам хмарних послуг мають надаватись гарантії щодо наведених нижче ключових проблем безпеки даних:

- застосування механізму запобігання несанкціонованого доступу до даних;
- можливість власникам даних часто створювати резервні копії;
- надання законних повноваження власникам даних на видалення, зміну даних і переміщення даних до іншого хмарного постачальника.

Клієнти зберігають свої конфіденційні дані на хмарному сервері, і постачальник SaaS може ними маніпулювати. Тому для захисту даних від витоку конфіденційної інформації застосовуються жорсткі методи шифрування мережевого трафіку для керування потоком даних у мережі, наприклад: Secure Socket Layer (SSL) і Transport Layer Security (TLS).

Цілісність даних передбачає правильність, доступність, високу якість і надійність збережених даних. Хмарою забезпечується цілісність сховищ даних для конфіденційності клієнтів. У розподіленому середовищі для досягнення цілісності даних у транзакціях бази даних беруть участь багато ресурсів даних. Додатку SaaS потрібно забезпечити середовище для обробки даних із кількома клієнтами та залучення більшої кількості сторонніх сторін. Як засоби досягнення цілісності даних розглядаються методи хешування, автентифікація повідомлень і цифрові підписи.

У випадку PaaS-послуг хмарні обчислення надають клієнтам обчислювальну платформу та системне програмне забезпечення. Користувачі хмари створюють програму, керуючи розгортанням програмного забезпечення та параметрами конфігурації від постачальників. З точки зору безпеки, вторгнення на основі хосту та мережі є складними факторами для постачальників PaaS. Основні загрози безпеки рівня PaaS стосуються розташування даних і привілеїв доступу.

Постачальники PaaS надають послуги з проектування додатків, розробки додатків, розгортання, командної співпраці, інтеграції веб-сервісів і тестування. На основі розташування даних модель PaaS забезпечує надійність своїм клієнтам. Хмарний постачальник має повні права доступу до даних, коли дані зберігаються в хмарному середовищі. У цьому хмарному середовищі немає конфіденційності даних. Таким чином, підтримувати привілейований доступ користувача можна за допомогою принаймні одного або двох підходів, доступних власникові даних. Перший – вибрати надійний метод шифрування для зберігання даних і використовувати інший метод шифрування для доступу до даних; другий – підтримувати високий стандарт конфіденційності даних, законодавчо встановлюючи вимоги постачальника хмарних послуг через договірні обов’язки та механізми забезпечення. Хмарний постачальник повинен мати перевірені політики контролю безпеки доступу, технічні рішення та частий аудит дій користувачів, щоб запобігти несанкціонованому доступу користувачів, і підтримувати принцип розподілу обов’язків для привілейованих користувачів, щоб запобігати та виявляти зловмисну внутрішню діяльність.

Інфраструктура як модель обслуговування у хмарних середовищах дозволяє клієнту використовувати різноманітні ресурси, такі як сервери, сховища, мережі та інші обчислювальні ресурси, як віртуалізовані системи, які отримують доступ через Інтернет. Користувачі можуть запускати будь-яке програмне забезпечення з безпекою на виділених ресурсах, тому IaaS забезпечує повний контроль і керування ресурсами. Отже, хмарні провайдери несуть відповідальність лише за налаштування політик

безпеки. Типовими проблемами безпеки, пов'язаними з IaaS, є атаки на веб-сервіс та DDoS-атаки.

