МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

КУСМАРЦЕВ Володимир Ігорович

Алгоритми захисту об'єктів авторського права і суміжних прав на web-ресурсах / Algorithms for Protecting Copyright and Related Rights on Web Resources

спеціальність: 125 – Кібербезпека

освітньо-професійна програма –Кібербезпека

Кваліфікаційна робота

Виконав студент групи КБм - 22
В.І. Кусмарцев

Науковий керівник
д.т.н., професор М.М. Касянчук

Кваліфікаційну роботу допущено
до захисту:

«____» _____ ___2023 р.

Завідувач кафедри
_____ В.В.Яцків

ТЕРНОПІЛЬ – 2023

Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки
Освітній ступінь «магістр»
спеціальність: 125 – Кібербезпека
освітньо-професійна програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ В.В.Яцків
«____» _____ 2022 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
КУСМАРЦЕВ ВОЛОДИМИР ІГОРОВИЧ

1. Тема кваліфікаційної роботи:
Алгоритми захисту об'єктів авторського права і суміжних прав на web-ресурсах / Algorithms for Protecting Copyright and Related Rights on Web Resources

керівник роботи: д.т.н., професор М.М. Касянчук

затверджені наказом по університету від 1 грудня 2022 року № 491

2. Строк подання студентом закінченої кваліфікаційної роботи 1 грудня 2023 р.

3. Вихідні дані до кваліфікаційної роботи: завдання на кваліфікаційну роботу студента, наукові статті, технічна література.

4. Основні питання, які потрібно розробити:
– огляд та аналіз проблематики технічного характеру для захисту об'єктів на веб-ресурсах;
– огляд нормативної складової у регулюванні авторського права у кіберпросторі;
– розробка комплексного алгоритму захисту об'єктів авторського права на веб-ресурсах;
– дослідження можливостей сучасних IT-рішень для реалізації алгоритму захисту об'єктів авторського права в мережі Інтернет.

5. Перелік графічного матеріалу у роботі:
– схеми хеш-технологій;
– схеми блокчейн систем;

– огляд перцепційних-хеш функцій;
– табличний аналіз технічних рішень.

6. Консультанти розділів кваліфікаційної роботи

	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання 8 грудня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Авторське право та суміжні права у кіберпросторі	12.2022 р. – 03.2023 р.	
2	Захист об’єктів авторського права та суміжних прав на веб-ресурсах	03.2023 р. – 05.2023 р.	
3	Інноваційні алгоритми для захисту авторського і суміжних прав на веб-ресурсах	05.2023 р. – 11.2023 р.	

Студент _____ Кусмарцев В.І.
(підпис)

Керівник роботи _____ д.т.н., професор М.М. Касянчук

АНОТАЦІЯ

Випускна кваліфікаційна робота на тему „Алгоритми захисту об’єктів авторського права і суміжних прав на web-ресурсах” на здобуття освітнього ступеня «Магістр» зі спеціальності 125 „Кібербезпека” освітньо-професійної програми «Кібербезпека» написана обсягом 89 сторінок і містить 19 ілюстрацій, 4 таблиці, 1 додаток та 40 джерел за переліком посилань.

Метою випускної кваліфікаційної роботи є розробка комплексного алгоритму захисту авторських прав на веб-ресурсах.

Методи дослідження. Аналітичний метод, компаративний (порівняльний) метод, метод синтезу, експериментальний метод, структурний аналіз.

Результати дослідження: Здійснено комплексний аналіз проблематики захисту авторського та суміжних прав на веб-ресурсах, включаючи технічний та правовий аспект. Виділено основні проблеми та описано алгоритм виходу на систематичне вирішення комплексного завдання щодо захисту інтелектуальної власності на веб-ресурсах.

Результати роботи можуть успішно застосовуватися для запровадження системного підходу для юридично-правового забезпечення захисту об’єктів авторського і суміжних прав на веб-ресурсах.

Ключові слова: АВТОРСЬКЕ ПРАВО, КІБЕРПРОСТІР, ІНТЕЛЕКТУАЛЬНА ВЛАСНІСТЬ, БЛОКЧЕЙН, ДЕЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ ПРАВАМИ.

ABSTRACT

The graduation thesis on the topic "Algorithms for Protecting Copyright and Related Rights on Web Resources" for the degree of "Master" in the specialty 125 "Cybersecurity" of the educational-professional program "Cybersecurity" is written on 89 pages and contains 19 illustrations, 4 tables, 1 appendix, and 40 sources in the list of references.

The purpose of the graduation thesis is to develop a comprehensive algorithm for the protection of copyright on web resources.

Research methods: Analytical method, comparative method, synthesis method, experimental method, structural analysis.

Research results: A comprehensive analysis of the issues related to the protection of copyright and related rights on web resources, including technical and legal aspects, has been carried out. The main problems are identified and an algorithm is described for the systematic solution of the complex task of protecting intellectual property on web resources.

The results of the work can be successfully applied to implement a systematic approach for the legal protection of copyright and related rights on web resources.

Key words: COPYRIGHT, CYBERSPACE, INTELLECTUAL PROPERTY, BLOCKCHAIN, DECENTRALIZED RIGHTS MANAGEMENT.

ЗМІСТ

ВСТУП

У сучасному світі із швидким розвитком цифрових технологій особливо важливою стає актуальність захисту авторських та суміжних прав у кіберпросторі, в тому числі на веб-ресурсах.

Метою даного дослідження є розробка оптимальних методів і прийомів для захисту цих прав на веб-ресурсах, з урахуванням сучасних технологій, таких як блокчейн, хеш-функції, та цифрові водяні знаки.

Об'єктом дослідження є процеси захисту інтелектуальної власності в інтернет-просторі, з увагою до всіх їх взаємозв'язків і нюансів. Предмет дослідження включає в себе аналіз і оцінку існуючих та потенційних методів захисту цих прав.

Використовуючи **методи аналітичного дослідження,** порівняльного аналізу та синтезу, дослідження прагне виявити найефективніші способи захисту та управління цифровим контентом. Наукова новизна полягає у розробці інтегрованого підходу, який враховує технологічні та юридичні аспекти, а також у визначенні найкращих практик у цій сфері.

Для досягнення мети ставились наступні **завдання**:

- аналіз існуючого стану захисту авторських та суміжних прав на веб-ресурсах;

- розгляд юридичних та технічних аспектів цієї проблематики;

- виявлення викликів юридичного захисту;

- оцінка основних проблем та викликів, з якими стикається захист авторських прав в Інтернеті, включаючи глобальний характер мережі, анонімність користувачів, відсутність уніфікованих стандартів тощо;

- вивчення технічних обмежень існуючих методів захисту;

- аналіз технічних обмежень, таких як хешування, блокчейн, та цифрові водяні знаки, та їх застосування у захисті авторських прав;

- розробка комбінованого алгоритму захисту, пошук нових підходів до захисту авторських та суміжних прав, що включають використання комбінації різних технологій та методів;

- обгрунтування відмови від централізованих систем управління правами для переходу до децентралізованих систем з метою підвищення безпеки, прозорості та масштабованості;

- аналіз та вибір оптимальної блокчейн-платформи, визначення найбільш підходящої блокчейн-технології з огляду на економічну вигідність та надійність;

- стандартизація з метою впровадження методів захисту, розробка та реалізація стандартів для хешування та використання цифрових водяних знаків;

- аналіз та обгрунтування можливості комбінування функцій хешування та цифрових водяних знаків з метою розробки інтегрованої системи захисту, що включає множинні технології для забезпечення надійного захисту авторських прав у цифровому середовищі.

Практичне значення дослідження виявляється у можливості його застосування в індустрії цифрових технологій та інтелектуальної власності, а також у підвищенні обізнаності та компетенцій авторів і власників прав у цифровому просторі.

Публікації та апробація КР.

1. Кусмарцев В.І., Дослідження кіберзагроз для об’єктів авторського та суміжних прав. Збірник матеріалів науково - практичної конференції молодих вчених, аспірантів та студентів «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ-2023), Тернопіль, 2023. С.90-92

2. Кусмарцев В.І., Несанкціонований доступ до веб-ресурсів та його особливості. Матеріали науково-практичного симпозіуму «Захист інформації». Тернопіль, 2023. С.104-107

1 АВТОРСЬКЕ ПРАВО ТА СУМІЖНІ ПРАВА У КІБЕРПРОСТОРІ

1.1 Будова та сучасний стан розвитку кіберпростору

Історія розвитку кіберпростору включає в себе ряд ключових подій та етапів, що відображають еволюцію використання технологій та Інтернету.

Початки Інтернету – 1960-1970 рр.. Ранній етап включав створення ARPANET, першої мережі, яка використовувалася для обміну інформацією між вченими. Це був фундамент для розвитку подальших мереж[39].

Створення та запуск World Wide Web – 1990 рр.. Тім Бернерс-Лі створив WWW (World Wide Web), що полегшило доступ до інформації та взаємодії в Інтернеті. Це відкрило нові можливості для комунікації та спільної роботи[39].

Поширення електронної комерції – 1990-2000 рр.. З'явилися перші електронні комерційні платформи, що призвело до збільшення онлайн-торгівлі та передачі фінансової інформації через Інтернет.

Зростання загроз кібербезпеки та розвиток соціальних мереж – 2000-теперішній час. Розширення використання технологій стало супроводжуватися загостренням кіберзагроз. Це включає в себе атаки на комп'ютерні системи, витоки даних, шкідливі програми та інші загрози кібербезпеки. Поява популярних соціальних мереж, таких як Facebook, Twitter, та інших, змінила спосіб спілкування та обміну інформацією.

Зростання хмарних технологій та розвиток Інтернету речей (IoT) – 2010-теперішній час. Хмарні технології дозволяють зберігати та обробляти великі обсяги даних в інтернет-хмарах, забезпечуючи зручний та ефективний доступ до ресурсів. Поява підключених до Інтернету пристроїв в домашньому та промисловому середовищі, що розширило мережу зв'язку та введення нових викликів у сфері кібербезпеки.

Інтернет 5G та розвиток штучного інтелекту – 2020-тепершній час. Розвиток технології 5G та розширення мережі IoT сприяють збільшенню швидкості та обсягів обміну даними. Штучний інтелект використовується для аналізу даних, кіберзахисту та автоматизації багатьох процесів в кіберпросторі.

Розвиток кіберпростору відбувався разом із зростанням технологій та інновацій, але при цьому виникали нові виклики, такі як питання кібербезпеки, приватності та етики використання технологій.

Сучасний кіберпростір – це складний та динамічний комплекс, який включає в себе різноманітні елементи, інфраструктуру та динаміку взаємодії. Це мережева інфраструктура, системи зберігання даних, хмарні технології, центри обробки даних, апаратне забезпечення, системи програмного забезпечення, інтерфейси та користувацькі пристрої, програми для кіберзахисту, тощо.

Ці складові взаємодіють між собою, створюючи складну та взаємозалежну систему, що потребує системного підходу до кібербезпеки та ефективного управління ризиками.

Ось кілька напрямків та технологій, які станом на зараз найбільш актуальні кіберпросторі: штучний інтелект (ШІ), когнітивні системи та розумні агенти, кібербезпека, квантова криптографія, інтернет речей та їх безпека (IoT), комп'ютерні мережі та 5G, блокчейн та криптовалюти, розширення застосувань блокчейну.

Ці технології представляють лише частину того, що відбувається в кіберпросторі, і їх розвиток продовжується. Кіберпростір є постійно змінюваною областю, і нові інновації постійно виникають для вирішення нових завдань та викликів.

Серед держав найбільший вплив на управління інтернетом та кіберпростором залишають за собою Сполучені Штати, що склалося історично із їхнім розвитком. Так, перший законодавчий акт Конгресу «Про високопродуктивні обчислення», прийнятий у 1991 р. за президентства Клінтона, ідеологом якого був віце-президент Альберт Гор, значною мірою вплинув на подальший розвиток інтернету, створивши правову базу для його приватизації та комерціалізації послуг [27].

Отже, стає зрозуміло, що кіберпростір – це новий вимір, який існує паралельно із реальністю та доповнює наше соціально-економічне буття. З технічної ж точки зору це складна система технологічних та програмних засобів, яка не має фактичних кордонів та обмежується лише технологіями (програмним

кодом, пропускною здатністю мереж, продуктивністю серверної частини, продуктивністю клієнтських пристроїв, тощо).

Сучасний кіберпростір також характеризується сегментованістю, яка виявляється у різних формах: від географічної, де контент адаптується під конкретні регіони, до політико-правової, з різними законами та цензурою в різних країнах. Технологічна сегментованість створює різні "екосистеми", залежно від платформ та пристроїв, а економічна сегментованість визначає доступ до сервісів залежно від фінансових можливостей. Соціально-культурні та мовні відмінності поділяють інтернет на нішеві спільноти, кожна з яких має свої унікальні звичаї та інтереси. Ця різноманітність формує складний та багатогранний ландшафт кіберпростору.

Актуальний етап розвитку кіберпростору переживає динамічний розвиток завдяки прогресу в таких областях як штучний інтелект та машинне навчання, що підвищують інтелектуальність та адаптивність цифрових систем, а також Інтернету речей, який збільшує взаємодію між фізичним і віртуальним світами. Розвиток розширеної та віртуальної реальності відкриває нові горизонти для інтерактиву, тоді як блокчейн та криптовалюти вносять зміни в сферу безпеки, прозорості та економічних відносин. Паралельно, розвиток 5G та швидкісних інтернет-технологій сприяє покращенню з'єднання та доступу до великих даних, а перспективи квантових комп'ютерів віщують радикальні зміни в обчислювальних можливостях, що має потенціал глибоко трансформувати кіберпростір.

Технологічний прогрес сьогодні відбувається з неймовірною швидкістю, впроваджуючи нові інновації та можливості майже щодня. Однак, цей стрімкий розвиток часто зіштовхується з відставанням нормативної бази та регулювання. Законодавчі та регуляторні органи зазвичай реагують на технологічні зміни з певним запізненням, що створює прогалини в правовому полі та викликає важливі питання щодо приватності, безпеки, етики та соціальної відповідальності. Це відставання може призвести до розриву між тим, що технологічно можливо, і тим, що регульовано та захищено законом, створюючи виклики для користувачів, компаній та суспільства в цілому. Таким чином, існує очевидна необхідність в

більш швидкій адаптації правових та нормативних рамок до швидкозмінної технологічної реальності.

Справді, важливим аспектом сучасного технологічного розвитку є не тільки врахування відставання нормативного регулювання, але й активне використання технологій для підтримки та поліпшення цього регулювання. Технологічні рішення можуть надавати інструменти для більш ефективного збору даних, аналізу, моніторингу дотримання правил, а також сприяти прозорості та відкритості у взаємодії між державою, бізнесом та громадянами.

Інтелектуальні аналітичні системи та алгоритми машинного навчання можуть допомогти в розробці більш точних та адаптивних нормативних рамок, які враховують змінні умови та потреби суспільства. Цифровізація процесів урядування дозволяє підвищити ефективність та доступність державних послуг. Також, технології блокчейн можуть бути використані для втілення безпечності, незмінності та прозорості управлінських рішень та транзакцій.

Отже, інтеграція технологічних рішень у процеси нормативного регулювання є ключовою для забезпечення того, аби правові рамки залишались актуальними, ефективними та відповідними до швидкоплинних змін сучасного світу.

Підсумовуючи історію розвитку кіберпростору можна підкреслити його динамічну і постійно еволюціонуючу природу. Від ранніх днів ARPANET до сучасного світу 5G, штучного інтелекту та Інтернету речей, кіберпростір продемонстрував неймовірну здатність до адаптації та інновацій. Цей процес розвитку відбивається не тільки в технологічному прогресі, але й у соціальних, економічних та політичних змінах, що впливають на глобальне суспільство.

З одного боку, розвиток кіберпростору сприяв виникненню нових форм комунікації, співпраці, комерції та розваг, зміцнюючи глобальну інтеграцію та взаємозв'язок. Проте, з іншого боку, цей прогрес породив виклики, пов'язані з кібербезпекою, приватністю, етикою використання технологій та інформації, а також з необхідністю адаптації правових та нормативних рамок.

Сучасний кіберпростір представляє собою складну, взаємопов'язану систему, що охоплює технологічні, соціальні, економічні та політичні аспекти. Його безперервний розвиток та зміни вимагають гнучкого підходу та інноваційного мислення для вирішення нових завдань та викликів. В кінцевому рахунку, кіберпростір продовжує бути динамічною сферою, що формує наше сучасне суспільство та спосіб життя, водночас пропонуючи безмежні можливості для майбутнього розвитку.

1.2 Проблеми захисту авторських прав породжені розвитком кіберпростору

Розвиток інтернету та супутніх технологій змінює соціально-економічні моделі але нормативно-правова база не встигає адекватно реагувати на ці зміни. Сучасне право залишається відсталим від цифрової революції і йому потрібен час для адаптації. Тим часом ті, хто вже працює з цифровими технологіями, повинні усвідомлювати юридичні умови та наслідки своєї діяльності в інтернеті, оскільки майбутнє регулювання цього простору хоч і залишається невизначеним, але все ж невідворотнє. Система інтелектуальної власності має еволюційний характер. Хоча природа самих прав на контроль і використання продуктів творчості та інновацій залишається відносно сталою, спосіб їх вираження та обміну постійно адаптується із розвитком базових технологій.

Варто підкреслити, що в міру того, як технологічні інновації, такі як розподілені обчислення (distributed computing), блокчейн та квантове кодування, все більше впроваджуються у повсякденне життя, виникає гостра необхідність в адаптації правових рамок, щоб забезпечити їх відповідність сучасним реаліям. Це включає у себе забезпечення захисту цифрових прав, регулювання використання великих даних (big data), штучного інтелекту (AI), машинного навчання (ML) та Інтернету речей (IoT).

В контексті системи інтелектуальної власності, важливо враховувати нові виклики, пов'язані з авторським правом у цифрову епоху, особливо з урахуванням поширення цифрових технологій, які дозволяють легке копіювання та

розповсюдження контенту. Окрім цього, слід враховувати питання щодо захисту персональних даних, зокрема в контексті GDPR (General Data Protection Regulation) та інших міжнародних стандартів.

