



DOI 10.28925/2663-4023.2025.28.854

УДК 004.056

Фещак Ірина Сергіївна

Студентка кафедри захисту інформації

Національний Університет «Львівська Політехніка», Львів, Україна

ORCID ID: 0009-0008-6827-1049

iryna.feshchak.kb.2023@lpnu.ua**Онофрійчук Соломія Василівна**

Студентка кафедри захисту інформації

Національний Університет «Львівська Політехніка», Львів, Україна

ORCID ID: 0009-0004-7047-2828

solomiia.onofriichuk.kb.2023@lpnu.ua**Гарасимчук Олег Ігорович**

Канд. технічних наук, доцент кафедри захисту інформації

Національний університет «Львівська політехніка», Львів, Україна

ORCID ID: 0000-0002-8742-8872

oleh.i.harasymchuk@lpnu.ua**ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ АВТОРСЬКИХ ПРАВ,
ЯК ІНСТРУМЕНТИ БОРОТЬБИ З ПІРАТСТВОМ ЕЛЕКТРОННИХ КНИГ**

Анотація. З розвитком цифрових технологій проблема захисту авторських прав стає все більш актуальною, особливо у сфері електронних книг. Це обумовлено невідомим зростанням кількості контенту, зручністю його розповсюдження через Інтернет і технічними можливостями копіювання без втрати якості. У зв'язку з цим виникає необхідність розробки ефективних засобів захисту авторських прав. У статті розглядаються основні аспекти захисту авторських прав, включаючи правові засади, технічні методи боротьби з піратством та їх ефективність. Зокрема, проаналізовано поточну ситуацію щодо оцінки користувачами наявних систем захисту та ставлення до піратства, яке є однією з головних перешкод для розвитку ринку електронних книг. Особливу увагу приділено дослідженню технічних методів, таких як DRM, шифрування, водяні знаки, онлайн-активація та обфускація коду, їх перевагам та недолікам. До прикладу, DRM може обмежувати законне користування вмістом, викликаючи негативну реакцію в користувачів, натомість водяні знаки дозволяють ідентифікувати першоджерело файлу без втрати якості та контенту. У статті зазначено, що жоден із методів не дає повної гарантії захисту, що обумовлює необхідність комплексного підходу. На основі аналізу існуючих проблем запропоновано інноваційний метод захисту електронних книг, що базується на поєднанні динамічного цифрового підпису та блокчейн-технологій. Динамічний підпис дозволяє змінювати значення авторизаційних даних залежно від користувача, а використання блокчейну забезпечує неможливість підробки та простежуваність усіх операцій, пов'язаних з контентом. У статті також обговорюються виклики та обмеження, пов'язані з впровадженням нових методів захисту, та наголошується на важливості комплексного підходу, що поєднує технічні, економічні та освітні заходи для ефективної боротьби з піратством у цифровому середовищі. Проблема піратства неможливо розв'язати лише технічними засобами — важливо забезпечити ефективну співпрацю між правовласниками, розробниками технологій та користувачами. Лише через поєднання зусиль на національному та міжнародному рівнях можна досягти сталого й ефективного захисту авторських прав у цифрову епоху.

Ключові слова: авторське право; електронні книги; піратство; цифровий захист; DRM (Digital Rights Management); водяні знаки (Watermarking); шифрування; онлайн-активація; обфускація коду; блокчейн; цифровий підпис; захист контенту.

ВСТУП

У сучасному світі електронні книги стали важливим джерелом знань та інформації, доступним широкій аудиторії. Хтось використовує їх для того, аби дізнатись чи навчитись чомусь новому, а хтось аби відпочити та поринути у світ історій, емоцій та переживань, це відбувається тому, що електронні книги мають низку переваг, які представлені на рисунку нижче:

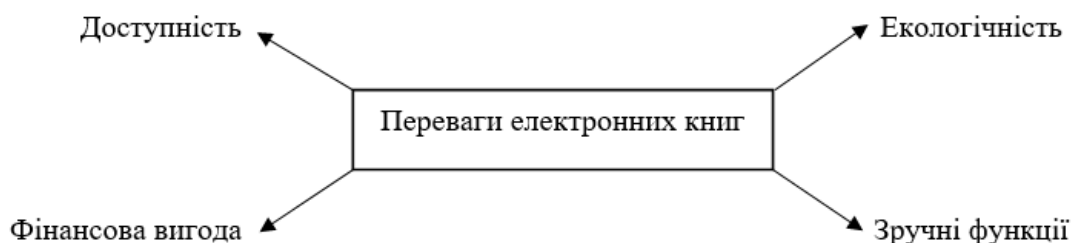


Рис. 1. Переваги електронних книг

Це свідчить про те, що книги можна читати на телефоні, планшеті чи ноутбуці; виробництво таких книг не вимагає витрат паперу; електронні книги значно дешевші.

Варто зазначити, що з розвитком цифрових технологій посилюється проблема захисту авторських прав. Незаконне поширення контенту, або цифрове піратство, завдає значних збитків авторам, видавцям та індустрії інтелектуальної власності загалом. Авторське право гарантує творцям виключне право контролювати використання своїх творів, що стимулює їх до подальшої творчості. Водночас надмірні обмеження у використанні інформації можуть стримувати науковий розвиток, культурний прогрес і ускладнювати доступ до освіти [1], [2].

Огляд літературних джерел

Перш ніж перейти до конкретних методів захисту авторських прав на електронні книги, варто розглянути методологічні засади цього питання. Хоча більшість користувачів електронних книг дотримуються закону, проте також існують і ті, хто порушує авторські права. Такі дії мають свої причини та можуть призвести до серйозних наслідків (див табл. 1.)

Таблиця 1

Причини та наслідки порушень авторських прав

Причина	Наслідок
Висока вартість — читачі шукаючи безкоштовні або дешевші альтернативи, натрапляють на піратські видання.	Фінансова втрата авторів та видань — знижується прибуток, який відповідно затримує випуск нових книг.
Легкодоступність — такі видання можна знайти в мережі за декілька кліків.	Загроза комп'ютерним пристроям — багато піратських сайтів містять віруси, шкідливе програмне забезпечення або шахрайські схеми.
Доступність піратських ресурсів — у мережі існують десятки сайтів, які надають безкоштовний доступ до книг без будь-яких юридичних наслідків.	Закриття малих видавництв та незалежних платформ — невеликі видавництва та онлайн-книгарні не можуть конкурувати з безкоштовними піратськими копіями.



Анонімність інтернету — користувачі можуть легко отримувати піратський контент, не боячись покарання.	Юридична відповідальність — за використання і розповсюдження піратського контенту передбачені штрафні санкції.
Відсутність правової культури — багато людей не сприймають скачування піратських книг як щось незаконне або неетичне.	Блокування доступу до легальних сервісів — видавництва можуть обмежувати доступ до контенту через масове піратство.

Авторське право виступає основним інструментом, який гарантує авторам належне визнання та винагороду за їхню інтелектуальну працю. Це право виникає автоматично з моменту створення твору, надаючи його творцю виключні можливості розпоряджатися своїм творінням. Основні засади авторського права включають:

Право на авторство — автор має право на зазначення свого імені під час використання твору, навіть якщо майнові права були передані іншій особі.

Обмеження прав — закон дозволяє використовувати твори в межах цитування та інших передбачених законом випадків.

Цифровий захист — сучасні технології, зокрема DRM (Digital Rights Management), сприяють захисту контенту від несанкціонованого копіювання та поширення.

Відповідальність за порушення — незаконне використання об'єктів авторського права може призвести до цивільної, адміністративної або кримінальної відповідальності згідно з чинним законодавством України.