Таким чином, питання безпеки є серйозною проблемою в хмарних ресурсах на всіх притаманних їм рівнях надання послуг. А найважливішою рушійною силою пошуку відповідних технічних і організаційних рішень є занепокоєння щодо захисту авторських прав на цифровий контент, регуляція доступу до сервісів та режимів їхнього функціонування. В контексті захисту навчального контенту рішення проблеми знаходять завдяки впровадженню програм мультимедійної системи безпеки (Multimedia Security Applications, MSA). За останні роки MSA продемонстрували значний прогрес і включають досить широкі функціональні можливості: захист авторських прав, конфіденційність, виявлення зловмисників, виявлення підробки, підтвердження доставки та підтвердження покупки. Для посилення захисту та забезпечення авторських прав на цифровий контент MSA використовують засоби криптографії та стеганографії і послуговуються такими інструментами як автентифікація, шифрування, позначення часу, хешування, цифровий електронний підпис та цифрові водяні знаки (рис. 2). Зараз найважливішим доступним інструментом захисту даних є шифрування. Цей інструмент захищає дані під час спілкування між відправником і одержувачем через Інтернет. Проте після отримання даних і їхньої розшифровки (дешифрування) вони більше не захищені.

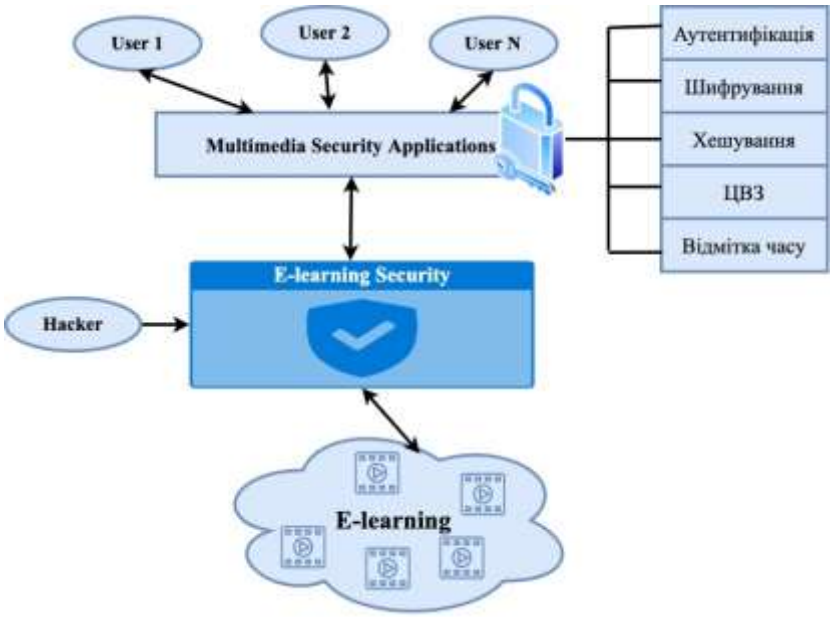

Рисунок 2 – Модель захищеної системи e-learning

2. Технологія цифрового водяного знаку та її застосування. Цифровий водяний знак (ЦВЗ) призначений для доповнення криптографічних процедур при вирішенні задачі захисту інтелектуальної власності в системах електронного навчання. Використання цієї технології спрямоване на створення додаткових ідентифікаційних ознак шляхом введення міток в оригінальний мультимедійний вміст для ідентифікації автору твору. Вона є одним із варіантів застосування методів стеганографії. За останні роки технологія ЦВЗ продемонструвала значний прогрес [13] і зараз широко застосовується для захисту права власності на цифрові зображення, аудіофайли, відео та текст. Таким чином, ця технологія має потенціал вирішення питань управління цифровими правами, захисту інформації та забезпечення конфіденційності. В електронному навчанні стеганографічні методи дозволяють вирішити такі завдання:

1. Захист авторських прав шляхом запобігання можливості копіювання та дублювання мультимедійних ресурсів. Можливість запровадження цифрового водяного знаку дозволяє відтворювати заборону копіювання та редагування мультимедійної інформації.

2. Автентифікація та ідентифікація. Визначення достовірності інформації, отриманої через мережу, залишається важливою проблемою електронного навчання, в якій знання студента оцінюються за результатами виконаної індивідуальної роботи та за результатами дистанційного тестування.