Виклики, що постають перед правовою системою, також включають необхідність розробки законодавства, що регулює використання криптовалют, смарт-контрактів, а також вирішення юридичних питань, пов'язаних із автоматизованими системами прийняття рішень, заснованими на AI.

Таким чином, майбутнє регулювання кіберпростору вимагає інтеграції комплексного підходу, який би враховував як технічні аспекти новітніх технологій, так і їх соціально-економічні наслідки, а також питання кіберетики та цифрової моралі.

Сучасна наука виділяє основні труднощі для авторського права у мережі Інтернет:

- неузгодженість законодавства в сфері інтелектуальної власності, відсутність спеціальних норм для регулювання інтернет- відносин, невідповідність норм сучасним реаліям;

- відсутність спеціалізованого судочинства, а саме в цьому разі нефункціонування Вищого спеціалізованого суду з питань інтелектуальної власності;

- низький рівень правової культури громадян, упевненість у правомірності своєї поведінки та боротьба за вільний доступ до інформації в мережі Інтернет;

- низький рівень підготовки державних службовців та програмістів;

- недостатнє фінансування з боку держави заходів щодо боротьби з піратством;

- анонімність користувачів мережі Інтернет, що робить складним або неможливим пошук винуватих у правопорушенні осіб;

- недостатній рівень знань авторів та правоволодільців у сфері захисту авторського права;

- швидкість розповсюдження неліцензійної продукції мережею Інтернет;

- складність фіксації доказів у мережі Інтернет та недостатність технологічного забезпечення осіб, які перешкоджають правопорушенням;

- негативна роль інтернет-посередників у порушенні авторських прав на твори, розміщені в мережі Інтернет [36].

Після появи ринку гіпертекстових ресурсів і популяризації інформаційних послуг інформаційне суспільство розвивається передусім шляхом "інтернетизації", тобто переведення суспільних відносин на платформу Інтернету. Щодня до мережі приєднується близько мільйона нових користувачів. І в 2019 р., за даними Міжнародного телекомунікаційного союзу (ITU), кількість користувачів інтернету перевищила 4 млрд, що становить 51 % від усього населення Землі. До 2030 р. світ досягне показника 7,5 млрд користувачів глобальної мережі. "Інтернетизація" ґрунтується на впровадженні популярних форматів і засобів обробки інформації й телекомунікації в поєднанні з технологічною конвергенцією, завдяки чому активно розвивається ринок інформаційно-комунікаційних технологій і масовий ринок послуг, що постачаються цифровим шляхом [40].

Фактично Інтернет створив прецедент одного єдиного цілісного простору в масштабі планети, де доводиться впроваджувати єдині правила, технологічні та юридичні стандарти, але через такий масштаб – це надзвичайно складно і з кожним днем швидкісної технологічної еволюції. – наближається до неможливого.

З огляду на вищеокреслені тезиси, можемо однозначно констатувати той факт, що глобалізація як явище надвичайно сильно почала рухатись вперед саме завдяки розвитку Інтернету, а суспільство перетворюється в кіберсуспільство, де Інтернет проникає у всі сфери життя. Це новий спосіб взаємодії, де персональна участь у створенні та поширенні контенту дозволяє реалізувати особистий потенціал. Це відкриває можливості для підприємництва та розвитку громадянського суспільства, але також створює загрози. Кіберпростір сприяє розвитку особистості та бізнес-проєктів, але також наростає конкуренція на ринку і на міжнародному рівні.

Інтелектуальна власність масштабно та невідворотньо перекочувала в Інтернет і модифікується відповідно до онлайн-середовища. Оцифрування творів

інтелектуальної власності за допомогою процесу, який перетворює текст, візуальні зображення та звук до зчитуваного комп'ютером двійкового коду «0» та «1», призвело до створення цифрових продуктів, які можуть переміщатися по мережі у кіберпросторі. Цю міграцію інтелектуальної власності в Інтернет можна спостерігати щодо кожного виду прав, але переважно міграція найкраще помітна у випадку авторського права та торгових марок.

Компанія International Data Corporation (IDC) оприлюднила прогноз щодо глобальної ІТ-галузі: йдеться про витрати на цифрову трансформацію організацій, продуктів та бізнес-практик. Нині більше половини (3,9 млрд) світового населення підключено до Інтернету, який є найбільш відкритим глобальним інформаційним суспільством. Роль інтелектуальної власності (ІВ) та цифрової інфраструктури обороту прав ІВ стає ключовим чинником, що визначатиме зростання національних економік. Передумови для цього створені розвитком глобальних цифрових мереж, де понад 70 % трафіку становить рух об'єктів ІВ. Про зростання ролі сфери ІВ у глобальному вимірі свідчить останній Звіт Всесвітньої організації інтелектуальної власності – World Intellectual Property Report 2022 (WIPR). За 35 років потроїлася кількість інновацій, пов'язаних з комп'ютерною технікою та суміжними галузями (ІКТ), на цей сектор припадає майже чверть усіх патентів, а щорічні темпи зростання становили 8 %. Нова революція у сфері інновацій пов'язана з цифровізацією, яка зумовлює трансформацію цілих галузей. Кількість цифрових інновацій зросла в чотири рази. На цей сектор припадає 12 % усіх патентних заявок, а щорічні темпи зростання патентної активності становлять 13 % [35].

Багато компаній на етапі початкового розвитку інтернету дотримувалися підходу, згідно з яким спочатку було важливіше зробити свою продукцію доступною, і таким чином закріпити присутність на ринку, а потім вирішити питання прибутку та прибутку на пізнішому етапі. Ентузіазм, викликаний доступністю такої кількості онлайн-інформації, легко доступної через веб-ресурси, посприяв формуванню поведінкової думки споживачів, що ця інформація безкоштовна, а її використання неконтролюються. Отже, однією із проблем є

очікування багатьох користувачів, що інформація та інтелектуальна власність, доступні на вер-ресурсах, безкоштовні вільні для споживання та користування.

Власники прав, як-от творці фільмів і музики, розробники програмного забезпечення, автори та видавці, зараз шукають способи зробити свої продукти доступними в Інтернеті, одночасно захищаючи свої права та окупаючи свої інвестиції. Певною мірою впровадження платних послуг інтелектуальної власності залежить від ефективного управління цими правами, а також від наявності робочих і безпечних методів мікроплатежів, які дозволять здійснювати покупки за одиницю, а також створення впевненості споживачів у безпеці онлайн-платежів та покупок, конфіденційності та захисту споживачів. Отже, ще одна проблема полягає в тому, що власники прав інтелектуальної власності хочуть відчувати себе в безпеці та бути впевненими, що вони можуть захистити свою власність від піратства та контролювати її використання, перш ніж вони захочуть зробити її доступною в Інтернеті.

Загальні тенденції щодо порушення авторського права можна відслідкувати за рівнем зростання піратства в порівнянні із 2021 до 2022 року на прикладі фільмів, телебачення, публікацій, музики та програмного забезпечення на рисунку 1.1.

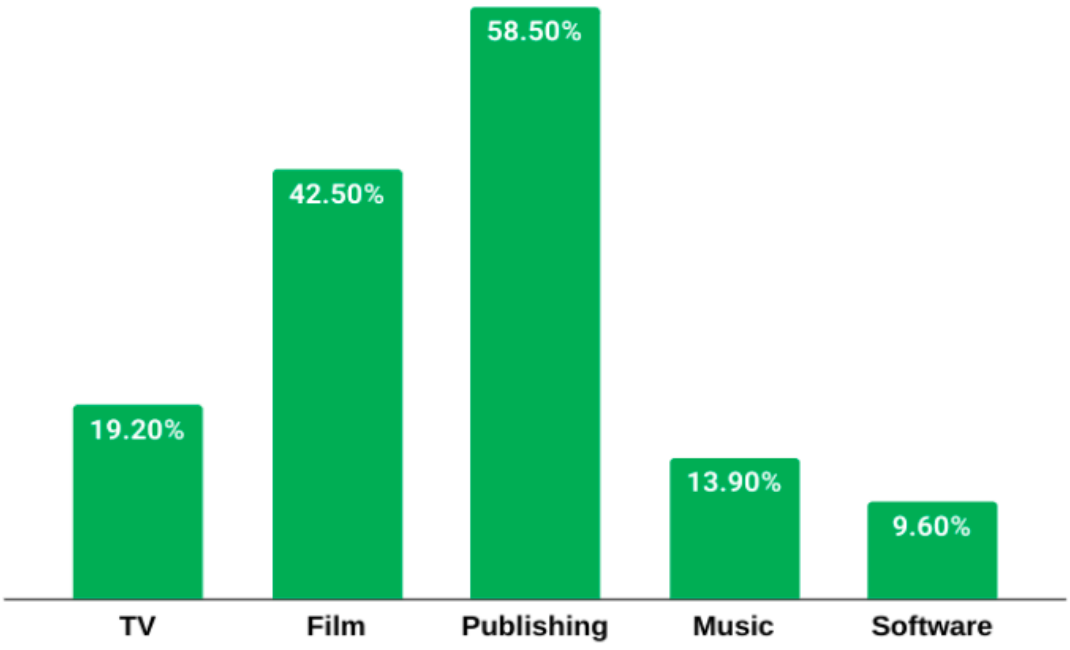


Рисунок 1.1 – Статистика зростання піратства у 2021-2022рр.[22]

Частково ці тенденції пов’язані із поширенням стрімінгових сервісів та їхньою популяризацією, переходом багатьох гігантів щодо розробки програмних продуктів на комерційну модель підписок на продукт. Великі медіа-сервіси усіляко обмежують можливості для споживання ліцензійного контенту за межами їхніх сервісів, де це можливо лише за оплату, а жага безкоштовно отримати щось вартісне нікуди не зникала у пересічних громадян, які до того ж насправді можуть справді не мати достатній матеріальний рівень власного забезпечення аби дозволити собі ліцензійний продукт. Програмні продукти як для прикладу Adobe – вже неможливо придбати разово і отримати доступ до ліцензії назавжди, а вартість підписки на місяць – достатньо дороговартісна для мешканців не найбільш забезпечених країн.

З іншого боку згадана нами тенденція глобалізації суттєво впливає на масштаби розповсюдження будь-якого із об’єктів авторського права, а порушник може бути за межами юрисдикції власника авторського права. І фактично попри наявність усіх нормативно-правових стверджуючих фактів наявності у автора прав – це не гарантує їхню захищеність та можливість компенсації чи припинення порушення.

Незліченна кількість творів літератури, кіно та мистецтва, а особливо комп’ютерних програм, уже масово оцифровано. Адже будь-який текстовий твір ідеально підходять для оцифрування, а попит на електронні книги зростає. Численні журналісти та письменники-початківці займаються публікаціями в Інтернеті, щоб розміщувати блоги, веб-журнали чи журнали, які дозволяють людям оприлюднювати свої погляди для громадськості без потреби в посередництві великих видавництв чи дистриб’юторів. У сфері образотворчого мистецтва, місцевих ремесел і артефактів численні музеї та художні галереї оцифрували свої колекції та зробили їх доступними для перегляду в Інтернеті.

Важливість дослідження нашої теми підкреслюється юридичною природою авторського та суміжного прав. Дані поняття існують та розвиваються у юридичній науці і практиці, у сучасному національному та міжнародному законодавстві, але не відбувається паралельного розвитку розуміння юридичною спільнотою

тенденцій розвитку технологій і відповідного швидкого реагування в нормативному плані, які впливають на право інтелектуальної власності. У наступних розділах ми розглянемо практичну сторону юридичного захисту авторського та суміжних прав більш детально, але якщо узагальнити – це дуже складний, довгий та не гарантуючий успіх процес. Кіберпростір занадто багатошаровий та масштабний для легкого вирішення проблем захисту об’єктів авторського і суміжних прав на веб-ресурсах, але в той же час – кіберпростір – єдиний (якщо не брати до уваги даркнет).

1.3 Об’єкти авторського права що доступні на web-ресурсах

Авторське право захищає різноманітні об'єкти інтелектуальної діяльності, які можуть бути доступні через Інтернет. Ось декілька основних об'єктів авторського права, які можуть розміщуватись на веб-ресурсах (хоч і список не є вичерпним):

- текстовий контент: це можуть бути статті, блоги, електронні книги, новини та інші види письмових робіт;
- зображення та графіка: фотографії, малюнки, діаграми, інфографіка та інші візуальні твори;
- відеоматеріали: це включають в себе відеофільми, анімаційні ролики, відеоблоги тощо;
- аудіоматеріали: музика, аудіокниги, подкасти, радіопередачі та інші звукові записи;
- програмне забезпечення та бази даних: це можуть бути комп'ютерні програми, мобільні додатки, веб-сайти та їх компоненти, а також бази даних;
- мультимедійні презентації та інтерактивний контент: це можуть бути онлайн-курси, електронні виставки, ігри тощо.

Кожен з цих типів контенту може бути захищений (і формально захищається) авторським правом. Авторське право надає авторам або правовласникам певні виняткові права, такі як право на відтворення, розповсюдження, публічне виконання, показ, переклад та адаптацію своїх творів [37]. Важливо дотримуватися

цих прав при використанні матеріалів, знайдених в Інтернеті, і отримувати відповідний дозвіл або використовувати контент відповідно до умов ліцензій.

Безпосереднє розміщення будь-якого із вищеперерахованих об’єктів авторського права – це автоматичне відкриття доступу до нього для усього кіберпростору. Тож окрім переліку самих об’єктів варто розуміти орієнтовний перелік можливих для розміщення веб-ресурсів. Існує великий перелік , який задовільняє потреби та інтереси людей і де будь-який із об’єктів авторського та суміжних прав може бути розміщений. Варто виділити декілька основних категорій:

- інформаційні та новинні сайти, які предоставляють актуальні новини, аналітичні матеріали, статті на тему поточних подій. Приклади включають сайти таких новинних агентств, як BBC, CNN, Reuters;
- освітні Ресурси, які пропонують онлайн-курси, лекції, навчальні матеріали, опулярні платформи включають Coursera, Khan Academy, EdX;
- наукові та дослідницькі ресурси, академічні журнали, наукові бази даних та бібліотеки, що надають доступ до наукових статей і досліджень. Наприклад, Google Scholar, JSTOR, PubMed;
- соціальні мережі, платформи для спілкування, обміну контентом і мережевої взаємодії. До них відносяться Facebook, Twitter, Instagram, тощо;
- електронна комерція – для онлайн-покупок, які пропонують широкий асортимент товарів та послуг. Приклади включають Amazon, eBay, AliExpress, OLX;
- розважальні сайти – стрімінгові сервіси фільмів та серіалів (Netflix, Hulu), музичні платформи (Spotify, Apple Music), ігрові портали;
- форуми та спільноти, платформи для обговорення, обміну досвідом і знаннями з однодумцями, популярні форуми включають Reddit, Quora, спеціалізовані форуми за інтересами;
- логи та персональні веб-сайти – індивідуальні або групові блоги, що пропонують персональні статті, блоги про подорожі, кулінарію, технології тощо;

- офіційні урядові сайти та сервіси – цифрові портали урядових установ, що надають інформацію та послуги громадянам;
- інструменти та утиліти – онлайн-інструменти для різних цілей, включаючи перевірку граматики, конвертацію файлів, обробку даних.

Кожен з цих ресурсів має свої унікальні функції та призначення, допомагаючи користувачам здійснювати пошук інформації, вчитися, спілкуватися, робити покупки та насолоджуватися різноманітним контентом, а будь-яка взаємодія із ними – це завжди доступ до об’єктів авторського права в тому чи іншому вигляді.

Об'єкти авторського права в контексті комп'ютерних систем – це будь-які дані або контент, які можуть бути цифрово збережені та оброблені. І важливо в контексті розуміння розміщення інтелектуальної власності на веб-ресурсах дослідити також об’єкти авторського права з технічної точки зору.

Комп'ютер "бачить" інформацію на веб-сайтах не так, як людина. Він інтерпретує веб-сторінки як дані, що складаються з різних компонентів.

HTML (HyperText Markup Language) – основна мова розмітки, яка визначає структуру веб-сторінки. Комп'ютер читає HTML-код, щоб розуміти розташування тексту, зображень, посилань та інших елементів.

CSS (Cascading Style Sheets) – використовується для оформлення веб-сторінок. Комп'ютер застосовує ці стилі для визначення вигляду елементів, наприклад, кольорів, шрифтів та розмірів.

JavaScript мова програмування дозволяє створювати інтерактивні елементи на веб-сторінках. Комп'ютер виконує JavaScript-код для реалізації динамічних функцій, таких як вспливаючі вікна, анімації, перевірка форм та інше.

Для зображень та мультимедіа комп'ютери використовують специфікації файлів зображень (наприклад, JPEG, PNG) та мультимедіа (наприклад, MP4) для відображення цих елементів на веб-сторінці.

HTTP/HTTPS протоколи комп'ютер використовує для спілкування з серверами та отримання або передачі даних веб-сторінок.

Метадані такі як теги `<meta>` у HTML, які можуть містити інформацію про веб-сторінку, яка не відображається безпосередньо, але використовується для пошукових систем та інших технічних цілей.

Всі ці компоненти обробляються веб-браузером, який перетворює ці коди та інструкції на візуальний формат, зрозумілий для людини.