Авторське право в Україні регулюється низкою нормативно-правових актів, нижче наведена таблиця з основними статтями та їх змістом (табл. 2):

Таблиця 2

Нормативно-правові акти щодо авторських прав в Україні

Нормативно-правовий акт	Стаття/Розділ	Зміст
Закон України «Про авторське право і суміжні права»	Загальний закон	Регулює охорону, передачу та захист авторських прав
Цивільний кодекс України	Глава 36	Містить загальні положення про інтелектуальну власність
Кримінальний кодекс України	Стаття 176	Передбачає кримінальну відповідальність за незаконне
Кодекс України про адміністративні правопорушення	Стаття 51, частина 2	Встановлює штрафи за порушення авторських прав

Окрім правових засобів захисту, існують також технічні (наприклад, DRM), економічні (ліцензування, монетизація) та освітньо-інформаційні методи, що допомагають боротися з піратством і підтримують правову культуру у сфері інтелектуальної власності. Ці підходи сприяють збалансованому захисту прав авторів і забезпечують доступ споживачів до культурних продуктів у межах закону [3].

Таким чином, дотримання основних принципів авторського права і використання комплексного підходу до захисту творчості є запорукою справедливого ставлення до авторів і ефективного функціонування системи охорони інтелектуальної власності в Україні.

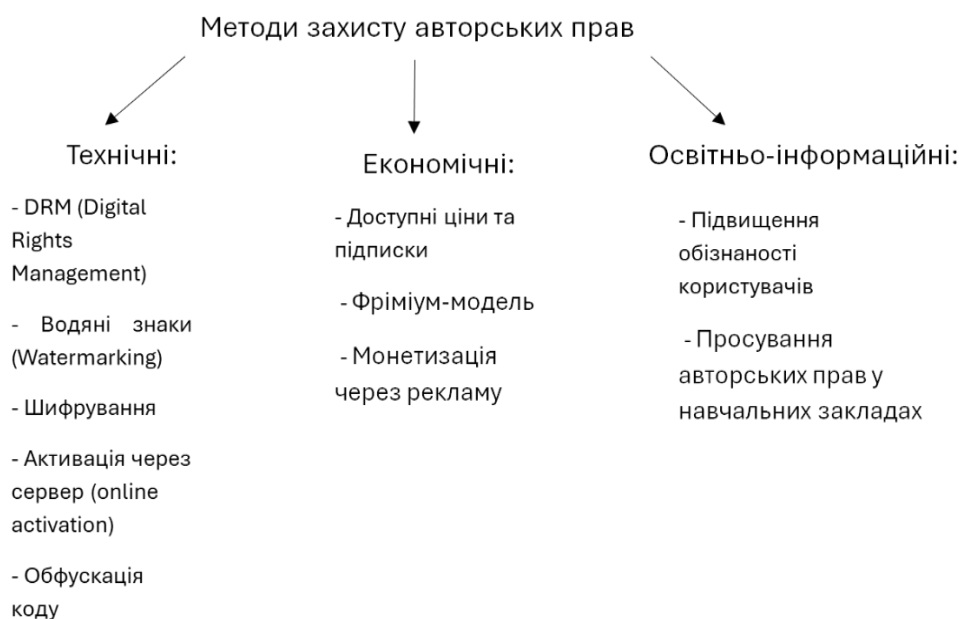


Рис. 2. Методи боротьби з піратством

Постановка проблеми. Головною метою цієї статті є дослідження ефективності сучасних методів захисту авторських прав на електронні книги та їхньої ролі у протидії піратству. Також передбачено формулювання рекомендацій щодо удосконалення захисту авторських прав у цифровому середовищі, зокрема пропозиції щодо покращення існуючих систем і перспектив їх подальшого розвитку.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Проблему захисту авторських прав досліджують різні науковці як в Україні, так і за кордоном. Зокрема, у статті О. М. Брайко [4]. розглянуто основні проблеми правової охорони авторського права в Україні, серед яких виділяються порушення немайнових і майнових прав авторів, такі як піратство, плагіат, а також ввезення на територію України творів без дозволу правовласників. Автор підкреслює необхідність удосконалення нормативно-правової бази для ефективного захисту авторських прав.

Міжнародний аспект захисту авторських прав розкрито у статті, присвяченій міжнародному правовому регулюванню авторських і суміжних прав у цифровому середовищі, (ВОІВ) від 20 грудня 1996 року: Договору ВОІВ про авторське право (чинний з 6 березня 2002 року) та Договору ВОІВ про виконання і фонограми (чинний з 20 квітня 2002 року). Ці договори забезпечують основу правового регулювання використання об'єктів авторського права і суміжних прав у цифровому середовищі, що охоплює боротьбу з онлайн-піратством, захист прав у соціальних мережах та сфері електронної комерції [5]. Автори звертають увагу на посилення заходів проти онлайн-піратства, захист прав у соціальних мережах та сфері електронної комерції, а також на необхідність модернізації національних систем інтелектуальної власності відповідно до міжнародних стандартів [6].