Завдяки цим можливостям використання ЦВЗ в електронному навчанні стає все більш популярним як важлива частина стратегії довіри до цифрового контенту систем e-learning. Крім того, для електронного навчання, яке передбачає використання високоякісних зображень, pdf-файлів тощо, захищеність авторського контенту є одним з чинників підвищення ефективності навчальної діяльності.

За своєю суттю ЦВЗ – це спеціальна мітка, яка вбудовується в цифровий контент (контейнер) з метою підтвердження цілісності даних. Одночасно, це потужна технологія для ідентифікації даних про авторські права. ЦВЗ оперує оцифрованою інформацією у вигляді тексту, зображення, аудіо чи відео, які вбудовано в оригінальну інформацію та можуть бути правильно вилучені за допомогою методу видалення водяного знаку для підтвердження права власності. Важливо, що для людського ока відмінність оригінальної інформації від інформації з водяним знаком є непомітною [14]. Завдяки цьому ЦВЗ дозволяє уповноваженим особам додавати приховані повідомлення про авторські права на цифрове аудіо, відео, зображення та текст. Цей метод придатний для маркування наборів даних і внесення відмітки для реєстрації права власності на основі зорової системи людини.

Отже, ЦВЗ є одним з методів автентифікації, який дозволяє контролювати спотворення в цифрових мультимедійних даних (Digital Multimedia Data, DMD). Система ЦВЗ має дві основні фази: вбудовування та вилучення (рис. 3).

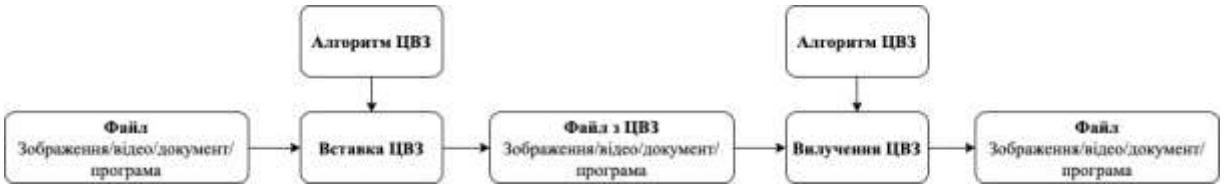

Рисунок 3 – Процес вставки/вилучення ЦВЗ

В практичних випадках ЦВЗ може бути логотипом установи, псевдовипадковою послідовністю або фоном зображення чи файлу pfd. Серед сукупності ознак, за якими класифікуються ЦВЗ, найбільш поширеною є ознака за ступенем сприйняття. Відповідно до цього класифікатора ЦВЗ поділяються на видимі (Visible Digital Watermark, VDW) та невидимі (Invisible Digital Watermark, IDW) [15]. Більшість досліджень присвячені вивченню IDW, оскільки вони частіше використовуються в ЦВЗ.

Видимий цифровий водяний знак – VDW – був початковим і, в основному, примітивним методом ЦВЗ, який є видимим для користувачів. Хоча VDW використовується протягом тривалого часу, він не є захищеною формою водяного знаку для DMD. Методика алгоритму VDW є недостатньою для захисту DMD. Водяний знак такого типу можна використовувати лише для ідентифікаційних цілей. Зокрема, в системах e-learning це доречно як один із заходів профілактики несанкціонованого втручання в цифрові мультимедійні дані.