Прикладом веб-сторінки варто розглянути веб-сайт технологічного гіганта Apple, як приклад зразкового правовласника на об’єкти інтелектуальної власності, що розміщені на їхньому веб-порталі за адресою www.apple.com. На рисунку 1.2 можемо бачити вигляд веб-сайту для пересічного користувача у вікні веб-браузера, де із об’єктів авторського та суміжних прав можна побачити – торгові марки, шрифти, зображення, на рисунку 1.3 це й же веб-сайт, але з точки зору програмного коду, який розуміє та інтерпретує комп’ютер і який також є об’єктом охорони:

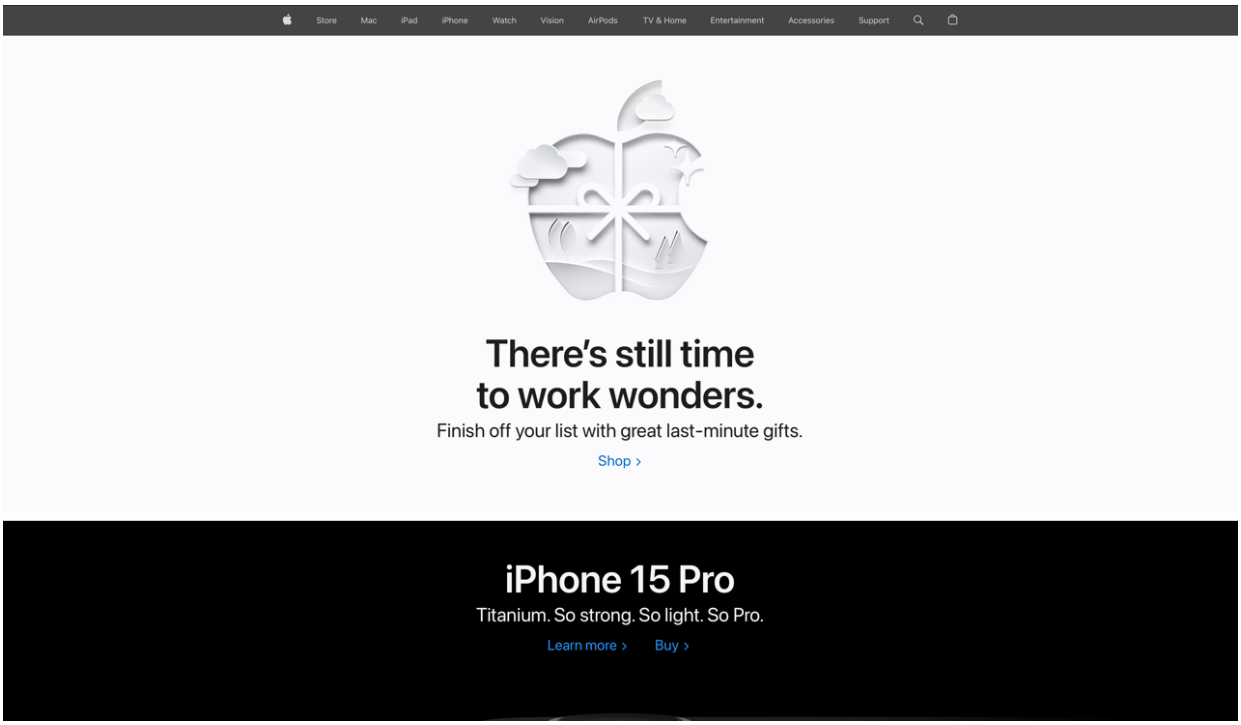


Рисунок 1.2 – Приклад візуальних об’єктів авторського права [17]

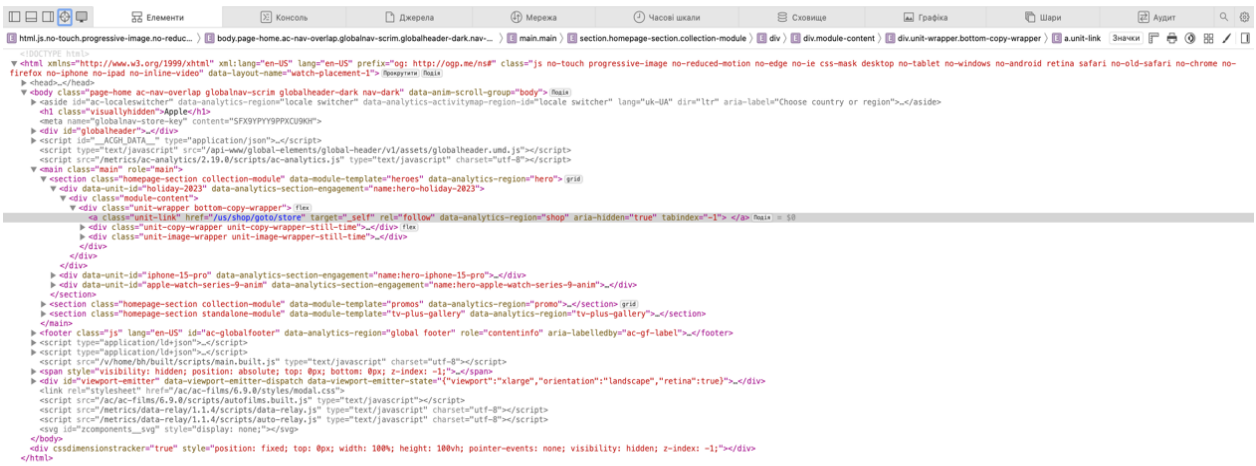


Рисунок 1.3 – Вихідний код як об’єкт авторського права [17]

Як видно на цих зображеннях – об’єкти авторського права на веб-ресурсах – це доволі різноманітний перелік можливих варіантів. Починаючи від самого вихідного коду веб-ресурсу і закінчуючи навіть шрифтами на ньому.

Узагальнюючи потрібно відзначити те, що з точки зору IT, об'єкти авторського права, які розміщені на веб-ресурсах легко копіюються та розповсюджуються. Цифровий контент можна легко і швидко копіювати без втрати якості. Це означає, що музику, зображення, тексти та інші види контенту можна незаконно розповсюджувати з великою швидкістю і масштабом. Важко індентифіковувати порушення, адже виявляти порушення авторських прав у цифровому просторі може бути складно – контент може бути змінений, переформатований або вбудований у інший контент. Інтернет не знає кордонів, тому контент, що порушує авторські права, може легко перетинати національні межі, що ускладнює правове регулювання. Інтернет забезпечує авторам можливість легкого та широкого розповсюдження їхніх творів, але водночас збільшує ризик незаконного використання рівно на той масштаб, який осягає інтернет.

2 ЗАХИСТ ОБ’ЄКТІВ АВТОРСЬКОГО ПРАВА ТА СУМІЖНИХ ПРАВ НА ВЕБ-РЕСУРСАХ

2.1 Правові способи захисту авторського права та суміжних прав на веб-ресурсах

Правові способи захисту об'єктів інтелектуальної власності на веб-ресурсах включають у себе наступний перелік юридично-технічних способів із доступних на сьогодні:

- реєстрація прав – це може бути авторське право, патенти, торговельні марки, реєстрація забезпечує визнання та офіційний захист прав;

- юридичні попередження та повідомлення на веб-сайті, які повідомляють про правовласника і забороняють несанкціоноване використання;

- моніторинг та виявлення порушень – постійне спостереження за інтернетом, щоб виявляти несанкціоноване використання ваших творів;

- звернення до пошукових систем та хостинг-провайдерів якщо виявлено порушення з проханням видалити контент або заблокувати доступ до нього;

- правові дії у разі серйозних порушень – можна вдатися до судових позовів для захисту своїх прав;

- ліцензування та угоди для встановлення чітких умов використання вашої власності, що можуть включати ліцензійні угоди.

Захист інтелектуальної власності в Інтернеті вимагає активного підходу та розуміння відповідного законодавства. Одночасно важливо відмітити, що авторське право на фото, відео та аудіотвори, програмний код – у більшості випадків виникає у автора в момент створення за винятком окремих випадків у відповідності до законодавства [37].

Узагальнений опис процедури реєстрації авторських прав включає наступні етапи: ідентифікація об'єкта, перевірка оригінальності, підготовка документації, вибір відповідного органу, оплата зборів, очікування на обробку заявки, отримання свідоцтва. Ця процедура може відрізнятися залежно від країни, а також від типу об’єкта, який реєструється і займає доволі тривалий час.

Одним із нормативино-правових інструментів є юридичні попередження та повідомлення на веб-сайтах, оскільки вони виконують важливу роль у захисті інтелектуальної власності та у регулюванні відносин із користувачами.

Попередження про авторські права вказують, що весь контент сайту, включаючи текст, графіку, логотипи, зображення тощо, захищено авторським правом. Часто вказують рік створення та ім’я власника прав. Розміщують повідомлення про обмеження відповідальності, інформуючи користувачів про те, що власник сайту не несе відповідальності за будь-які помилки чи неточності в контенті, а також за наслідки використання інформації з сайту. Заява про конфіденційність описує, як збираються, використовуються та захищаються особисті дані користувачів. Умови використання визначають правила та умови, за якими користувачі можуть використовувати сайт, включаючи заборону на несанкціоноване використання контенту.

Наступним інструментом захисту авторського та суміжних прав в мережі інтернет є моніторинг та виявлення порушень авторського права, і цей спосіб вимагає систематичного підходу та використання різних інструментів та стратегій.

Найпростіший – автоматизований моніторинг. Використання спеціалізованого програмного забезпечення, яке автоматично сканує Інтернет на предмет копій вашого контенту. Це може бути сканування тексту, зображень, аудіо та відео, програмних продуктів.

Можливе також виявлення через пошукові системи – регулярний пошук у Google або інших пошукових системах за ключовими словами, пов'язаними з вашим контентом, може допомогти виявити несанкціоноване використання.

Google Alerts можна налаштувати для творів, імен, торговельних марок або інших відповідних фраз, щоб отримувати повідомлення, коли вони з'являються в новому контенті в Інтернеті.

Сервіси моніторингу зображень, такі як TinEye або Google Reverse Image Search, дозволяють знаходити копії ваших зображень в Інтернеті.

Співпраця з провайдерами – подавання повідомлень про порушення авторських прав до веб-хостів для видалення порушуючого контенту відповідно до законодавства, як для прикладу DMCA (в США).

Залучення професіоналів або компаній, які спеціалізуються на моніторингу та захисті авторських прав в Інтернеті.

Підписка на спеціалізовані сервіси, які пропонують більш розширені можливості для виявлення та відстеження порушень авторських прав.

Використання цих методів моніторингу допоможе вам бути в курсі можливих порушень ваших авторських прав в Інтернеті і дозволить вжити заходів для їх усунення, але аж ніяк не передбачає того, шо це буде легко реалізувати. Оскільки окрім виявлення факту порушення після цього потрібно запустити юридичний механізм, де наступним із можливих є судовий захист.

Судовий спосіб захисту інтелектуальної власності розпочинається із підготовки та подачі позову. До порушника звертаються з вимогами: видалити контент, переделегувати домен або виконати інші дії, які відновлять права IT-компанії. Важливо довести, що ви власник прав на об’єкти інтелектуальної власності. Далі розгляд справи у суді і винесення рішення. Процес триває від року і довше. Позивач і відповідач можуть звернутися в апеляційний і касаційний суди для оскарження рішення [38].

Узагальнено ми сформували порівняльну таблицю 2.1 за критеріями складності реалізації, надійності та актуальності для сьогодення у кіберпросторі для охарактеризованих правових методів захисту інтелектуальної власності.

Ми поверхнево описали можливості юридичного захисту авторського і суміжного прав на об’єкти, що розміщено на веб-ресурсах. Насправді є багато тонкощів, а також є і проміжні варіанти захисту, але усі вони виходять із того, що права автора вже може бути порушено. Тобто, людина яка хотіла скористатись інтелектуальною власністю без відповідного дозволу на це, може доволі довго продовжувати порушувати законні права правовласника аж допоки не виявиться таке порушення і не буде вжито заходів. Виявлення такого порушення – окремий часовий проміжок. Відновлення порушених прав – також час. Ну і зрештою

часовий та матеріальний ресурс правовласника не завжди дозволяє взагалі починати юридичну процедуру припинення порушення та компенсації за заподіяну йому шкоду.

Таблиця 2.1 – Порівняльний огляд правових засобів захисту

Правові методи захисту	**Складність реалізації**	**Надійність захисту**	**Актуальність для сьогоднішніх умов кіберпростору**
Реєстрація прав	Середня	Висока	Висока
Юридичні попередження та повідомлення на веб-сайті	Низька	Середня	Висока
Моніторинг та виявлення порушень	Середня	Висока	Висока
Звернення до пошукових систем та хостинг-провайдерів	Середня	Висока	Висока
Правові дії у разі серйозних порушень	Висока	Висока	Висока
Ліцензування та угоди	Середня	Висока	Висока

Правові методи вимагають більше часу для впровадження та реакції на порушення, але забезпечують більш стійку та довгострокову правову основу для захисту чи відновлення порушених прав. Однак з огляду на те, що покарання за порушення авторських та суміжних прав не є невідворотнім, то сам факт існування правових обмежень не зупиняє від посягання на такі права, а отже не є гарантованим надійним превентивним засобом. А оскільки об’єкти авторського права та суміжних прав, що розміщені на веб-ресурсах, є у вільному доступі, то порушення цих прав для будь-якого із об’єктів є лише питанням часу, якщо не вжито більш переконливих заходів для попередження порушення чи полегшення встановлення такого факту для подальшого застосування санкцій та обмежень.

2.2 Технічні засоби захисту авторського права та суміжних прав на веб-ресурсах

Авторське та суміжні права на веб-ресурсах можна захистити у різний спосіб. У попередньому розділі ми розглянули загальний підхід, можливості та особливості для захисту юридичного поняття «авторське та суміжне право» у юридичній площині. Однак, як було описано нами вище, авторське та суміжі права із площини інтелектуальної власності не можуть існувати без юридичної характеристики та юридичного захисту, оскільки саме поняття права на авторство загалом виникло задовго до винайдення навіть телебачення чи радіо. І в той час скопіювати книгу на 600 сторінок за 1 секунду було неможливо, тож про це ніхто не задумувався. Те ж стосувалось і фільмів чи музики, адже носії аудіо- чи відео-творів були обмежені видами, а програвачі взагалі були дуже слабо поширені.

Дуже важливо для нашого дослідження описати загальні наявні вихідні умови, у яких існує кіберпростір та інтелектуальна власність у ньому, перш ніж більш детально охарактеризувати актуальні технічні способи захисту авторського права і суміжного права на веб-ресурсах.

Юриспруденція – специфічна галузь, оскільки закони первісно формувались зі звичаю, який походив від усталених норм взаємовідносин у суспільстві. І основна ідея та основні положення – тягнуться із далекого минулого, але постійно вдосконалюючись під актуальні реалії вимог того ж таки суспільства. Однак, що важливо, так це те якою складною і неповороткою є ця система, якщо порівняти із IT сферою. Ще 10 років назад для нас швидкість мобільного інтернету вище 2мбіт/с – видавалась фантастикою, а зараз 5G може пропускати цілий гігабіт в секунду. В той же час закон не пережив революції, оскільки в цілому суспільство все ще існує на нормах чорного і білого, хорошого і поганого. І юридична думка стосовно складних технологічних викликів все ще перебуває у розвитку, оскільки виклики сьогодення з’являються швидше, ніж їхні правові регулятивні рішення.

Станом на сьогодні більш-менш робочими рішеннями захисту інтелектуальної власності на веб-сайтах та в Інтернеті загалом з використанням сучасних IT-методів є наступні технології та підходи:

- цифрові водяні знаки для зображень, аудіо та відеофайлів, що дозволяє ідентифікувати автора або власника прав і відстежувати розповсюдження контенту;

- шифрування даних забезпечує, що тільки уповноважені особи можуть його переглядати або завантажувати;

- технологія блокчейн для створення незмінної і прозорої історії транзакцій, що допомагає відслідковувати ліцензування та розподіл прав;

- NFT (Non-Fungible Tokens) – для унікального представлення цифрових активів, забезпечуючи авторам та художникам контроль над їхніми творами;

- системи виявлення порушень авторських прав на основі спеціалізованого програмного забезпечення для сканування та виявлення несанкціонованого використання контенту в Інтернеті;

- авторські вказівки та метадані – включення ясних авторських вказівок та метаданих в цифровий контент для спрощення ідентифікації прав власності.

Ці методи можуть бути використані як окремо, так і в комбінації для забезпечення комплексного захисту інтелектуальної власності в онлайн-просторі. Але основна проблема – це відсутність загальноприйнятого стандартизованого підходу із легким доступом та легкістю втілення для пересічного автора.

Найбільш популярним способом захистити себе як автора від можливих порушень – є цифрові водяні знаки для зображень, аудіо та відеофайлів. Вони мають як переваги, так і недоліки.

Переваги цифрових водяних знаків:

- дозволяють власникам прав доволі ефективно відстежувати та управляти використанням їхнього контенту в Інтернеті;

- мають мінімальний вплив на оригінал, оскільки як правило, цифрові водяні знаки розміщуються таким чином, щоб мінімально впливати на якість оригінального зображення або звуку;

- стійкі до маніпуляцій – багато цифрових водяних знаків розроблені так, щоб витримувати спроби видалення або модифікації;

- можливість прихованого розміщення – водяні знаки можуть бути невидимими для неозброєного ока, не порушуючи естетику оригінального твору;

- судові докази – можуть служити як доказ у судових справах, пов'язаних з порушенням авторських прав.

Недоліки цифрових водяних знаків:

- потенційне зниження якості – в деяких випадках, особливо при неправильному застосуванні, цифрові водяні знаки можуть знижувати якість оригінального зображення або звуку;

- можливість видалення або зміни – хоч водяні знаки розроблені для стійкості, існують складні методи їх видалення або маскування;

- витрати на реалізацію – розробка та впровадження ефективної системи цифрових водяних знаків може бути витратною;

- правові обмеження у деяких юрисдикціях можуть накладати правові обмеження на використання цифрових водяних знаків, особливо якщо вони втручаються в конфіденційність або дані користувачів;

- технічні обмеження у цифрових водяних знаках можуть бути неефективними проти деяких форм стиснення файлів або зміни формату.

Використання цифрових водяних знаків вимагає зважения їх переваг та недоліків, а також врахування конкретного контексту та потреб власників авторських прав.