Серед закордонних досліджень заслуговує уваги робота «Cross-Border Enforcement of Copyright Judgments: Balancing Rights and Research Freedoms» [7], присвячена проблемам виконання іноземних рішень щодо авторських прав. Автор аналізує ризики,

пов'язані з екстериторіальним застосуванням рішень судів, та підкреслює, що це може підривати баланс між захистом прав авторів і правом на дослідження, особливо у транскордонних спорах.

В українському контексті важливу роль у захисті авторських прав відіграє Українська агенція з авторських та суміжних прав (УААСП) [8], яка займається колективним управлінням майновими правами, юридичною підтримкою авторів і співпрацею з міжнародними організаціями для захисту прав українських авторів за кордоном.

З метою дослідження ставлення користувачів до піратства електронних книг було проведено опитування серед студентів та молодих фахівців у галузі інформаційних технологій. В опитуванні взяли участь 70 респондентів у віці від 18 до 30 років. Анкетування здійснювалося за допомогою Google Forms у квітні 2025 року.

Результати опитування

На рис. 3 подано відповіді на запитання: «Де ви зазвичай берете електронні книги?»



Рис. 3. Основні джерела отримання електронних книг

Як видно з рисунка, аж 56,9% опитаних завантажують книги з безкоштовних сайтів і лише 10,3% купують на офіційних платформах

На рисунку 4 представлено результати на запитання: «Які основні причини, на вашу думку, спонукають людей завантажувати піратські електронні книги? (можна обрати кілька варіантів)».

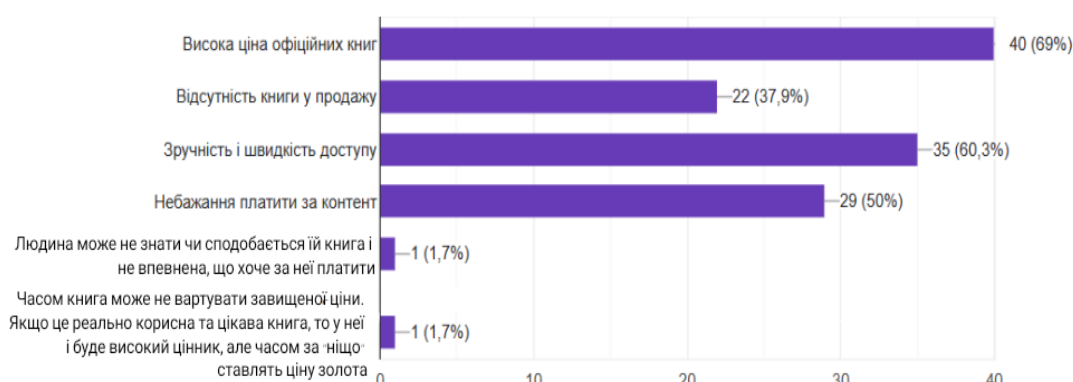


Рис. 4. Причини піратства електронних книг

Рис. 5 демонструє відповіді людей на питання: «Як ви оцінюєте ефективність технічних заходів боротьби з піратством (DRM, водяні знаки, обмеження доступу тощо)?».



Рис. 5. Ефективність технічних заходів боротьби з піратством

На рис. 6 представлено результати на запитання: «Який спосіб боротьби з піратством, на вашу думку, найкращий?».