Невидимий цифровий водяний знак – IDW – можна виконати за допомогою різних технік, і найпростіша з них – це приховати водяний знак у DMD. Переваги приховування полягають у тому, що навіть якщо частину зображення буде обрізано, одержувач може отримати потрібне повідомлення, оскільки водяний знак вставляється у нього багато разів. Якщо змінити найважливіші біти у повідомленні, то це матиме великий вплив на властивості початкового файлу (наприклад, може помітно змінитися колір зображення). Навпаки, якщо змінити найменш значущі біти, це матиме мінімальний ефект. У випадку захисту мультимедійних зображень, якщо змінити лише один або два молодших біта у даних, це супроводжуватиметься мінімальним візуальним ефектом, оскільки людське око може помітити лише близько шести частинок кольору. Наприклад, якщо ми маємо справу з кодовим записом 10001100 і змінюємо його на 10001101, він буде аналогічно сприйматись людським оком. Даний метод вбудовування ЦВЗ отримав назву метода вбудовування даних в молодші біти або метода LSB (найменш значущого біта), та є одним із найпростіших і одним із найшвидших методів ЦВЗ (рис. 4).

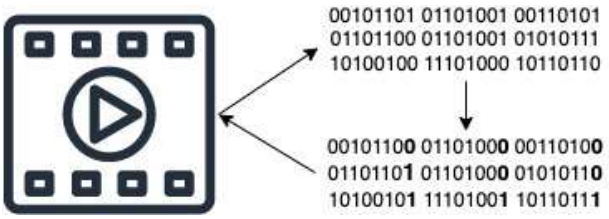

Рисунок 4 – Вставка ЦВЗ методом інвертування молодших бітів

Метод LSB є одним із найдавніших методів стеганографії та використовується для вбудовування захисних ознак у різні види мультимедійного контенту [16-17]. Для підвищення довговічності захисту, як правило, використовується секретний ключ, який визначає набір пікселів, доступних для вбудовування.

Більшість розроблених на сьогодні методів побудови цифрового водяного знаку, які можуть бути використані для задач захисту документів, побудовані на основі саме методу LSB. Проте, для більшості з них характерна вразливість, низька стеганографічна стійкість.

3. Метод комбінованого застосування криптографії та стеганографії для захисту контенту у системах e-learning. Враховуючи можливі ризики порушення захищеності складових системи e-learning, очевидно, що неможливо обійтися засобами лише криптографії чи стеганографії. В зв'язку з цим необхідний комплексний підхід до забезпечення інформаційної безпеки на всіх рівнях функціонування системи e-learning. Зокрема, з огляду на недоліки наявних методів вбудовування захисних (ідентифікаційних) компонентів, пропонується алгоритм побудови цифрового водяного знаку, який базується на операціях матричного криптографічного перетворення.

Мультимедійний файл, який підлягає захисту за допомогою накладання ЦВЗ, є контейнером для вбудовування ідентифікаційної інформації. Як вже зазначалось, при маркуванні контенту цифровим водяним знаком задіяні два процеси – вставка та вилучення. Вставка виконується безпосередньо власником контенту, щоб додати право власності на нього. Ці процеси протилежні один одному, але пов'язані між собою, оскільки вставка ЦВЗ має виконуватись таким чином, щоб вилучити інформацію могли лише авторизовані користувачі. Розглянемо ці процеси детальніше.

Eman 1. Вставка водяного знаку. Спочатку ЦВЗ вбудовується в вихідний файл-контейнер за алгоритмом [18]:

1) задати послідовність чисел та матрицю, на основі якої здійснюватиметься перетворення значень з проміжку;

2) виконати операції матричного криптографічного перетворення послідовності чисел; отримані значення вкажуть на байти, в яких будуть інвертуватись біти;

3) визначити параметр інверсії – біт(біти), який буде інвертуватись;

4) після інвертування бітів у всіх байтах з результатів виконання матричних перетворень вважаємо, що ЦВЗ вбудований у файл.

Суть запропонованого алгоритму полягає в тому, що спочатку над заданими значеннями, з визначеного проміжку, виконується матричне перетворення (рис. 5).