Шифрування також використовується для захисту інформації, але має свої особливості, складнощі та недоліки. До особливостей варто віднести те, що шифрування перетворює дані в код, який може бути розшифрований лише за допомогою спеціального ключа. Використовуються симетричні та асиметричні алгоритми шифрування. Складнощі полягають у великій кількості алгоритмів і потребі у виборі найбільш підходящого; необхідність забезпечити безпеку ключів шифрування; комплексність управління ключами великої організації. До недоліків шифрування відносемо ризик втрати доступу до даних у разі втрати ключа;

потенційна можливість дешифрування за допомогою квантових комп'ютерів; збільшення часу обробки даних через шифрування. Для ефективного захисту важливо правильно вибирати алгоритми шифрування, належно управляти ключами та враховувати потенційні ризики. Однак безпосередньо для інформації на веб-ресурсах цей спосіб не вдасться застосувати, оскільки тоді інформація не буде розміщена на веб-порталі у відкритому доступі і ризики для таких даних суттєво знижуються впринципі, а тема нашого дослідження розкриває особливості захисту об’єктів авторського права і суміжних прав на веб-ресурсах у вільному доступі.

Наступним інструментом захисту є технологія блокчейн – вона базується на концепції розподіленого реєстру, де дані зберігаються у вигляді ланцюжка блоків. Кожен блок містить пакет транзакцій та криптографічно зв'язаний з попереднім блоком, створюючи неперервний ланцюг. Це забезпечує незмінність та прозорість даних. Важливим елементом є консенсусні алгоритми (наприклад, Proof of Work або Proof of Stake), які гарантують безпеку та синхронізацію між вузлами мережі. Блокчейн знайшов застосування в криптовалютах, смарт-контрактах, ланцюгах поставок та інших сферах. Для розгортання блокчейн-інфраструктури потрібні значні ресурси та складні технічні рішення – Для розгортання блокчейн-інфраструктури потрібні значні ресурси та складні технічні рішення – мережеві вузли, продуктивні та масштабовані обчислювальні ресурси, надійні криптографічні протоколи та забезпечення безпеки мережі, потреба у створенні та підтримці розподіленої мережі, яка може ефективно синхронізувати дані. Всі ці фактори вимагають фахових знань та інвестицій, особливо для великих та складних блокчейн-проектів. Але блокчейн, на відміну від традиційних баз даних, пропонує унікальну комбінацію децентралізації, прозорості, незмінності даних та безпеки. Це досягається завдяки розподіленій структурі, де кожен блок даних криптографічно зв'язаний з попереднім, забезпечуючи цілісність ланцюжка. Прозорість і відкритість транзакцій, разом з неможливістю їх зміни після запису, робить блокчейн важливим інструментом у сферах, де важливі довіра та безпека даних, а для захисту інтелектуальної власності шляхом створення незмінної та прозорої системи запису прав і транзакцій – дозволяє авторам та власникам

інтелектуальної власності безпечно реєструвати, ліцензувати та передавати права на свої твори, забезпечуючи цілісність даних та знижуючи ризики несанкціонованого використання або підробки.

Також одним із варіантів захисту є NFT, або незамінний токен, це тип цифрового активу на блокчейні, який представляє унікальне володіння або права на певний об'єкт чи роботу. Кожен NFT є унікальним і не може бути замінений на інший токен однакової вартості, на відміну від звичайних криптовалют. Це дозволяє застосовувати NFT для цифрового представлення власності на мистецтво, музику, відео та інші форми творчості, а також для цифрового сертифікації автентичності та власності.

Хоч і не ідеальним, але доволі поширеним інструментом захисту є системи виявлення порушень авторських прав в інтернеті, такі як Content ID від Google чи системи виявлення плагіату, які використовують алгоритми для сканування та порівняння контенту з базами даних. Основні недоліки цих систем включають: ймовірність помилкових позитивних результатів, невірне ідентифікування легального використання як порушення, алгоритми можуть не виявляти деякі порушення через обхідні методики або недосконалості у виявленні, системи можуть помилково обмежувати легітимний контент, особливо у випадках використання цитат, пародії або критики. Ці системи важливі для захисту прав, але мають свої обмеження та потребують удосконалення.

Авторські вказівки та метадані теж служать як важливі технічні інструменти для захисту об'єктів авторського права в цифровому світі. Метадані, які включають інформацію про авторство, права власності, історію створення та розповсюдження цифрового контенту, дозволяють забезпечити відстежуваність та верифікацію походження цифрових активів. Використання метаданих у цифрових медіа-файлах, таких як фотографії, відео, аудіозаписи та документи, створює шар захисту авторських прав, дозволяючи авторам та власникам прав легко ідентифікувати свої твори та стежити за їх використанням. Це може включати інформацію про автора, назву твору, дату створення, а також специфічні умови ліцензування та використання.

Усі ці методи технічного захисту авторських прав мають спільну складність: вони вимагають балансу між ефективністю захисту, зручністю використання та впливом на оригінальний контент. Цифрові водяні знаки, шифрування даних, та метадані можуть бути обійдені технічно досвідченими користувачами, в той час як блокчейн і NFT залежать від складної та високотехнологічної інфраструктури. Системи виявлення порушень авторських прав часто стикаються з проблемами невірного ідентифікування контенту. Це підкреслює складність розробки універсальних та ефективних рішень у цій сфері.

Наше дослідження має на меті дослідити загальні тенденції та визначити пріоритетні напрямки для подальших наукових пошуків. У таблиці 2.2 ми надали порівняльний огляд методів захисту, враховуючи їх відповідність сучасним викликам і потребам у кіберпросторі, надійності та складності впровадження.

Таблиця 2.2 – Порівняльний огляд технічних засобів захисту

Методи захисту	**Складність реалізації**	**Надійність захисту**	**Актуальність для сьогоднішніх умов кіберпростору**
Цифрові водяні знаки	Середня	Середня	Висока
Шифрування даних	Висока	Висока	Висока
Технологія блокчейн	Висока	Висока	Висока
NFT (Non-Fungible Tokens)	Висока	Висока	Середня
Авторські вказівки та метадані	Низька	Низька	Середня
Системи виявлення порушень авторських прав	Середня	Середня	Висока

Тож, як і з правовою площиною захисту об’єктів авторського і суміжних прав на веб-ресурсах, простих та надійних рішень немає, а актуальність нашого дослідження стає все більш очевидною.

2.3 Трансформація методологій захисту авторських та суміжних прав на веб-ресурсах у контексті кіберпростору: аналіз та перспективи

Сучасний розвиток інформаційних технологій та їх проникнення в усі сфери життєдіяльності суттєво впливає на парадигми захисту авторських та суміжних прав. Розширення кіберпростору вимагає переосмислення традиційних підходів до інтелектуальної власності, адаптації юридичних норм та розробки нових технічних методів захисту. Особливо це стає актуальним для веб-ресурсів, де зростаюча цифрова інтеграція викликає потребу в більш гнучких, адаптивних та ефективних способах захисту.

З розвитком кіберпростору, охорона авторського права зазнала значних змін, що відображає взаємозв'язок між правовими та технічними аспектами інтелектуальної власності. Цей взаємозв'язок виявляється у тому, що із розвитком Інтернету та цифрових технологій, з'явилася потреба в нових методах захисту цифрового контенту. Це включає розробку технологій, таких як цифрові права на копіювання (DRM), хешування та цифрові водяні знаки. Однак, законодавство часто відстає від цих технологічних інновацій, створюючи прогалини в ефективності захисту авторських прав.

Інтернет спрощує нелегальне поширення захищеного контенту, що вимагає від законодавців і технологічних компаній співпраці в розробці нових методів боротьби з піратством. Використання блокчейн-технологій може стати одним із таких методів, дозволяючи простежувати походження та розповсюдження контенту.

Глобалізація Інтернету викликає потребу в міжнародному регулюванні авторських прав. Це вимагає не тільки законодавчих угод між країнами, але й технологічної інтеграції та сумісності.

Юриспруденція потребує постійної адаптації, щоб відповідати новим технологічним реаліям. Це означає внесення змін до існуючих законів та розробку нових норм, які відображають зміни в технологічному ландшафті.

В цілому, зв'язок між правовими та технічними явищами у сфері інтелектуальної власності є динамічним і взаємопов'язаним. Юриспруденція та технології повинні розвиватися разом, щоб ефективно відповідати на виклики, які ставить сучасний цифровий світ.

В оцінці ефективності охорони авторських прав у сучасному цифровому світі існує взаємодія між правовими нормами та технологічними інноваціями. Обидва аспекти відіграють важливу роль, хоча правові норми створюють необхідний фундамент для захисту авторських прав, все ж технологічні рішення часто виявляються більш оперативними та гнучкими у відповіді на сучасні виклики. Таким чином, у сучасному контексті технології можуть вважатись більш ефективними для безпосереднього захисту авторських прав, в той час як правові рамки забезпечують необхідну юридичну підтримку та санкції.

У майбутньому охорона авторських прав зіштовхнеться з необхідністю поєднання технологій в постійному розвитку з адаптивним та гнучким законодавством. З одного боку, законодавчі органи повинні оновлювати правові рамки, щоб вони відповідали швидким змінам у технологіях, в той час як потрібно забезпечувати міжнародну гармонізацію та знаходити баланс між захистом прав авторів і правами користувачів. З іншого боку, технології, такі як DRM, блокчейн, та штучний інтелект, мають потенціал для більш ефективного контролю за розповсюдженням цифрового контенту, але водночас стикаються з викликами, пов'язаними з надмірними обмеженнями, етикою та приватністю. Це вимагає ретельної координації між правовими та технологічними сферами, де ключовими будуть гнучкість, адаптивність та врахування інтересів різних зацікавлених сторін.

У контексті охорони авторських прав на веб-ресурсах, існують суперечливі тенденції. З одного боку, зростаюча доступність та обсяг цифрового контенту у веб-просторі можуть сприяти збільшенню порушень авторських прав, оскільки контент стає легше копіювати та розповсюджувати. З іншого боку, розвиток технологій, таких як цифрові водяні знаки, хешування, блокчейн, а також підвищення обізнаності про авторські права та посилення законодавства, сприяють зміцненню захисту авторських прав та зменшенню порушень. Це створює складну динаміку,

де зростання випадків порушень авторських прав зустрічається з більш ефективними методами їх запобігання та виявлення.

Тож у розвитку алгоритмів захисту авторського права на веб-ресурсах, спостерігається певний вектор, який характеризується інтеграцією технологічних інновацій та посиленням правових рамок. Основні тенденції можна виокремити як:

Технологічний прогрес із використання передових технологій, таких як блокчейн, штучний інтелект, цифрові водяні знаки, та хешування, стає все більш поширеним. Ці технології дозволяють автоматизувати процеси виявлення та запобігання порушенням авторських прав, забезпечуючи ефективніший контроль над розповсюдженням цифрового контенту.

Адаптивне законодавство над яким активно працюють законодавчі органи задля оновлення та адаптації правових норм, щоб відповідати змінам у технологічному ландшафті. Це включає розробку нових законів та міжнародних угод, які враховують особливості цифрової ери.

Баланс між захищеністю та доступністю є важливою тенденцією для авторських прав та забезпеченням доступності та свободи інформації для користувачів. Це включає врахування прав споживачів та впровадження гнучких моделей ліцензування.

Міжнародна координація з урахуванням глобального характеру Інтернету, співпраця між країнами для стандартизації захисту авторських прав – набувають особливої важливості.

Враховуючи ці тенденції, можна зробити висновок, що вектор розвитку алгоритмів захисту авторського права на веб-ресурсах спрямований на інтеграцію інноваційних технологій з удосконаленим та адаптивним законодавством. Це включає застосування передових технічних рішень для ефективного виявлення та запобігання порушень, а також створення гнучких правових рамок, які враховують швидкі зміни в цифровому світі та потреби всіх зацікавлених сторін.

3 ІННОВАЦІЙНІ АЛГОРИТМИ ДЛЯ ЗАХИСТУ АВТОРСЬКОГО І СУМІЖНИХ ПРАВ НА ВЕБ-РЕСУРСАХ

3.1 Виявлення копій на основі хешування на прикладі аудіозаписів

Завдяки розвитку Інтернет-технологій кожен може користуватися мультимедійним вмістом, таким як текст, відео, зображення чи аудіо на веб-сайтах для обміну даними. До того ж, популярність мультимедійного вмісту зросла останні кілька років [16]. Усе це сильно взаємопов’язано із зусиллями авторів, які постійно створюють і завантажують новий вміст у Інтернет, щоб розважити глядачів. Тим не менше, попри усі вдосконалення Інтернету, ці творці контенту стикаються з проблемами монетизації своїх робіт. Порушення авторських прав є одним з найпідступніших викликів у цій галузі, особливо в музичній індустрії, яка страждає значні економічні втрати внаслідок піратства [20]. Дублювання або внесення незначних змін до вмісту та отримання прибутку за роботу, тоді як автор не отримує очікуваного прибутку, є одним із найпоширеніших випадків порушень авторського права.

Технологія блокчейн застосовується в різних галузях, окрім фінансів, таких як інформація та безпека, управління ланцюгом поставок та охорона здоров’я [11], [14], [19]. Блокчейн створює спільну розподілену книгу на основі консенсусу між усіма учасниками мережі. Використання стороннього верифікатора більше не потрібне, що забезпечує безпеку і повністю децентралізованість системи. Таким чином, система є децентралізована, безпечна і має спільний захищений від несанкціонованого доступу реєстр, який не може бути модифікований [24]. Технологія блокчейн може вирішити реалізацію ефективного, конфіденційного обміну даними завдяки своїй стійкій і децентралізованій інфраструктурі [12]. На думку Лі Ет Аль [31], технологєю блокчейн можна покращити захист авторських прав і підтримати творців контенту, що вигідно для майбутнього розвитку музичної індустрії.

Хоча управління авторським правом просунулося, поточний децентралізований захист авторських прав не є бездоганним. Як пише Груєр [3],

Audios, одна з найвидатніших децентралізованих музичних платформи, дозволяє користувачам завантажувати файли у їхню систему. Audios стверджує, що на їхній платформі немає вмісту який можна цензурувати або стерти. Можливість користувачам завантажувати будь-що може створити значні проблеми для агентств і музикантів якщо не існує системи претензій щодо авторських прав. Крім того, Діаль [6] заявив, що на веб-сайті немає механізму для подання позов про порушення. Через відсутність технології виявлення звуку на їхній платформі, стаття [1] стверджує, що Audios має високий рівень піратства з великою кількістю незаконного вмісту на сайті. Отже, сканування вмісту перед його виходом в Інтернет має важливе значення для запобігання поширенню вмісту, що порушує авторські права децентралізовані платформи для обміну музикою.

Перцептивна хеш-функція є методом ідентифікації вмісту мультимедійних даних. На відміну від звичайної хеш функції, яка дуже чутлива до змін, перцептивна хеш-функція розроблена так, щоб не змінюватися суттєво коли мультимедійні дані зазнають незначних змін, тому що незначні зміни або маніпуляції у вхідних даних спричиняють незначні зміни на виході. Іншими словами, перцептивну хеш-функцію можна розглядати як унікальний ідентифікатор для кожного аудіо. Перцептивні хеші також довели свою ефективність у виявлення модифікованого мультимедійного вмісту [21], з одним із найпопулярніші програми впровадження перцептивного хешування є Shazam.

Ми розглянемо декілька підходів до виявлення маніпуляцій зі звуком. Наприклад, Лінь і Канг [28] представив структуру виявлення фальсифікації аудіо, яка використовує навчання під наглядом. Даз та ін. [23] пропонують модель, яка використовує акустичні характеристики, їхній підхід використовує глибоку нейронну мережу для відокремлення справжнього від підробленого мовні дані. Лю та ін. [4] реалізовано на основі трансформатора CNN для виявлення підробки аудіо з кращим результатом ніж попереднє дослідження. У роботі Ванг ет Аль [33] представлена структура, яка використовує глибоке навчання для виявлення підробленого аудіо.

Характеристика перцептивного хешу полягає в тому, що створений хеш не змінюється суттєво, якщо відбувається зміна даних. Перцептивний хеш зазвичай використовуються для ідентифікації вихідних даних і широко застосовується для автентифікації вмісту, виявлення підробок, та виявлення подібності [29].

Отже, щоб довести, що алгоритм є стійким до модифікацій, надійність алгоритму повинна бути перевірена, щоб визначити, чи має змінений аудіо-файл подібності до оригінального аудіо. Тест повинен включати повний список потенційних атак [32] тому ми розглянемо різні поширені модифікації аудіосигналу де-синхронізовані атаки для зміни звукового сигналу. Загальні модифікації аудіосигналу включають LPF, додавання шумів і стиснення MP3 і AAC; приклади атак десинхронізації включають модифікацію масштабу, часу і зміщення висоти тону. На рисунках 3.1 і 3.2 проілюстровано, як модифікації впливають на звук у часовій та спектральній області.