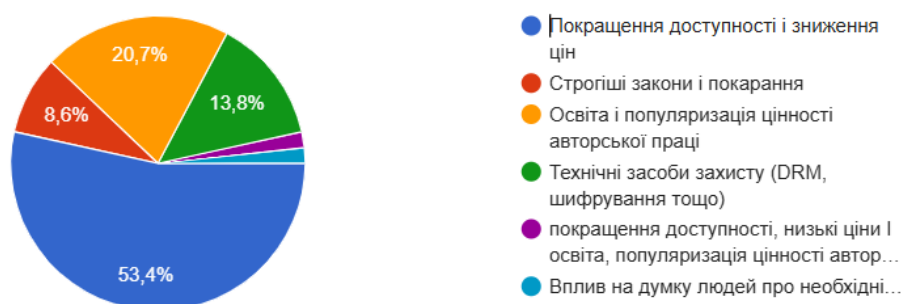


Рис. 6. Способи боротьби з піратством

Аналізуючи результати опитування можна зрозуміти, що постає необхідність аналізу ефективності сучасних методів у захисті авторських прав електронних книг та розгляду їх ролі у боротьбі з піратством, а також необхідно сформулювати рекомендації щодо вдосконалення захисту авторських прав у цифровому середовищі — запропонувати шляхи покращення існуючих систем та перспективи їхнього розвитку.

Технічні методи захисту електронних книг від піратства являють собою сукупність заходів, спрямованих на запобігання несанкціонованому копіюванню, розповсюдженню та використанню цифрового контенту. Основні цілі таких методів включають *контроль доступу*, що обмежує використання електронних книг лише авторизованими користувачами; *запобігання копіюванню* шляхом ускладнення або блокування створення копій; *відстеження нелегального розповсюдження* через ідентифікацію джерел витоку; *захист цілісності контенту*, що запобігає його зміні або модифікації [9] – [11].

Розглянемо дані методи **детальніше**:

- *DRM (Керування цифровими правами)* — це технології, які обмежують використання цифрового контенту, такого як електронні книги, музика, фільми та програмне забезпечення, з метою запобігання несанкціонованому копіюванню та поширенню, захищаючи права власників авторських прав [12],



[13]. DRM застосовує різні методи, зокрема шифрування, контроль доступу та обмеження використання, щоб регулювати дії користувачів із цифровим контентом. Шифрування перетворює дані у формат, який можна відкрити лише за допомогою спеціального ключа, а контроль доступу може включати авторизацію, ліміти на кількість пристроїв або час користування [14].

У лютому 2025 року Amazon закрила функцію «Завантаження та передача через USB» у Kindle, яка дозволяла завантажувати книги у форматі AZW3 — саме цей формат пірати використовували для легкого зняття DRM-захисту. Це рішення покликане ускладнити піратство, але при цьому користувачі все ще можуть передавати книги через Wi-Fi. Зміни викликали занепокоєння серед читачів, які звикли робити локальні резервні копії та конвертувати книги для інших пристроїв [15].

- *Шифрування* — спосіб зробити інформацію таємною. Це як написати повідомлення незрозумілою мовою, яку може прочитати лише той, хто знає секретний ключ. Електронні книги можуть бути зашифровані як окремі файли, що вимагають пароль для відкриття. Це забезпечує додатковий рівень захисту, особливо для конфіденційних документів або книг, які не призначені для широкого розповсюдження. Формат PDF дозволяє шифрувати файли та встановлювати паролі для відкриття або редагування. У своїй основі, шифрування — це процес перетворення звичайного тексту (відкритого тексту) на зашифрований текст (криптотекст), який виглядає як набір випадкових символів. Це досягається за допомогою спеціальних алгоритмів (методів шифрування) та ключів [16].

Алгоритм шифрування — це набір математичних правил, які визначають, як саме відкритий текст буде перетворено на криптотекст. Існує безліч різних алгоритмів шифрування, кожен зі своїми особливостями та рівнем безпеки.

Можемо виділити наступні переваги шифрування електронних книг [17]:

- *Конфіденційність.* забезпечує, що лише авторизовані особи можуть отримати доступ до вмісту книги. Це особливо важливо для документів, що містять приватну, комерційну або іншу чутливу інформацію.
- *Захист авторських прав.* може ускладнити несанкціоноване копіювання та розповсюдження книг, хоча це не є абсолютною гарантією від піратства.
- *Контроль доступу.* дозволяє авторам або власникам книг контролювати, хто і за яких умов може переглядати або редагувати їхні твори.
- *Безпека передачі даних.* при передачі зашифрованих файлів через інтернет або інші канали зв'язку ризик того, що їх зможуть прочитати сторонні особи, значно знижується.