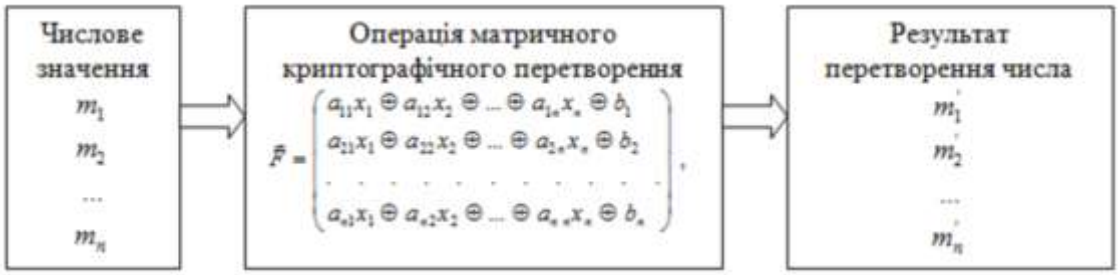

Рисунок 5 – Матричне криптографічне перетворення числових значень

З рис. 5 видно, що над кожним значенням m_1, m_2, ..., m_n виконується матричне криптографічне перетворення, в результаті якого отримуємо нові значення m'_1, m'_2, ..., m'_n, які вказують на байти, в яких будуть інвертуватися біти [19].

Інверсія може виконуватися над будь-яким бітом в байті чи кількома одразу. Найпростіший спосіб – інвертувати молодший біт у байті. Саме для ускладнення завдання вибору параметру інверсії й варто використовувати матричне криптографічне перетворення. Тобто, за допомогою матриці маємо перетворювати задане число, а отриманий таким чином результат перетворення вказуватиме на порядковий номер біта в байті, який буде інвертуватися.

В результаті матричних криптографічних перетворень будуть знайдені байти, в яких відбулася інверсія бітів. На перший сторонній погляд здається, що байти, в яких відбулася інверсія бітів, вибрані в хаотичному порядку. І цей ефект підвищує стеганографічну стійкість алгоритму вбудовування міток цифрового водяного знаку.

Eman 2. Вилучення ЦВЗ. Операції процесу видалення ЦВЗ аналогічні операціям його вставки: за допомогою матричного перетворення чисел з заданого діапазону визначаються потрібні байти та інвертуються відповідні біти у них.

Таким чином, з впровадженням додаткових криптоопераций переваги застосування ЦВЗ як ідентифікаційного засобу для позначення права власності або авторства на дані та мультимедійні об’єкти посилюються завдяки кращій захищеності ідентифікаційної інформації. В системах e-learning такі стійкі ідентифікатори можуть бути застосовані не лише для захисту навчального контенту, але й для створення індивідуальних прихованих міток для позначення робіт здобувачів освіти. Разом із засобами керування візуалізацією таких позначень з боку уповноважених користувачів, застосування таких інструментів має сприяти впровадженню принципів академічної доброчесності та спрощенню контролю щодо їхнього дотримання в межах конкретного сервісу e-learning в локальних освітніх групах. Особливо ефективною така функція може бути у випадку оцінювання потоків робіт значного обсягу, виконаних за ідентичними або подібними завданнями.

Запропоновані захисні механізми можуть бути інкорпоровані в існуючі та розроблювані системи електронного навчання шляхом додавання відповідних фрагментів коду (snippets) чи незалежно скомпільованих програмних модулів (plugins).

Висновки. Забезпечення цілісності навчального контенту та конфіденційності мережі є важливим завданням в системах електронного навчання. Захист ресурсів мережі має бути забезпечено на різних рівнях: виявлення фактів пошкодження або втрати повідомлень, оцінок, даних, завдань, а також робіт, виконаних здобувачами освіти. Актуальною є й ідентифікація викрадених або скомпрометованих ідей та інновацій, фіксація статусу скомпрометованих користувачів (як здобувачів освіти, так і викладачів).