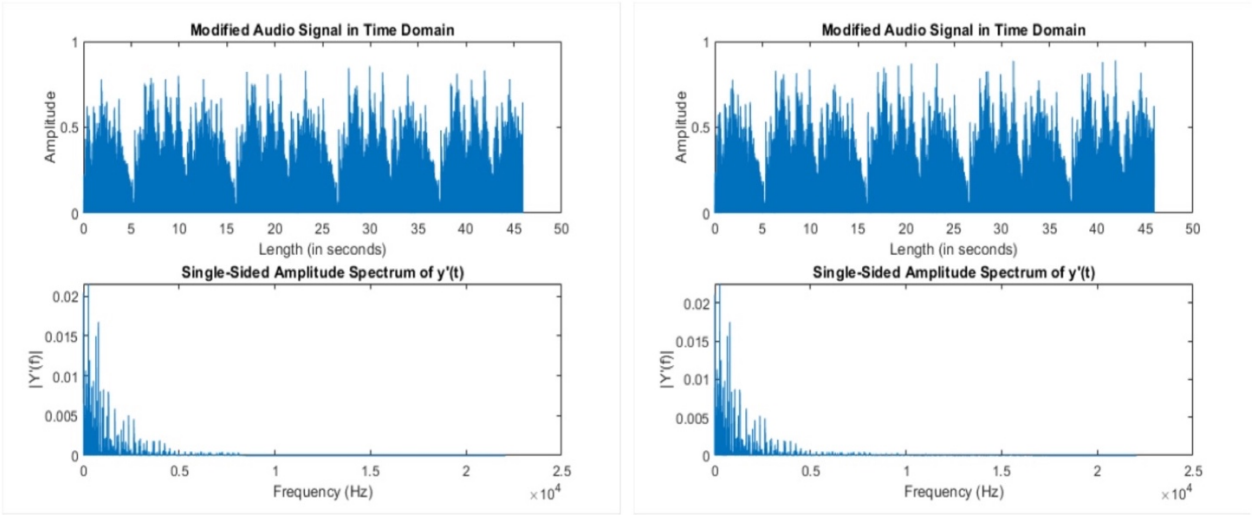
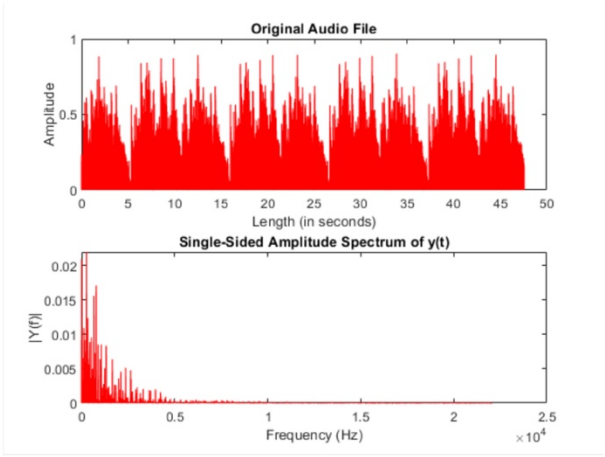
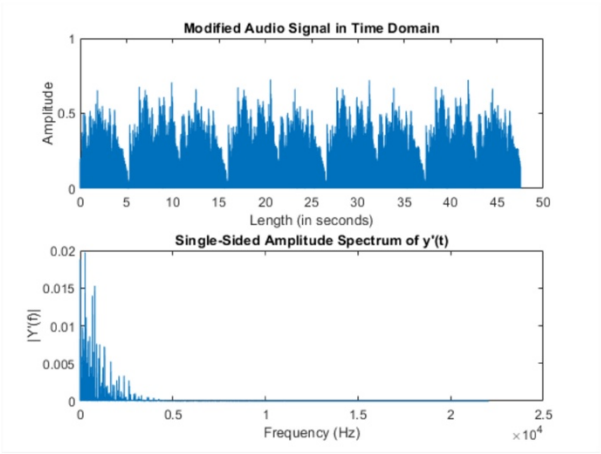


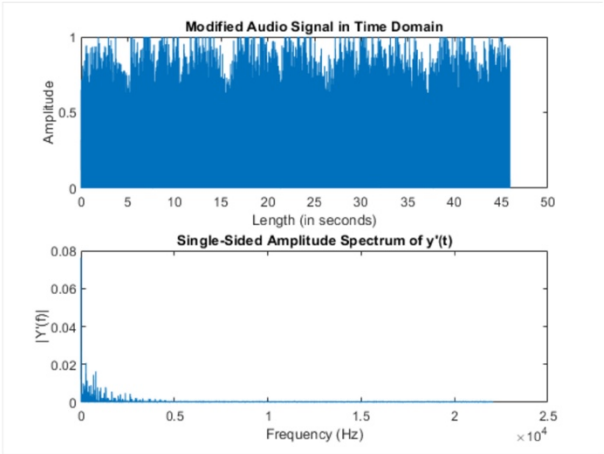
Рисунок 3.1 – Модифікація аудіофайлу в контексті впливу на хеш



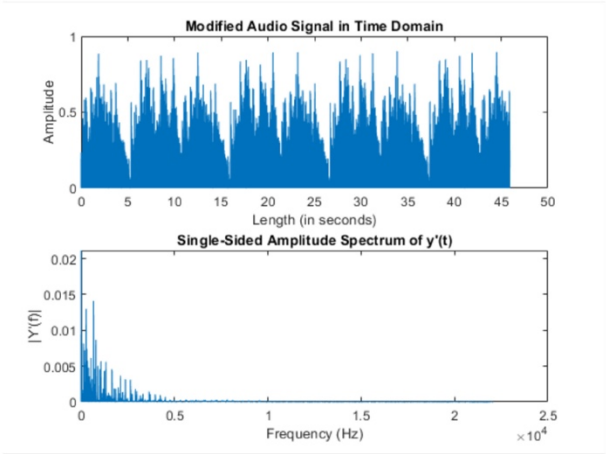
Original Audio



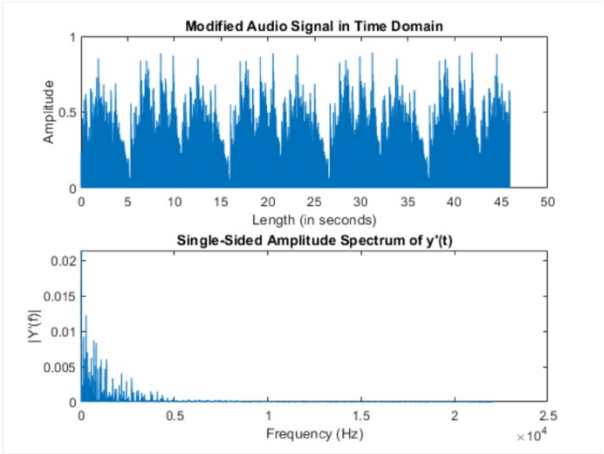
Modified with LPF 3KHz



Modified with Adding Noise 0dB



Modified with Time Scale Modification 0.96 times



Modified with Pitch Shifting 0.96 times

Рисунок 3.2 – Вплив на перцепційне хешування змін у аудіо

У наведених далі поясненнях містяться відомості про кожну атаку на аудіофайли, виконану в щодо зразків:

- LPF: фільтр, який пропускає аудіосигнали з частотою нижче вибраної частоти зрізу та затухання – споживає сигнали з частотою, вищою за граничну частоту;

- додавання шуму: шум додається до аудіофайлу, поки не буде досягається бажаний SNR;

- модифікація шкали часу: темп і тривалість звуку змінюється, зберігаючи висоту;

- зміна висоти: висота звуку зменшується, зберігаючи темп і тривалість;

- стиснення MP3: MP3-кодер використовується для зниження бітрейт аудіо;

- стиснення AAC: для зниження використовується кодер AAC бітрейт аудіо.

Далі буде описано деталі перцептивного хеш-методу та виявлення порушення авторських прав запропонованою системою включно із використанням блокчейн технологій для реєстрації прав. Головна схема, яка використовується в цій системі, проілюстрована на рисунку 3.3.

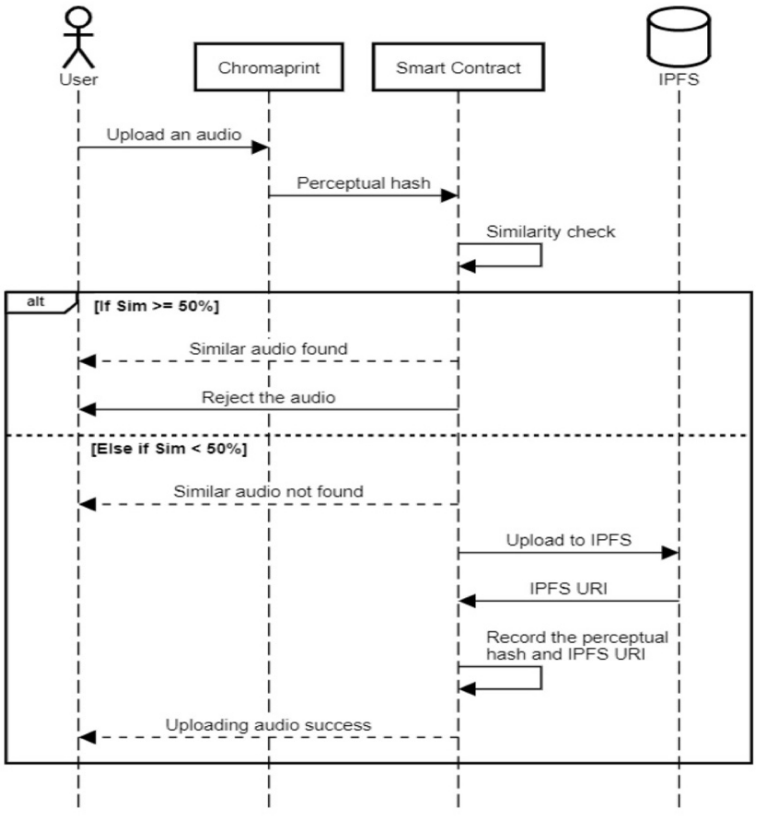


Рисунок 3.3 – Головна схема реалізації блокчейн технології

Це дослідження базується на перцептивному хеш-підході Chromaprint, інструменті з відкритим кодом для зняття відбитків аудіо. Лукас Лалінський розробив Chromaprint як бібліотеку на стороні клієнта який витягує зліпок з будь-якого аудіоджерела. Наступне це покрокове пояснення того, як генерує Chromaprint перцептивні хеші з аудіо [15], [7]:

1) вхідний аудіосигнал перетворюється на моно і зменшується до 11025 Гц

2) звуковий сигнал перетворюється на частоту домену за допомогою STFT із розміром кадру 4096 вибірок і перекриття на дві третини

3) потім спектр ділиться на 12 бінів. Кожен контейнер представляє інше значення кольоровості

4) ще 16 фільтрів генеруються за допомогою AdaBoost метод, описаний в [7] з різними розмірами від шість фільтрів

5)12 x 16 сканує по значенню кольоровості на кожному зразку, створюючи допоміжне зображення

Алгоритм 1 – генерація перцептивного хешу аудіо за допомогою Chromaprint:

Result: Hash Value of An Audio
initialization;
import chromaprint;
import pyacoustid;
audioPHash ← 0;
audioPHash ← getFingerprint(audiofile);
Return audioPHash;

(продовжуємо до Алгоритму 2)

6) для кожного кадру вікно фільтрується за допомогою 16 згенерованих фільтрів

7) фільтр додає значення енергії в білій області та віднімає її від чорної області, отримуючи єдине значення. Крім того, значення енергії кодується у вигляді двобітного числа (від 0 до 3) за допомогою коду Грея

8) повторіть кроки 7 і 8 для кожного підзображення, і буде отримано аудіовідбиток.

Щоб виявити аудіо, подібне до існуючого в системі, перцептивне хеш-значення аудіо має бути спочатку згенеровано за допомогою методу Chromaprint . Псевдокод генерації перцептивного хешу з аудіо проілюстровано в Алгоритмі 1.

Алгоритм 1 показує, як перцептивний хеш можна отримати з аудіо. Спочатку виберіть потрібний аудіофайл, який потрібно додати до системи. Функція *getFingerprint* від Chromaprint генерує перцептивний хеш вибраного аудіо, який зберігає значення в *змінній audioPHash* . Після отримання хеш-значення значення *audioPHash* порівнюється з існуючим перцептивним хеш-значенням з мережі блокчейн за допомогою правила відстані Хеммінга в Алгоритмі 2.

Метою Алгоритму 2 є обчислення подібності між перцепційним хешем аудіофайлу-кандидата та перцептивними хешами, що зберігаються в мережі блокчейн.

Алгоритм 2 - Виявлення звуку:

```
Result: Audio Acceptance or Rejection
initialization;
h1 ← audioPHash;
audioPHashList ← hades.phashList;
percentage ← [];
similar ← FALSE;
i ← 1;
//Hamming Distance //
while i ≤ length(audioList) do
    h2 ← audioPHashList[i];
    minLen ← min(length(h1),length(h2));
    similar ← FALSE;
    distance ← 0;
    k ← 1;
    while k ≤ minLen do
        if h1[k] ≠ h2[k] then
            distance ← distance + 1;
        else
            continue;
        end
        k ← k + 1
    end
    i ← i + 1;
    percentage[i] ← (distance×100)÷minLen;
end
j ← 1;
while j ≤ length(percentage) do
    if percentage[j] ≥ 50% then
        similar ← TRUE;
        reject the audio;
    else
        continue;
    end
    j ← j + 1;
end
```

Моделювання в цьому розділі проводилося на Macbook Air на основі чіпа M2 з 10-ядерним графічним процесором, 8 ГБ оперативної пам'яті та 512 ГБ пам'яті. Аудіофайл, протестований для запропонованого підходу, мав роздільну здатність 16 біт, тривалість 47 с і частоту дискретизації 44 100 Гц. Аудіоманіпуляції виконувалися за допомогою MATLAB 2021a.

У цьому розділі представлено надійну систему виявлення звуку для захисту авторських прав. У запропонованій системі перцепційний хеш використовується для виявлення порушень авторських прав в аудіофайлах. Технікою перцептивного хешування, використаною в цьому дослідженні, був Chromaprint, бібліотека аудіовідбитків із відкритим кодом. Результати показали, що запропонована система є високостійкою до атак обробки сигналів, таких як EPF, додавання шуму, модифікація масштабування часу, зсуву висоти, стиснення MP3 та стиснення AAC.

Середня схожість між оригінальним аудіо та його модифікованими версіями становила не менше 90% для будь-якого сценарію, що означає, що запропонована система може ефективно виявляти порушення авторських прав. Крім того, середній час виявлення звуку запропонованої системи становив лише 616,3 мс.

3.2 Цифровий водяний знак для об'єктів захисту

Однією з великих переваг цифрових медіа порівняно з аналоговими є те, що цифрові дані можна легко та нескінченно відтворювати без втрати якості. Ця перевага, однак, може також стає головним болем для власників авторських прав, які хочуть захистити свої твори від несанкціонованого відтворення. За словами високопрофільних організацій з захисту авторських прав, таких як SDMI та DVD-CCA, відсутність захисту від порушення авторських прав часто наводиться як причина повільного розповсюдження цифрових медіа [25].

Добре відомо, що шифрування може захищати цифрові дані від доступу несанкціонованими сторонами. Шифрування змішує дані згідно з секретним ключем таким чином, що доступ до даних може бути відновлений лише стороною, яка знає ключ. Однак це не запобігає нелегальному копіюванню або повторному

транслюванню законними користувачами, адже вони отримують секретний ключ, щоб мати змогу отримати доступ до сервісу.

Стеганографія — це наука про приховування інформації в основному документі таким чином, щоб приховану інформацію можна було відновити лише призначеним користувачем, а основний документ залишається придатним для його звичайного використання. *Цифровий водяний знак* широко використовується для застосування стеганографічних методів до цифрових об'єктів.

У цьому розділі ми зосередимося на цифрових водяних знаках для захисту авторських прав. Ми ознайомимося з відповідними технічними аспектами цифрових водяних знаків, а потім опишемо запропоновані механізми захисту авторських прав на основі водяних знаків. Ми опишемо потреби систем водяних знаків, спрямованих на запобігання порушенням авторських прав, і розкриємо обмеження технологій водяних знаків.

Цифровий водяний знак — це просто сигнал, який потрібно вбудувати в цифровий об’єкт, який ми називатимемо хостом. Потужність сигналу водяного знака набагато нижча, ніж потужність сигналу хоста, тому головний об’єкт зберігає свою корисну цінність після вбудовування водяного знака. Водяні знаки можуть бути *помітними* або *непомітними* для людини-споживача. Більшість алгоритмів створення водяних знаків створюють непомітні водяні знаки, які може виявити лише машина. Непомітні водяні знаки менш шкодять головному об’єкту та є більш захищеними від зловмисників, які бажають знищити або маніпулювати водяним знаком. Підходи водяних знаків, описані в цьому розділі, зазвичай використовують непомітні водяні знаки. Хоч і простіші помітні (візуальні) водяні знаки знайшли застосування на телебаченні, все ж Ватиканська бібліотека використовує більш складну для візуального сприйняття систему [18].

Дуже простий непомітний водяний знак, наприклад, можна вбудувати за допомогою *вбудовування LSB,* у якому ми замінюємо найменш значущий (тобто крайній правий) біт кожного зразка на біт з якогось шаблону водяного знака. На рисунку 3.1 показано растрове зображення 4x4 з виділеним крайнім бітом (8-бітної шкали сірого).

11111111 11111110 11111101 11111100

11111110 11111101 11111100 11111011

11111101 11111100 11111011 11111010

11111100 11111011 11111010 11111001

Рисунок 3.1 - Растрове зображення 4x4 з виділеним крайнім бітом

Ми можемо розглядати наш водяний знак як бінарний растровий візерунок, тобто зображення лише з двома кольорами , які ми називатимемо `0' та `1' (які можуть бути зіставлені з білим і чорним для відображення). Візерунок водяного знака матиме ті самі розміри, що й головне зображення, і буде вбудовано в головне зображення шляхом заміни крайнього біта кожного пікселя на відповідний біт у зображенні водяного знака. На рисунку 3.2 показано растрове зображення 4x4 із зображенням літери `N', яку ми вставили в зображення на рисунку 3.1, щоб сформувати зображення з водяним знаком, показане на малюнку 3.3.

1 0 0 1

1 1 0 1

1 0 1 1

1 0 0 1

Рисунок 3.2 - Растрове зображення 4x4 із зображенням літери `N'

11111111 11111110 11111100 11111101

11111111 11111101 11111100 11111011

11111101 11111100 11111011 11111011

11111101 11111010 11111010 11111001

Рисунок 3.3 – Сформоване зображення із вбудованим водяним знаком

Зміна крайнього біта пікселя зазвичай непомітна для глядача, але комп’ютеру легко виявити водяний знак, зчитуючи значення молодших бітів. На рисунку 3.4 показано головне зображення (а) та версія, на яку нанесено водяний знак за допомогою растрового зображення (б), показаного на рисунку 3.5.

а) б)

Рисунок 3.4 – Головне зображення (а) та версія, на яку нанесено водяний знак за допомогою растрового зображення (б)

Рисунок 3.5 – Водяний знак

У контексті захисту авторських прав припускаємо, що у нас є детектор водяних знаків (комп'ютерна програма або спеціально створений пристрій), який, отримавши зразок водяного знака та об'єкт, може перевірити наявність цього зразка в об'єкті. Зверніть увагу, що водяний знак може існувати в носії чисто випадково – легко побачити, що піксельні дані рисунку 3.1 містять "водяний знак", що складається з чергуючихся одиниць і нулів.