Оскільки використання традиційних методів захисту не забезпечує актуального рівня захищеності систем e-learning, доцільним є застосування комплексного використання кількох методів. Продуктивним напрямом є поєднання методів стеганографії та криптографії. Для підвищення ефективності захисту на першому етапі пропонується накладати ЦВЗ на контент, потім обчислювати хеш-функцію. Для обчислення хеш-функції придатні всі існуючі методи, зокрема, на основі операцій матричних криптографічних перетворень, які запропоновані в роботі [20]. В результаті інтеграції двох технологій досягається підвищення стеганографічної стійкості захисних ознак. Такий підхід дозволить створювати цифровий контент з гарантією авторства та автентичності вмісту. Практичне впровадження відповідних програмних інструментів підтримає стратегію довіри до он-лайн матеріалів і діяльності в освітній галузі, особливо – до мультимедійних ресурсів.

Більш потужну схему захисту контенту і даних у системах e-learning можна побудувати за допомогою композиціювання ЦВЗ разом із сучасними м’яким обчислювальними інструментами, притаманними методам штучного інтелекту. Зокрема, такі рішення можуть ґрунтуватися на застосуванні генетичних алгоритмів, нейронних мереж та нечіткої логіки.

Список використаних літератури та джерел:

1. Shahmoradi, L., Changizi, V., Mehraeen, E., Bashiri, A., Jannat, B., & Hosseini, M. (2018). The challenges of E-learning system: Higher educational institutions perspective. *Journal of education and health promotion*, *7*.
2. Masud, M. A. H., & Huang, X. (2012). An e-learning system architecture based on cloud computing. *International Journal of Information and Communication Engineering*, *6*(2), 255-259.
3. Zuev, V. I. (2012). E-learning security models. *Management Information Systems*, *7*(2), 024-028.
4. Aljawarneh, S. (2011). A web engineering security methodology for e-learning systems. *Network Security*, *2011*(3), 12-15.
5. Hasan, S. H., Alghazzawi, D. M., & Zafar, A. (2014). E-Learning systems and their Security. *BRIS Journal of Adv. S & T (ISSN. 0971-9563) vol*, *2*, 83-92.
6. Riahi, G. (2015). E-learning systems based on cloud computing: A review. *Procedia Computer Science*, *62*, 352-359.
7. Banerjee, S., & Karforma, S. (2017). Object oriented modeling for authentication of certificate in e-learning using digital watermarking. *International Journal of Advanced Research in Computer Science*, *8*(8).
8. Al-Ajlan, A. S. (2014). E-Learning Certificate Using Digital Watermarking Technology. *IOSR J. Comput. Eng*, *16*(4), 81-93.
9. Banerjee, S., & Karforma, S. (2016). Authentication of certificate in e-learning using secret key digital watermarking. *International Journal of Information Science and Computing*, *3*(2), 53-58.
10. Ghobadi, A. R., Boroujerdizadeh, A., Yaribakht, A. H., & Abd Manaf, A. (2012, September). How watermarking secures e-learning system. In *2012 International Conference on E-Learning and E-Technologies in Education (ICEEE)* (pp. 99-104). IEEE.
11. Heniedy, H. S., Ouda, O. M., & Khozium, M. O. (2020). Sequring the e-learning materials using digital watermarking approach. Vol.9, No, 11, pp.1559-1563, November, 2020.