По цій причині тест є статистичним тестом. Детектор повертає оцінку виявлення, яка представляє впевненість детектора в тому, що зразок не виник випадково. Якщо оцінка вища за певний поріг, ми припускаємо, що водяний знак присутній, інакше припускаємо, що його немає.

Однак через статистичний характер тесту залишається можливість, що детектор зробить помилку. Детектор може виявити водяний знак, який не був вставлений (хибно позитивний результат), або не виявити водяний знак, який був вставлений (хибно негативний). Добре спроектовані алгоритми водяних знаків повинні мінімізувати кількість хибно позитивних та хибно негативних результатів, але існує компроміс між ними, і неможливо повністю усунути жоден у цій нетривіальній системі.

Водяний знак вважається стійким, якщо його присутність все ще можна виявити після того, як носій-хост був якимось чином оброблений, не завдаючи йому шкоди в прийнятних межах. Об'єкт може бути оброблений в ході невинних процесів обробки сигналу, таких як стиснення, або він може бути оброблений зловмисно атакуючим, який хоче видалити водяний знак. Для надійного захисту авторських прав нам потрібні водяні знаки, які є стійкими до будь-якої обробки, що призводить до створення об'єкту, який зберігає свою комерційну цінність.

Схема вбудовування LSB (Least significant bit) не є стійкою. Легко вбудувати інший візерунок у найменш значимі біти, стираючи оригінальний водяний знак без подальшого пошкодження зображення. Було запропоновано багато більш складних алгоритмів, які використовують складності людських сприймальних систем для створення водяних знаків, які не можна так легко знищити. Огляди технік

цифрового водяного знаку наведено у різних наукових працях Свансона, Кобяші, Тефіка [26], Хартунга і Кутера [9] та інших.

На жаль, для потенційних користувачів водяних знаків, захист їхньої інтелектуальної власності не такий простий, як може здатися з описаних вище базових моделей. Творець контенту не може просто вибрати схему водяних знаків (стійку) на свій вибір, вбудувати довільний водяний знак і розповсюджувати об'єкт із водяним знаком, будучи впевненим, що порушників авторських прав притягнуть до відповідальності.

Крейвер із колегами науковцями [5] описали загальну процедуру, яка подолала багато, якщо не всі, відомі на той час алгоритми водяного знаку, атакою відомою як атака інверсії. Використовуючи цю процедуру, шахрай може створити підроблений оригінальний об'єкт і водяний знак таким чином, що водяний знак шахрая здається присутнім у справжньому оригіналі.

Таким чином, будь-який алгоритм водяного знаку, який піддається атаці інверсії, не може бути використаний для доведення власності, оскільки інвертований алгоритм може бути використаний для "доведення" того, що будь-хто є власником об'єкта.

Крім того, оскільки тест на наявність водяного знака є статистичним, шахраю може бути вигідно неодноразово генерувати водяні знаки, доки він або вона не натрапить на зразок водяного знаку з достатньо високим відсотком виявлення для претендування на власність. Тому користувачам водяних знаків не варто легковажно обирати довільні зразки водяних знаків – або зразок повинен бути зареєстрований у довіреному органі, або зразки повинні бути обмежені тими, які мають якийсь сенс для людини-спостерігача.

Базова модель водяних знаків не вирішує проблему виявлення порушення авторських прав на початковому етапі – вона займається лише виробленням доказів проти когось, хто підозрюється у порушенні.

Однак, водяні знаки, що позначають власність, можуть бути використані в розширеному вигляді механізмами, які активно шукають порушення авторських прав. Веб-павук – це частина програмного забезпечення, яка шукає в Інтернеті,

вивчаючи сторінки у кіберпросторі та переходячи за посиланнями на них, щоб знайти більше сторінок і більше посилань для подальшого відстеження. Таке програмне забезпечення може шукати в Інтернеті дані з водяними знаками та повідомляти підозрілі сторінки автору або якомусь відповідальному органу.

Подібні методи моніторингу, в принципі, можуть бути використані для контролю за іншими медіа. Але спроба моніторити весь Інтернет, а також будь-який інший носій, який може містити підозрілі дані, здається геркулесовим завданням, і не зрозуміло чи такий процес є реалістичним. Тим не менше, навіть якщо таким способом вдасться знайти лише невелику частину порушників авторських прав, це може забезпечити хоча б якусь стримуючу дію на потенційних піратів.

Однією із невирішуваних проблем для водяного знаку є імітація. Водяні знаки забезпечують механізм для демонстрації існування копії, зробленої неінтелектуальним механічним процесом, таким як ксерокопіювання, або дублювання комп'ютером. Ми називатимемо такі неінтелектуальні відтворення прямими копіями.

Припускаємо, що водяні знаки не змінюють семантичної цінності даних. Отже, водяні знаки не можуть і не повинні забезпечувати захист від більш інтелектуальних процесів копіювання, які вилучають семантичне значення твору та відтворюють його незалежно. Наприклад, для музикантів просто скопіювати музичний твір, граючи його на своїх інструментах. Жоден водяний знак, як ми його розуміємо, не міг би продовжити своє існування в такому процесі, який ми називатимемо імітацією.

Хоча імітація, безумовно, вимагає більше зусиль і зазвичай більшої майстерності, ніж пряме копіювання, не здається нерозумним вірити, що потенційні порушники авторських прав можуть мати легкий доступ до необхідних зусиль і навичок. Хтось, хто стверджує, що написав і виконав пісню, ймовірно, є музикантом, для якого не складно зіграти задіяну музику. Компанії, які можуть порушувати права на проекти будівель, машин тощо, мають легкий доступ до конструкторів у своєму штаті, для яких не складно намалювати схему.

З іншого боку, однак, не всі "імітації" є порушенням, навіть якщо пряме копіювання може ним бути. Наприклад, якщо Олена зробить фотографію Тернопільського Драматичного театру ім.Т.Г.Шевченка з вершини ЦУМу, це не є порушенням для Віктора піднятися на вершину ЦУМу мосту та зробити власну фотографію, в той час як незаконним залишається для Віктора робити несанкціоновані прямі копії фотографії Олени. Водяні знаки можуть розрізнити ці два випадки.

Якщо водяний знак має відповідати вимогам непомітності, необхідно припустити, що носій містить певний вид "порожнього простору", де може знаходитися прихований сигнал, тобто, надлишкові або незначні частини об'єкта. Аудіовізуальні дані, на яких зосереджена більшість досліджень водяних знаків, містять багато інформації, яка є непомітною для людського слухача або глядача, тому водяний знак можна приховати, маніпулюючи цими непомітними даними, не суттєво впливаючи на основні дані.

Однак це не стосується всіх даних. Текст, наприклад, містить мало або жодної непомітної інформації; навіть дуже дрібні зміни в тексті легко помітні людському читачеві.

Тим не менш, деякі рішучі дослідники розробили алгоритми водяних знаків для тексту, які вбудовують водяні знаки в текст, роблячи дрібні зміни в розміщенні рядків та слів [2]. Ці водяні знаки легко видалити, повторно вбудувавши водяний знак у текст, тому вони, здається, мають мало або жодного практичного застосування для захисту авторських прав. Інші запропоновані водяні знаки передбачають перестановку фраз у документі.

Подібні проблеми виникають і для простих дизайнів, таких як логотипи компаній, прапори та іконки, які не містять достатньої інформації носія, в якій можна було б сховати водяний знак.

Багато спостережень вище натякають на те, що для ефективного захисту авторських прав водяні знаки повинні бути регульовані. На відміну від методів запобігання, таких як шифрування та запобігання копіюванню, водяні знаки

повинні задовольнити незалежного арбітра (який може не бути технічно підкованою особою), що вони, дійсно, доводять щось.

Водяний знак повинен бути відомим (або вважатися логічним) надійним проти атак інверсії, а зразки водяних знаків повинні відповідати певним прийнятним стандартам.

У світлі вищенаведених фактів, стає зрозуміло, що водяні знаки – це складний інструмент, який вимагає чіткої регуляції та стандартизації для ефективного використання у сфері захисту авторських прав. Оскільки різні типи даних (такі як аудіовізуальні матеріали, текст або логотипи) мають різні можливості для вбудовування водяних знаків, важливо розробити гнучкі, але надійні методики, які б враховували специфіку кожного виду контенту.

Крім технічних аспектів, важливо також враховувати юридичні та етичні виміри, забезпечуючи, що водяні знаки не порушують права користувачів та не втручаються в законне використання контенту. У цьому контексті регуляція та стандартизація водяних знаків має включати як технічні рішення, так і чіткі правові рамки для їх використання, а також механізми для вирішення конфліктів і суперечностей, які можуть виникнути у сфері цифрових авторських прав.

3.3 Блокчейн як основа системи управління та захисту авторських прав

З розвитком інтернет-індустрії, створення та реалізація різноманітних цифрових авторських творів переходять від традиційної паперової форми до електронної. Враховуючи сучасне середовище та з огляду на викладені нами у дослідженні факти, захист цифрових прав та їх торгівля не досягли синхронного розвитку. Існує багато проблем та прогалин, які призводять до частих порушень цифрових авторських прав. На даний момент не існує ефективного способу захисту прав та інтересів творців, що серйозно підриває ініціативу творців до створення. Блокчейн, як найвпливовіша технологія в найближчі десятиліття, може вирішити всі види проблем, які існують у захисті та торгівлі цифровим авторським правом [8]. Технологія блокчейн також чітко включена в планування будівництва

інформатизації. Вона відіграватиме провідну роль у базових дослідженнях та розробці нових технологій та буде у пріоритеті майбутнього.

Система блокчейн головним чином складається з даних, мережі, консенсусу, інцентивів, контрактів та аплікаційних шарів. Шар даних капсулює базові дані блоків та фазові алгоритми. Мережевий шар включає механізм розподіленої мережі, механізм передачі даних та механізм перевірки даних. Шар консенсусу капсулює різні алгоритми консенсусу мережевих вузлів [34]. Шар інцентивів головним чином включає механізм розподілу та механізм розподілу. Шар контрактів капсулює різні сценарії, алгоритми та інтелектуальні контракти, які є основою блокчейна. Аплікаційний шар капсулює різні сценарії застосування та випадки використання блокчейна. Серед них, структура блокчейна на основі часових відміток, механізм консенсусу та програмований інтелектуальний контракт є представницькими технологіями блокчейна. Її конкретна структура показана на рисунку 3.6 нижче.

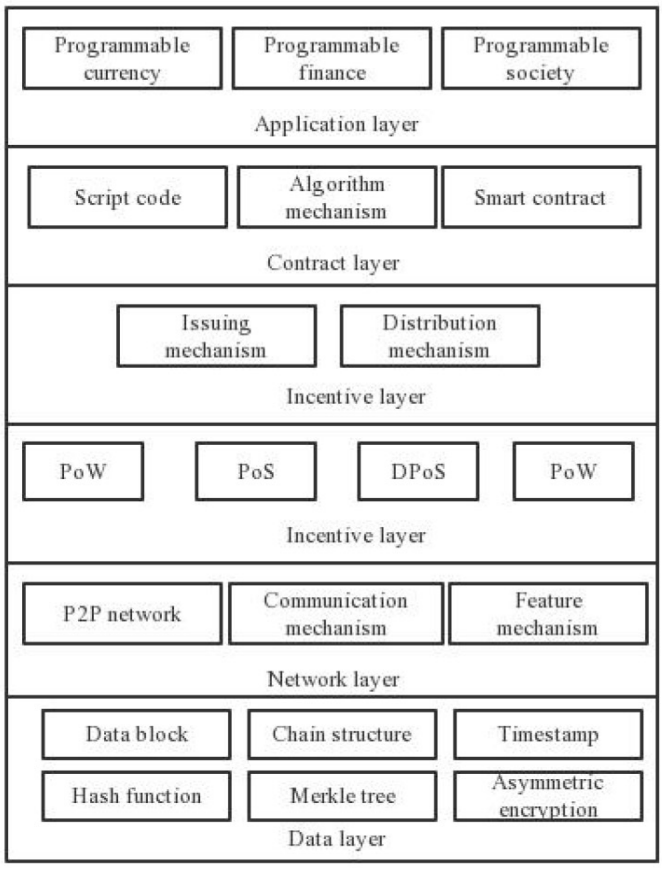


Рисунок 3.6 – Структура блокчейн технології

Управління та захист інформації про цифрове авторське право здійснюється головним чином через Ethereum блокчейн. Це може ефективно вирішити існуючі болючі точки в реєстрації авторських прав, зберіганні, перевірці, авторизації, передачі та запитах, а також реалізувати протидію підробкам у реєстрації цифрових авторських прав. Зокрема, при проведенні транзакцій, деякі авторитетні організації управління діють як частина вузла управління в системі, а коли автори завантажують цифрові авторські твори, вузол управління їх перевіряє. Транзакція здійснюється лише за згодою певної кількості вузлів, і до бази даних додається новий запис про транзакцію цифрових прав. Це децентралізоване управління є безпечнішим та ефективнішим, ніж традиційні системи цифрових прав. У порівнянні з традиційним механізмом аутентифікації авторських прав третьої сторони, система торгівлі цифровими авторськими правами на основі технології блокчейн має коротший час перегляду, відсутність реєстраційного збору, кращу безпеку архітектури та розширюваність, масштабованість. Технологія блокчейн має великий потенціал стати потужною силою для еволюції та розвитку управління інформацією про авторські права.

Мережеве середовище на блокчейні забезпечує зручність торгівлі та створює безпечне та ефективне середовище для транзакцій цифровими авторськими правами. Така транзакція конкретна в своїх правах та обов'язках, а кредитний механізм алгоритму є більш безпечним і надійним. Потік функцій системи показаний на рисунку 3.7.

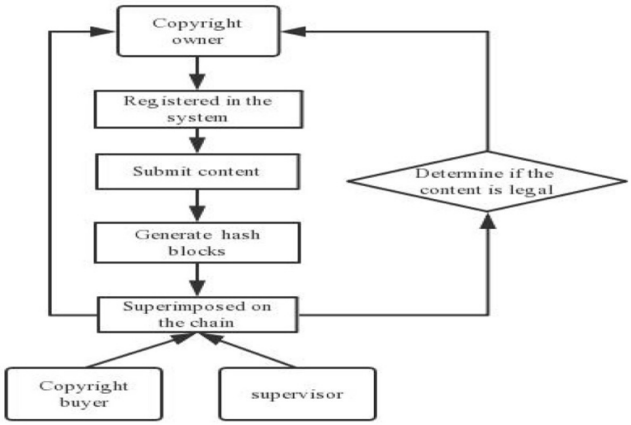


Рисунок 3.7 - Потік функцій блокчейн системи

У порівнянні з реєстрацією традиційних авторських творів, система цифрових авторських прав, заснована на технології блокчейн, яка описана у цьому розділі, є простішою та зручнішою у використанні. Власник авторських прав може заповнити форму і пройти перевірку. Процес завершується за три секунди після аудиту, що значно скорочує часові витрати та спрощує процес реєстрації. Оскільки відсутня необхідність в аудиті з боку третьої сторони, немає потреби платити відповідні комісійні збори протягом усього процесу реєстрації. Це економить користувачам значну суму зборів за реєстрацію цифрових авторських прав та сприяє підвищенню свідомості власників авторських прав щодо їх реєстрації [13].

Учасникам угоди необхідно спільно розробити контракт та завершити підписання своїх власних приватних ключів, щоб забезпечити дійсність контракту та уникнути втручання шкідливих дій у виконання контракту. У процесі усієї транзакції не потрібне втручання третьої сторони, і право на використання цифрових авторських прав може здійснювати трансфер між власником та покупцем. Після завершення транзакції кошти негайно зараховуються. Весь процес безкоштовний і відкритий для всієї мережі, що забезпечує безпеку та надійність усього процесу. У смарт-контракті зобов'язання представлені у вигляді даних. Учасники контракту заздалегідь транслюють угоду в систему блокчейн. Транзакція повинна забезпечити, що пропорція цифрового підпису за допомогою приватного ключа не менша за встановлену вагу, інакше транзакція не може набути чинності. Це значно знижує ризик порушення авторських прав у процесі обігу та підвищує безпеку транзакції.

Інформація про авторське право також є інформацією, збереженою в блоку, включаючи хеш-значення блоку, обсяг транзакцій та час першого публікування. Уся інформація про твори, які пройшли перевірку та не містять плагіату, може бути зареєстрована для сертифікації авторського права. Після того, як інформація про твір сертифікована та успішно зв'язана, її не можна змінювати. Для вищезазначеної інформації система має забезпечити, що інформація незмінна та абсолютно надійна, і використовує блокчейн для запобігання шахрайству.

Блокчейн можна вважати специфічною структурою даних, в якій кожен цифровий блок поєднується ланцюгом в порядку подій. Методи зберігання даних у блокчейні поділяються на розподілені та точка-до-точки. Це можна розглядати як інноваційну модель застосування, яка використовує низку комп'ютерних технологій, таких як алгоритми шифрування. Вперше блокчейн було застововано для запуску Біткоїна. Біткойн – це криптовалюта, а блокчейн – основна технологія. Зараз ключовими технологіями блокчейна є розподілений реєстр, асиметрична технологія шифрування, механізм консенсусу та розумний контракт [10].

Традиційна база даних може виконувати чотири основні операції з даними: додавання, видалення, зміну та перевірку. На відміну від традиційного розподіленого зберігання, кожен вузол учасника у мережі блокчейн має повне зберігання даних, і кожен вузол послідовно зв'язується ланцюгом хешів. Тому в блокчейні можна виконувати лише операції додавання та запиту даних, а зміни та видалення неможливі, що забезпечує максимальну незмінність даних.

У відмовостійких розподілених обчисленнях різні комп'ютери досягають консенсусу шляхом обміну інформацією для співпраці відповідно до набору правил. Однак іноді комп'ютери-учасники системи можуть помилятися і відправляти неправильну інформацію, що призводить до руйнування інформації, спричиняючи різні реакції членів мережі на загальну стратегію співпраці та порушуючи консистентність системи. Це також відомо як Задача візантійських генералів (Byzantine fault), що є проблемою відмовостійкості розподілених однорангових мереж у блокчейні.