12. Zemtsov, A. (2020, November). Data Protection of Multimedia Content for E-Learning Using Discrete Wavelet Transform. In *8th Scientific Conference on Information Technologies for Intelligent Decision Making Support (ITIDS 2020)* (pp. 268-273). Atlantis Press.
13. Evsutin, O., Melman, A., & Meshcheryakov, R. (2020). Digital steganography and watermarking for digital images: A review of current research directions. *IEEE Access*, *8*, 166589-166611.
14. Saeed, F., & Dixit, A. (2018, September). Digital Watermarking Techniques for Content Integrity on E-Learning Systems. In *2018 International Conference on Computing, Power and Communication Technologies (GUCON)* (pp. 748-753). IEEE.
15. Rashid, A. (2016). Digital watermarking applications and techniques: a brief review. *International Journal of Computer Applications Technology and Research*, *5*(3), 147-150.
16. Thangadurai, K., & Devi, G. S. (2014, January). An analysis of LSB based image steganography techniques. In *2014 International Conference on Computer Communication and Informatics* (pp. 1-4). IEEE.
17. Jung, K. H., & Yoo, K. Y. (2015). Steganographic method based on interpolation and LSB substitution of digital images. *Multimedia Tools and Applications*, *74*(6), 2143-2155.
18. Розломій І.О., Косенюк Г.В. (2017) Спосіб формування цифрового водяного знаку для електронних документів на основі операцій матричного криптографічного перетворення. Вісник Хмельницького національного університету. Технічні науки, 4(251), 229–233.
19. Кулик С.В., Люта М.В., Розломій І.О. (2017) Дослідження нанесення QR-коду для захисту графічних зображень. Вісник Хмельницького національного університету. Технічні науки, 5(253), 244–248.
20. Розломій І.О. (2016) Методи обчислення хеш-функції електронного документу на основі матричних криптографічних перетворень. Вісник ЧДТУ. Технічні науки. 4. С. 88–94.

References:

1. Shahmoradi, L., Changizi, V., Mehraeen, E., Bashiri, A., Jannat, B., & Hosseini, M. (2018). The challenges of E-learning system: Higher educational institutions perspective. *Journal of education and health promotion*, *7*.
2. Masud, M. A. H., & Huang, X. (2012). An e-learning system architecture based on cloud computing. *International Journal of Information and Communication Engineering*, *6*(2), 255-259.
3. Zuev, V. I. (2012). E-learning security models. *Management Information Systems*, *7*(2), 024-028.
4. Aljawarneh, S. (2011). A web engineering security methodology for e-learning systems. *Network Security*, *2011*(3), 12-15.
5. Hasan, S. H., Alghazzawi, D. M., & Zafar, A. (2014). E-Learning systems and their Security. *BRIS Journal of Adv. S & T (ISSN. 0971-9563) vol*, *2*, 83-92.
6. Riahi, G. (2015). E-learning systems based on cloud computing: A review. *Procedia Computer Science*, *62*, 352-359.
7. Banerjee, S., & Karforma, S. (2017). Object oriented modeling for authentication of certificate in e-learning using digital watermarking. *International Journal of Advanced Research in Computer Science*, *8*(8).
8. Al-Ajlan, A. S. (2014). E-Learning Certificate Using Digital Watermarking Technology. *IOSR J. Comput. Eng*, *16*(4), 81-93.
9. Banerjee, S., & Karforma, S. (2016). Authentication of certificate in e-learning using secret key digital watermarking. *International Journal of Information Science and Computing*, *3*(2), 53-58.
10. Ghobadi, A. R., Boroujerdizadeh, A., Yaribakht, A. H., & Abd Manaf, A. (2012, September). How watermarking secures e-learning system. In *2012 International Conference on E-Learning and E-Technologies in Education (ICEEE)* (pp. 99-104). IEEE.
11. Heniedy, H. S., Ouda, O. M., & Khozium, M. O. (2020). Sequring the e-learning materials using digital watermarking approach. Vol.9, No, 11, pp.1559-1563, November, 2020.
12. Zemtsov, A. (2020, November). Data Protection of Multimedia Content for E-Learning Using Discrete Wavelet Transform. In *8th Scientific Conference on Information Technologies for Intelligent Decision Making Support (ITIDS 2020)* (pp. 268-273). Atlantis Press.
13. Evsutin, O., Melman, A., & Meshcheryakov, R. (2020). Digital steganography and watermarking for digital images: A review of current research directions. *IEEE Access*, *8*, 166589-166611.
14. Saeed, F., & Dixit, A. (2018, September). Digital Watermarking Techniques for Content Integrity on E-Learning Systems. In *2018 International Conference on Computing, Power and Communication Technologies (GUCON)* (pp. 748-753). IEEE.
15. Rashid, A. (2016). Digital watermarking applications and techniques: a brief review. *International Journal of Computer Applications Technology and Research*, *5*(3), 147-150.

16. Thangadurai, K., & Devi, G. S. (2014, January). An analysis of LSB based image steganography techniques. In *2014 International Conference on Computer Communication and Informatics* (pp. 1-4). IEEE.
17. Jung, K. H., & Yoo, K. Y. (2015). Steganographic method based on interpolation and LSB substitution of digital images. *Multimedia Tools and Applications*, *74*(6), 2143-2155.
18. Rozlomii, I. O., Kosenyuk, H. V. (2017) Sposib formuvannia tsyfrovoho vodianoho znaku dlia elektronnykh dokumentiv na osnovi operatsii matrychnoho kryptohrafichnoho peretvorennia [Method of forming a digital watermark for electronic documents based on operations of matrix cryptographic transformation]. Visnyk Khelnytskoho natsionalnoho universytetu. Tekhnichni nauky, 4(251), 229–233 [In Ukrainian].
19. Kulyk, S. V., Lyuta, M. V., & Rozlomii, I. O. (2017) Doslidzhennia nanesennia QR-kodu dlia zakhystu hrafichnykh zobrazhen [Studying of the techniques of a QR-code using to protect graphic images]. Visnyk Khelnytskoho natsionalnoho universytetu. Tekhnichni nauky, 5(253), 244–248 [in Ukrainian].
20. Rozlomii I.O. (2016) Metody obchyslennia khesh-funktsii elektronnoho dokumentu na osnovi matrychnykh kryptohrafichnykh peretvoren [Methods for calculating the hash function of electronic document on the basis of matrix cryptographic transformations]. Visnyk Cherkaskoho derzhavnoho tekhnolohichnoho universytetu. Tekhnichni nauky. 4. 88–94 [in Ukrainian].

ROZLOMII Inna,
Ph. D., Senior Lecturer, Bohdan Khmelnytsky National University of Cherkasy
YARMILKO Andrii,
Ph. D., Ass. Prof., Docent, Bohdan Khmelnytsky National University of Cherkasy

INTEGRATED ENCRYPTION-STEGANOGRAPHY PROTECTION OF MULTIMEDIA CONTENT AND DATA IN E-LEARNING SISTEMS

Abstract. Introduction. *The article focuses on the modern research and the practice of using information security tools in e-learning systems. It has been noted that, in most cases, e-learning systems ensure the confidentiality and addressability of information processes and the security of educational materials when using open communication channels. However, a comprehensive approach to e-learning systems protection needs to be better researched.*

Purpose. *Developing a data and multimedia content protection method in e-learning systems using an integrated cryptographic-steganographic approach.*

Methods. *Steganography, cryptography.*

Results. *The strengthening of data and multimedia content protection in e-learning systems was proposed using an integrated cryptographic-steganographic approach. This method applies the digital watermark construction algorithm based on matrix cryptographic transformation operations. The complex application of two protection methods is aimed at increasing the steganographic stability of the digital watermark embedding algorithm by complicating the task of selecting the bit inversion parameter in the bytes intended for embedding identification features. An additional protective effect is provided by the non-obviousness of the choice of the byte in the file container for embedding a digital watermark and the possibility of their identification only using cryptographic procedures by authorized users. This approach is productive in forming a trust strategy in online materials and remote activities in the educational field. Incorporating the proposed security mechanisms into existing and developing e-learning systems is offered by snippets or plugins adding.*

Conclusion. *The practical implementation of software tools according to the developed method should contribute to the increase of trust between the participants of the e-learning system due to the possibility of identifying stolen or compromised ideas and innovations in the content of the educational resources, fixing the status of compromised users among both students and teachers.*

Keywords: *e-learning, digital watermark, encryption, steganography, cryptography, copyright protection.*