Технологія асиметричного шифрування застосовується для захисту інформаційної безпеки в блокчейнs, і існують два методи цифрового шифрування та цифрового підпису. Цифрове шифрування відноситься до введення відповідної інформації в систему. Інформація оснащується відповідною парою ключів згідно з певним алгоритмом генерації. Система отримує пару ключів через відповідний алгоритм, коли є певний ввід (публічний та приватний ключі). Публічний ключ є загальнодоступним, а приватний ключ є приватним. Підписана цифровим методом криптовалюта спочатку доповнюється підписаним цифровим підписом на кінці і

відправляється наступному власнику після завершення перевірки на підробку. Після обробки будь-яке підмінення буде виявлено під час передачі. Цифрове шифрування та цифрова взаємодія разом забезпечують максимальну безпеку цифрової інформації. Процес асиметричного шифрування показано на рисунку 3.8 нижче.

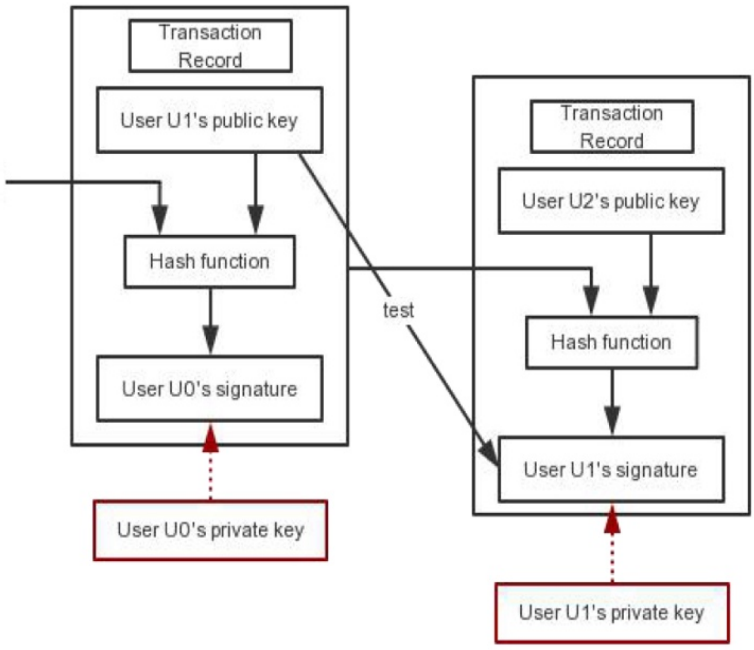


Рисунок 3.8 – Процес асиметричного шифрування

Смарт-контракти можуть бути застосовані лише у випадку, якщо середовище є достатньо надійним та безпечним, що майже неможливо досягти у нашому реальному світі. Таким чином, розумні контракти не використовувались у реальному житті, доки не був винайдений Біткоїн. Смарт-контракт – це контракт, який спільно розробляють користувачі в блокчейні для розповсюдження, перевірки та виконання комп'ютерних протоколів в інформаційній формі. Він дозволяє здійснювати довірені, відстежувані та незворотні контрактні транзакції без залучення третіх сторін. Розумний контракт у блокчейні – це фрагмент коду, написаний на блокчейні, який автоматично виконується, коли подія спричиняє виконання пункту контракту. Завдяки своїй децентралізації, відкритості та

прозорості, блокчейн забезпечує безпечне та достовірне середовище для застосування розумних контрактів.

Розумний контракт відіграє роль у оцінці блокчейну. Основним є верифікаційний вузол у блокчейні, який оцінює, чи може відповідна інформація бути перевірена та виконана за поточних умов. Після того, як вузол досягає стану консенсусу, блокчейн запускає механізм консенсусу та автоматично повідомляє користувача, який уклав контракт. У більш широкому розумінні, розумний контракт – це набір правил, закодованих мовою програмування, які ініціюють попередньо визначений набір дій, якщо ці правила виконані, без необхідності участі довіреної третьої сторони. Наразі розумні контракти часто застосовуються через нову архітектуру, вбудовану у блокчейн. Модель архітектури інтелектуальних контрактів показано на рисунку 3.9 нижче.

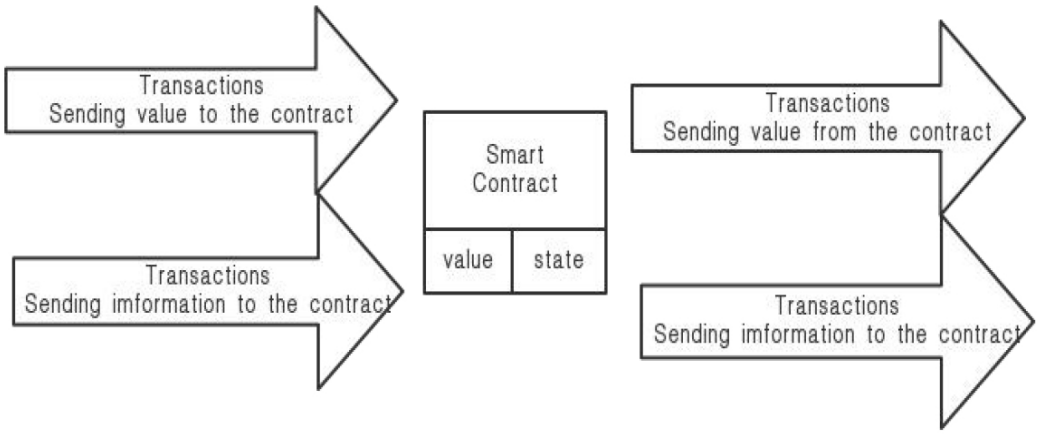


Рисунок 3.9 – Модель архітектури інтелектуальних контрактів

Основні функції системи захисту та транзакцій на основі блокчейну включають шифрування інформації про авторські права, перевірку інформації про авторські права та безпечну цифрову транзакцію авторських прав. Інформація про цифрові авторські права гарантовано захищена і надійна на рівні програмного забезпечення.

Якщо в системі є відповідний ввід інформації, алгоритмом буде генеруватися пара ключів, тобто публічний ключ і приватний ключ. Під час передачі даних

цифровий підпис буде доданий наприкінці цифрової валюти після певного процесу. Потім вона відправляється наступному користувачеві, щоб забезпечити асиметричне шифрування під час передачі. У цій роботі в основному використовується алгоритм шифрування цифрового підпису на еліптичних кривих для генерації відповідної пари ключів та цифрового підпису в процесі шифрування, як показано на рисунку 3.10:

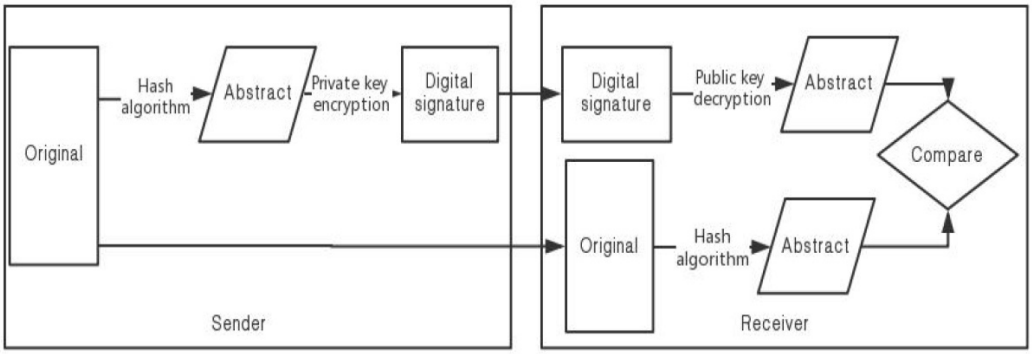


Рисунок 3.10 – Алгоритм шифрування цифрового підпису на еліптичних кривих

Пара ключів переважно є асиметричним шифруванням, яке реалізує весь процес передачі інформації. Спочатку інформація про транзакцію, збережена у блоку, хешується для отримання ключової інформації, а відправник шифрує ключову інформацію за допомогою приватного ключа та додає цифровий підпис на кінці інформації. Коли отримувач отримує цифровий підпис, використовується публічний ключ відправника для розшифровки інформації, та відновлюється сумарна інформація. Порівнюючи з ключовою інформацією, згенерованою з оригінального тексту, до наступного кроку переходить лише точно така ж інформація.

Першим є асиметричне шифрування, яке відноситься до ключа, пов'язаного з парою математичних алгоритмів. Інформацію, отриману шляхом шифрування одного з ключів, можна розшифрувати лише використовуючи ключ, пов'язаний з іншим алгоритмом шифрування. Публічний ключ можна викликати публічно, а

приватний ключ не можна розкривати. Шлях захисту публічного ключа, коли розшифровується публічний ключ показано на рисунку 3.11:

```
memset((void*)pFileAllPath,0,nPathLen);
strcpy(pFileAllPath,pFilePath);
strcat(pFileAllPath,"\\");
strcat(pFileAllPath,pPublicKey);
int nWritePublicKeyRet = WritePublicKeyToFile(pFileAllPath,ec_key);
```

Рисунок 3.11 – Шлях захисту публічного ключа, коли розшифровується публічний ключ

Приватний ключ в основному використовується для шифрування, і приватний ключ зберігається таким чином як показано на рисунку 3.12:

```
memset((void*)pFileAllPath,0,nPathLen);
strcpy(pFileAllPath,pFilePath);
strcat(pFileAllPath,"\\");
strcat(pFileAllPath,pPrivateKey);
int nWritePrivateKeyRet = WritePrivateKeyToFile(pFileAllPath,ec_key,ec_group);
```

Рисунок 3.12 – Спосіб зберігання приватного ключа

Коли користувач натискає кнопку перегляду, система переходить у стан інтелектуального аналізу. Запис потрапляє в чергу повідомлень, обробляється за допомогою dt, перетворюється у файл відбитків пальців, і id та статус цього запису відправляються до черги повідомлень. Після того, як сервісна система прослуховує це повідомлення, вона коригує статус запису для відповідності бібліотеці авторських прав та викликає інтерфейс порівняння відбитків пальців, щоб перевірити, чи існує новостворений відбиток у бібліотеці відбитків пальців. Якщо відбиток вже існує або частково існує, статус оновлюється як підтверджений, і з'являється посилання для перегляду користувачем. Посилання містить оригінальну адресу цифрових авторських прав та метадані, на цьому етапі користувач може вибрати, чи продовжувати подавати запит, чи ні. Якщо не

подавати, це вважається невдачею. Якщо продовжити подавати або статус коригується на розгляд. За замовчуванням, під час перегляду цифрових авторських прав існують деякі загальні описи для швидкого вибору. Весь процес аудиту потребує лише запиту інформації для порівняння блоків.

Поєднуючи традиційний процес транзакції авторських прав та концептуальну модель контракту на надання авторських прав, використовуючи характеристики технологію блокчейн та групову інтеграцію, ця робота головним чином конструює нейтралізовану модель транзакції авторських прав та пропонує модель смарт-контракту блокчейна, як показано на рисунку 3.13:

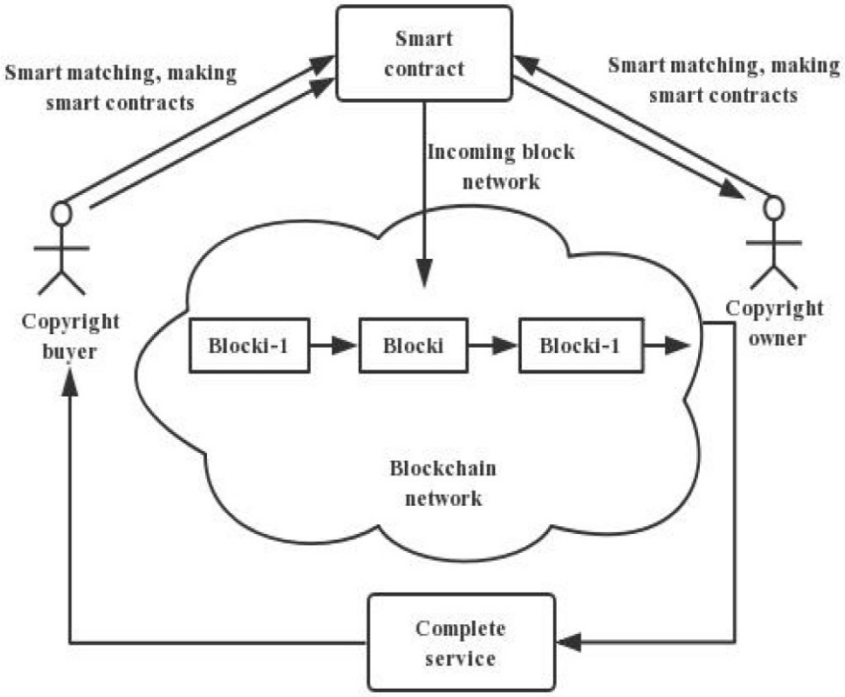


Рисунок 3.13 – Модель смарт-контракту блокчейна

Найважливішою функцією блокчейна в усій системі є поєднання важливої інформації. Вона включає ланцюг інформації про авторські права, ланцюг інформації про транзакції авторських прав та інформацію про авторизацію авторських прав. Ланцюжок реалізує незмінність інформації в блоку та забезпечує безпеку інформації про цифрові авторські права. На даний момент основний ланцюжковий код усієї системи становить близько 5 КБ. Після встановлення та

ініціалізації ланцюжкового коду на кожному вузлі мережі, час встановлення та ініціалізації ланцюжкового коду одного вузла тестувався як близько 9770 мс, а час одноразового ланцюжкового коду становить від 0.7 до 3с. Локальне середовище – це особистий комп'ютер Macbook Air на основі чіпа M2 з 10-ядерним графічним процесором, 8 ГБ оперативної пам’яті та 512 ГБ пам’яті.

Технологія блокчейн має характеристики децентралізації, незмінності та масштабованості. Вона може ефективно вирішити низку існуючих проблем захисту реєстрації цифрових авторських прав, відіграє ключову роль у захисті прав оригінальних творців та захисті цифрових авторських прав, і є новим способом управління інформацією про цифрові авторські права. Проте блокчейн також є новою технологією. Вона наразі не дуже зріла, і необхідно враховувати риизики від різних проблем у процесі використання. Технологія блокчейн може не тільки використовуватися у захисті цифрових авторських прав, але також може продовжувати розширюватися на фінансові послуги, соціальні послуги та глобалізуватись у майбутньому з розвитком технологій.

3.4 Алгоритм комбінованого використання інструментів для захисту авторського і суміжних прав на веб-ресурсах

Алгоритми захисту об’єктів авторського права і суміжних прав на web-ресурсах є стрижнем нашого дослідження – у попередніх розділах та підрозділах ми дослідили природу та актуальний стан розвитку як безпосередньо об’єктів авторського та суміжних прав на веб-ресурсах, так і кіберпростору. Ми розглянули технічну та юридичну сторону цієї складної сфери для пошуку вдосконалених рішень для технічного та правового врегулювання актуальних проблем.

Юридичний захист авторських прав на веб-ресурсах стикається з численними викликами, зокрема через глобальний та безкордонний характер Інтернету, що ускладнює контроль та визначення юрисдикції, а також через технологічні особливості, такі як легкість копіювання та поширення цифрового контенту, анонімність користувачів, відсутність уніфікованих міжнародних

стандартів, та виклики забезпечення справедливого використання. Ці фактори роблять ефективний захист авторських прав складним і вимагають гнучких та адаптивних юридичних підходів.

В той же час і технічна сторона як можливий шлях вдосконалення захисту авторського та суміжних прав в Інтеренті шляхом використання одного технічного рішення для захисту авторських прав на веб-ресурсах є складним через декілька ключових причин:

1) Різноманітність контенту веб-ресурси містять широкий спектр контенту, включаючи текст, зображення, аудіо, відео та інші мультимедійні формати. Кожен з цих типів контенту має унікальні характеристики та вимоги до захисту, які можуть не бути повністю задоволені одним технічним рішенням.

2) Технічні обмеження:

- хешування ефективне для виявлення змін у даних, але воно не дозволяє визначити авторство або контролювати розповсюдження контенту, крім того, хешування чутливе до будь-яких змін у контенті, що може бути проблематичним для динамічного веб-контенту;

- блокчейн хоч і забезпечує високу ступінь прозорості та незмінності, він може бути непрактичним для великого об'єму даних через обмеження масштабування та високі витрати на обробку та зберігання;

- цифровий водяний знак ефективний для певних типів медіа, але водяні знаки можуть бути видалені або пошкоджені, і їх застосування може бути складним для різних типів цифрового контенту.

3) Складність інтеграції технологій хешування, блокчейну та цифрових водяних знаків у існуючі системи управління веб-контентом може бути технічно складною та вимагати значних ресурсів для розробки та підтримки.

4) Змінність та динаміка веб-контенту, де веб-ресурси часто оновлюються та змінюються, що вимагає гнучких методів захисту, які можуть швидко адаптуватися до змін.

У зв'язку з цими викликами, часто ефективніше використовувати комбінацію різних технологій та методів для захисту авторських прав на веб-ресурсах, замість намагання знайти універсальне рішення.

Тож ми у даному дослідженні, висвітливши та розглянувши різні аспекти регулювання правового та технічого для об’єктів авторського права, приходимо до висновку, що така нетривіальна задача потребує пошуку нових алгоритмів захисту.

Якщо розміщені на веб-ресурсах об’єкти захисту можуть мати різний формат, то необхідно стандартизувати та впроваджувати комплексний захист шляхом комбінування блокчейну, хешування та цифрових водяних знаків як комбінований та такий, що повинен братись за основу в доповнення до юридичної складової.

Ми пропонуємо поступово відмовитись від централізованих систем управління правами. Перехід від централізованих до децентралізованих систем управління правами може значно підвищити безпеку та прозорість, оскільки вони менш вразливі до атак та цензури завдяки відсутності одиночних точок відмови та централізованого контролю. Такі системи також підвищують гнучкість та масштабованість, дозволяючи легше адаптуватися до змін та зростання, а також знижують загальні витрати на утримання та адміністрування, в той час як сприяють інноваціям та творчості завдяки більшій відкритості та можливостям для колаборації. Однак цей перехід вимагає уважного підходу з урахуванням технічних та юридичних викликів, що виникають у процесі реалізації децентралізації.

Важливо також враховувати рівень складності адміністрування централізованих і децентралізованих систем управління правами за ключовими аспектами, що можна побачити у таблиці 3.1.

Але попри окреслені вище особливості, при застосуванні комбінованого алгоритму захисту об’єктів авторського права, децентралізована система управління правами не обов’язково повинна бути реалізована найбільш технологічним шляхом та із застосуванням найбільш передових технологій, а лише виходячи із співвідностості умовної вартості об’єкта охорони до технології децентралізованого управління. Виходячи із умовного призначення кожного із

засобів захисту, про які ми говорили вище, застосування технології блокчейн – це етап первісної реєстрації авторського права, а отже – це умовний момент фіксації авторського та суміжних прав у цифровому середовищі, який практично неможливо змінити за рахунок технології його реалізації, що було неможливо при застосуванні традиційних способів за засобів.

Таблиця 3.1 – Ключові аспекти централізованих та децентралізованих систем

Аспект	**Централізовані Системи**	**Децентралізовані Системи**
Адміністрування	Спрощене управління та координація завдяки єдиному центру контролю.	Складне управління через необхідність координації між численними незалежними учасниками.
Масштабування та обслуговування	Обмежене масштабування; підвищення потужності вимагає розширення центральної інфраструктури.	Легше масштабування, оскільки нові вузли можуть бути додані без значного навантаження на існуючу інфраструктуру.
Безпека	Підвищені ризики через одиночні точки відмови; вразливість до централізованих атак.	Знижені ризики одиночних точок відмови; розподіл відповідальності сприяє забезпеченню безпеки.

Вибір технології блокчейну, яка є водночас недорогою і надійною, залежить від конкретного використання та потреб. На даний момент існують декілька популярних блокчейн-платформ, які вважаються відносно економічно вигідними та надійними.

Ethereum є однією з найбільш використовуваних блокчейн-платформ, особливо для розробки децентралізованих додатків (dApps) та смарт-контрактів. Хоча вартість транзакцій на Ethereum (відома як "gas fees") може коливатися, платформа відома своєю гнучкістю та широким співтовариством.

Binance Smart Chain (BSC) – пропонує схожі можливості, як Ethereum, але з нижчими комісійними за транзакції. Вона швидко набула популярності завдяки своїй економічній ефективності та сумісності з Ethereum.

Polygon (раніше Matic Network) – працює як "другий шар" для Ethereum, надаючи додаткові можливості масштабування та зменшуючи вартість та час транзакцій.

Stellar орієнтований на спрощення та зниження вартості міжнародних транзакцій. Він ідеально підходить для крос-кордонних платежів та має відносно низькі комісійні.

Cardano хоча і ще розвивається, вона відома своїм науковим підходом та високим ступенем безпеки. Платформа покликана надати високу ефективність з мінімальними витратами на транзакції.

Перед вибором платформи ми рекомендуємо ретельно проаналізувати власні потреби, вартість транзакцій, можливості масштабування, спільноту та підтримку, а також ступінь надійності та безпеки, який надає кожна платформа, але як перший крок у алгоритмі захисту авторського і суміжних прав на веб-ресурсах – блокчейн відповідає найнеобхіднішим критеріям.

Після реєстрації авторського та суміжних прав у децентралізованій системі управління правами автор може більш безпечно розмістити об’єкт своєї інтелектуальної діяльності на веб-ресурсах. Наступним кроком варто використовувати окремо чи комбіновано у залежності від типу об’єкту захисту – хешування та/і цифровий водяний знак. Ці інструменти також потрібно вивести у стандартизовану площину, реалізувати їхнє застосування у більш простий спосіб для користувача.

Як ми вже згадували, хеш може бути звичайний (або криптографічний хеш) та перцептивний і використовуються вони для різних цілей та мають істотні відмінності в своїй структурі та застосуванні, які ми відобразили у таблиці 3.2.

Поєднання та комбінування функції хешування при реєстрації авторського права у децентралізованій системі управління правами дозволяє створити додатковий ступінь фіксації прав на конктретний об’єкт захисту та подальшої ідентифікації і пошуку можливих фактів порушення.

Таблиця 3.2 – Порівняння криптографічного та перцептивого хешування

Критерій	Звичайний Хеш	Перцептивний Хеш
Мета	Перевірка цілісності даних, аутентифікація, криптографічне застосування.	Виявлення подібності в мультимедійному контенті (зображення, аудіо).
Властивості	Унікальний та незворотний вихід; маленька зміна в даних призводить до значної зміни в хеші (ефект лавини).	Генерує схожі хеші для схожих даних, толерантний до деяких змін у контенті.
Застосування	Криптографічне шифрування, безпека даних, хеш-таблиці.	Пошук дублікатів зображень/аудіо, кластеризація мультимедійного контенту.
Приклади	SHA-256, MD5.	pHash, dHash.

Як третій ступінь захисту для утворення цілісного алгоритму ми рекомендуємо використовувати цифрові водяні знаки там, де це можливо (як ми дослідили – для тексту цей варіант не підходить). Цей етап рекомендований безпосередньо перед розміщенням об’єктів на веб-ресурси.

Тож описаний нами алгоритм захисту авторських та суміжних прав на веб-ресурсах, що комбінує реєстрацію прав у децентралізованих системах, використання хеш-функцій та застосування цифрових водяних знаків, демонструє високу ступінь надійності та життєздатності з огляду на сучасні вимоги цифрової економіки.

Використання блокчейн-технологій для реєстрації авторських прав забезпечує іммутабельність (незмінність) та прозорість реєстраційних записів. Децентралізація даних сприяє відсутності єдиних точок відмови, зменшуючи ризики цензури чи маніпуляцій. Консенсусні механізми, такі як Proof of Work або Proof of Stake, забезпечують валідацію транзакцій та дійсність записів.

Використання криптографічних хеш-функцій для створення унікального ідентифікатора цифрових активів є ключовим для забезпечення цілісності та автентичності контенту. Хеші можуть служити як цифрові "відбитки пальців" для контенту, гарантуючи, що будь-які зміни в документі чи файлі можуть бути легко виявлені.

Інтеграція цифрових водяних знаків надає додатковий шар захисту, дозволяючи вбудовувати невидимі ідентифікаційні маркери в мультимедійний

контент. Це забезпечує захист від несанкціонованого копіювання та розповсюдження, а також дозволяє відстежувати походження та використання контенту.

Об'єднання цих трьох компонентів дозволить створити комплексну та багаторівневу систему захисту авторських прав, яка є адаптивною до сучасних викликів цифрового контенту. Такий підхід забезпечить глибоку інтеграцію технологій із юридичними рамками авторського права, сприяючи ефективному управлінню правами та забезпечуючи надійний захист інтелектуальної власності в онлайн-середовищі.

ВИСНОВКИ

У даній роботі нами досліджено алгоритми захисту авторських та суміжних прав на веб-ресурсах, враховуючи як юридичні, так і технічні аспекти цієї сфери. Проаналізовано, що юридичний захист авторських прав стикається з численними викликами, пов'язаними з глобальним характером Інтернету, технологічними особливостями, такими як легкість копіювання та поширення цифрового контенту, а також відсутністю уніфікованих міжнародних стандартів. З іншого боку, технічний захист обмежений через різноманітність контенту, технічні обмеження різних методів (хешування, блокчейн, цифрові водяні знаки) та складності їх інтеграції в системи управління веб-контентом.

Дослідження вказує на необхідність комбінування різних технологій для ефективного захисту прав на веб-ресурсах. Рекомендується перехід від централізованих до децентралізованих систем управління правами, що забезпечує більшу безпеку, прозорість, гнучкість та масштабованість. Такий підхід може сприяти інноваціям та творчості, однак вимагає урахування технічних та юридичних викликів. Пропонується використання комбінованого алгоритму, який включає блокчейн для первісної реєстрації прав, хешування для створення унікальних ідентифікаторів контенту та цифрові водяні знаки для захисту мультимедійного контенту. Це дозволяє створити комплексну систему захисту прав, адаптовану до викликів цифрового контенту, інтегруючи технології з юридичними рамками для ефективного управління правами та захисту інтелектуальної власності в онлайн-середовищі.

Досліджено, розглянуто та проаналізовано використання технологій блокчейну, хеш-функцій, та цифрових водяних знаків для захисту авторських та суміжних прав на веб-ресурсах. Було вивчено юридичні та технічні аспекти захисту цих прав.

Використано сучасні технологічні рішення, такі як блокчейн, для створення надійної та ефективної системи захисту прав. Було розглянуто різні аспекти кожного інструменту, включаючи їхні переваги та недоліки.

Розроблено комплексний алгоритм, що використовує переваги кожного із зазначених інструментів.

Можливість використання результатів у соціально-економічному житті полягає у тому, що цей алгоритм може значно підвищити безпеку, прозорість та ефективність управління авторськими правами в цифровому просторі та сприяти розвитку цифрової економіки.

Практична цінність відображена у можливості застосування цього підходу компаніями та індивідуальними авторами з метою допомогти ефективно захищати свої права на цифровий контент.

Рекомендації щодо використання результатів у навчальному процесі:

- цей алгоритм може бути використаний як важливий навчальний матеріал у курсах з цифрової безпеки, права інтелектуальної власності та інформаційних технологій.

Напрямками подальших досліджень можна окреслити наступні:

- розвиток додаткових методів для забезпечення сумісності з різними типами цифрового контенту;

- адаптація та інтеграція алгоритму в існуючі системи управління контентом;

- дослідження потенціалу використання штучного інтелекту для покращення автоматизації процесів реєстрації та моніторингу прав.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. A. Jones. “Audius’ next-generation streaming service is plagued by piracy: Billboard.” Feb. 2022. [Електронний ресурс]. – Режим доступу: https://www.nmpa.org/audius-next-generation-streaming-service-is-plagued-by-piracy/
2. Brassil, J.T., Low, S., Maxemchuk, N.F. and O'Gorman, L., 'Electronic marking and identification techniques to discourage document copying', IEEE Journal on Selected Areas in Communications, 13, 1995, pp 1495-1504; N.F. Maxemchuk and Low, S., 'Marking text documents', IEEE International Conference on Image Processing, IEEE, 1997, pp 13-16;
3. C. Gruhier. “Audius: The streaming platform that pays its artists (and listeners) the most?” Mar. 2021. [Online], Available: https://www. haumeamagazine.com/en/audius-the-streaming-platform-that-pays-its-artists-and-listeners-the-most/
4. C. Liu, J. Li, J. Duan, H. Shen, and H. Huang, “LightCvT: Audio forgery detection via fusion of fight CNN and transformer,” in Proc. 10th Int. Conf. Comput. Pattern Recognit., 2021, pp. 99-105
5. Craver, S., Memon, N., Yeo, B.L. and Yeung, M.M., 'Resolving rightful ownerships with invisible watermarking techniques', IEEE Journal on Selected Areas in Communications, 16, 1998, pp 573-586.
6. D. Deahl. “New blockchain-based music streaming service Audius is a copyright nightmare.” Oct. 2019. [Електронний ресурс]. – Режим доступу: https://www.theverge.com/2019/10/9/20905384/audius-blockchain-music-streaming-service-copyright-infringement-piracy
7. D. Jang, C. D. Yoo, S. Lee, S. Kim, and T. Kalker, “Pairwise boosted audio fingerprint,” IEEE Trans. Inf. Forensics Security, vol. 4, pp. 995-1004, 2009.
8. E. Staff, Blockchains: Ths great chain of being sure about things, Econom.Retriev. 18 (2016).
9. Hartung, F. and Kutter, M., 'Multimedia watermarking techniques', Proceedings of the IEEE, 87, 1999, pp 1079- 1107;

10. Hu guang. Application scenario research of intelligent intellectual property management based on block chain technology. Journal of henan university of technology (social science edition), 2019,15(02): 50-55

11. I. S. Igboanusi, K. P. Dirgantoro, J.-M. Lee, and D.-S. Kim, “Blockchainside implementation of pure wallet (PW): An offline transaction architecture,” ICT Exp., vol. 7, no. 3, pp. 327-334, 2021.

12. J. L. Zhao, S. Fan, and J. Yan, “Overview of business innovations and research opportunities in blockchain and introduction to the special issue,” Financ. Innov., vol. 2, p. 28, Dec. 2016.

13. Jing yi . Research on quality management framework of manufacturing supply chain based on block chain.Electromechanical engineering technology, 2019(05):165-168.

14. K. P. Dirgantoro, J. M. Lee, and D.-S. Kim, “Generative adversarial networks based on edge computing with blockchain architecture for security system,” in Proc. Int. Conf. Artif. Intell. Inf. Commun. (ICAIIC), 2020, pp. 039-042.

15. LukaS Lalinsky, «How does chromaprint work?». 2011. [Електронний ресурс]. – Режим доступу: https://oxygene.sk/2011/01/how-does-chromaprint-work/

16. M.-J. Kim, C. Yoo, and Y.-W. Ko, “Multimedia file forensics system exploiting file similarity search,” Multimedia Tools Appl., vol. 78, pp. 5233-5254, Mar. 2019.

17. Main Page Apple.com [Електронний ресурс]. – Режим доступу: https://www.apple.com

18. Mintzer, F., Gazes, A., Giordano, F., Lee, J., Magerlein, K. and Schiatterella, F., 'Capturing and preparing images of Vatican Library manuscripts for access via Internet', IT&T's 48th Annual Conference, Washington DC, USA, 1995, pp 74-77.

19. N. Nizamuddin, K. Salah, M. A. Azad, J. Arshad, and M. H. Rehman, “Decentralized document version control using Ethereum blockchain and IPFS,” Comput. Elect. Eng., vol. 76, pp. 183-197, Jun. 2019.

20. P. Rai, “Copyright laws and digital piracy in music industries: The relevance of traditional copyright laws in the digital age and how music industries should cope with

the ongoing piracy culture," Ph.D. dissertation, Dept. Music Manag., Universitetet i Agder, Kristiansand, Norway, Feb. 2021.

21. P. Samanta and S. Jain, "Analysis of perceptual hashing algorithms in image manipulation detection," Procedia Comput. Sci., vol. 185, pp. 203-212, Jun. 2021.

22. Pirate Site Traffic Surges With Help From Manga Boom [Електронний ресурс]. – Режим доступу: https://torrentfreak.com/pirate-site-traffic-surges-with-help-from-manga-boom-220503/

23. R. K. Das, J. Yang, and H. Li, "Long range acoustic and deep features perspective on ASVspoof 2019," in Proc. IEEE Autom. Speech Recognit. Understanding Workshop (ASRU), 2019, pp. 1018-1025.

24. S. Nakamoto. "Bitcoin: A peer-to-peer electronic cash system." Mar. 2009. [Електронний ресурс]. – Режим доступу: https://www.metzdowd.com

25. Secure Digital Music Initiative, SDMI portable device specification version 1.0, 8 July, 1999; 'Frequently-asked questions', DVD Copy Control Association, [Електронний ресурс]. – Режим доступу: http://www.dvdcca.org/faq.html

26. Swanson, M.D., Kobayashi, M. and Tewfik, A.H., 'Multimedia data-embedding and watermarking technologies', Proceedings of the IEEE, 86, pp 1064-1087;

27. The US Congress High–Performance Computing Act of 1991 [Електронний ресурс] // NITRD (The Networking and Information Technology Research and Development Program). – Режим доступу: http://www.nitrd.gov/congressional/laws/102–194.pdf

28. X. Lin and X. Kang, "Supervised audio tampering detection using an autoregressive model," in Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP), 2017, pp. 2142-2146.

29. X. Wang, X. Zhou, Q. Zhang, B. Xu, and J. Xue, "Image alignment based perceptual image hash for content authentication," Signal Process. Image Commun., vol. 80, Feb. 2020, Art. no. 115642.

30. Y. Jiang, C. Wu, K. Deng, and Y. Wu, "An audio fingerprinting extraction algorithm based on lifting wavelet packet and improved optimal-basis selection," Multimedia Tools Appl., vol. 78, no. 21, pp. 30011-30025, 2019.

31. Y. Li, J. Wei, J. Yuan, Q. Xu, and C. He, “A decentralized music copyright operation management system based on blockchain technology,” Procedia Comput. Sci., vol. 187, pp. 458-463, 2021, Jun. 2021.

32. Y. Lin and W. H. Abdulla, Audio Watermark, vol. 146. Cham, Switzerland: Springer, 2015.

33. Z. Wang, Y. Yang, C. Zeng, S. Kong, S. Feng, and N. Zhao, “Shallow and deep feature fusion for digital audio tampering detection,” EURASIP J. Adv. Signal Process., vol. 2022, no. 1, pp. 1-20, 2022.

34. Zhao Feng, around. Analysis on digital copyright protection based on block chain technology . Science, technology and law, 2017,29 (1)

35. Андрощук Г.О. Цифрове піратство та контрафакція в умовах цифрової трансформації: аналіз стану, тенденції, механізми протидії / Андрощук Г.О. // Теорія і практика інтелектуальної власності - 2023. - №3. – с.97-98.

36. Деякі проблеми захисту авторських прав у мережі інтернет [Електронний ресурс] : Юридичний науковий електронний журнал / Яницька О.Л., Амбруш Г.Л., Коваль О.М. // 2019. - №6. – с.147. – Режим доступу: http://www.lsej.org.ua/6_2019/35.pdf

37. Закон України «Про авторське право і суміжні права» від 01.12.2022 № 2811-IX (Редакція станом на 15.04.2023) [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2811-20

38. Захист авторських прав в мережі Інтернет. Поради юристів Stalirov & Co [Електронний ресурс]. – Режим доступу: https://stalirov.lawyer/uk/posts/zahist-intelektualnoyi-vlasnosti-v-interneti

39. Історія інтернету - Матеріал з Вікіпедії — вільної енциклопедії [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Історія_Інтернету

40. Федонюк С.В. Міжнародні аспекти безпеки кіберпростору : монографія / Волинський національний університет імені Лесі Українки. Луцьк : Вежа-Друк, 2022., с.10