Звісно, як і будь-яка технологія, шифрування має свої недоліки, а деякі аспекти його функціонування можуть викликати занепокоєння щодо довгострокової безпеки.

Недоліки шифрування [18] :

- **Залежність від надійності пароля (або ключа).** Як вже згадувалося, якщо пароль слабкий, його можуть підібрати або зламати за допомогою різних методів (наприклад, brute-force атаки, словникові атаки). Також, якщо ключ шифрування буде скомпрометовано, вся зашифрована інформація стане доступною зловмисникам.
- **Проблема втрати пароля.** Якщо користувач забуде пароль, відновлення доступу до зашифрованих даних може бути вкрай складним або навіть неможливим. Для особистих файлів це може призвести до втрати важливої інформації.



- **Ризик «бекдорів» та вразливостей в алгоритмах.** Теоретично, в алгоритмах шифрування можуть існувати невідомі вразливості («баги»), які з часом можуть бути виявлені та використані для злому. Також існує занепокоєння щодо можливого навмисного вбудовування «бекдорів» (прихованих способів обходу захисту) в деякі алгоритми або програмне забезпечення. Хоча широко використовувані та ретельно перевірені алгоритми, такі як AES, наразі вважаються стійкими, майбутні відкриття не виключені.
- **Обмежена ефективність проти певних видів атак.** Шифрування захищає дані від несанкціонованого доступу під час зберігання або передачі. Однак воно не може запобігти атакам, спрямованим на отримання доступу до даних у момент їх використання (наприклад, шляхом перехоплення даних з пам'яті комп'ютера або використання шкідливого програмного забезпечення, яке реєструє натискання клавіш).
- **Потреба в обчислювальних ресурсах.** Процеси шифрування та дешифрування можуть вимагати значних обчислювальних ресурсів, особливо при роботі з великими обсягами даних. Це може впливати на продуктивність пристроїв, особливо на слабких або застарілих.
- **Складність управління ключами.** У складних системах з великою кількістю зашифрованих даних управління ключами (їх генерація, зберігання, розподіл, відкликання) може бути складною задачею і створювати додаткові ризики безпеки, якщо ключі зберігаються неналежним чином.

Водяні знаки (watermarking) — це технологія захисту цифрового контенту, яка полягає у вбудовуванні в нього прихованих міток, що не помітні для пересічного користувача, але дозволяють у разі витоку відстежити джерело поширення. На відміну від DRM, водяні знаки не обмежують доступ або використання контенту, а радше діють як «невидимий підпис» або слід, який залишається з файлом навіть після копіювання, перетворення в інший формат або легкого редагування файлу [19].

Впровадження водяного знаку не впливає на зовнішній вигляд або функціональність контенту для кінцевого користувача, що робить цю технологію менш нав'язливою та більш зручною у використанні порівняно з DRM. Водночас, якщо контент розповсюджується нелегально, водяний знак дозволяє ідентифікувати джерело витоку — наприклад, конкретний обліковий запис або пристрій. Саме тому водяні знаки широко застосовуються у корпоративному секторі, видавничій справі, тестуванні нових матеріалів та при передрелізному доступі до контенту. Головна перевага водяних знаків полягає у тому, що вони не створюють бар'єрів для легальних користувачів і не погіршують їхній досвід, а натомість фокусуються на відповідальності користувачів, які отримали доступ до контенту, адже у разі витоку їх можна ідентифікувати. У сфері цифрової безпеки водяні знаки вважаються більш етичною та ефективною альтернативою DRM, оскільки не порушують конфіденційність і не обмежують особисте використання, але при цьому допомагають боротися з нелегальним розповсюдженням на рівні джерел, а не загалом користувачів [20].

Активация через сервер (online activation) — це процес, при якому програма для читання електронних книг під час першого відкриття файлу встановлює з'єднання з сервером активації видавця або платформи. Під час цього з'єднання передається інформація про покупку, обліковий запис користувача та ідентифікатор пристрою, що дозволяє перевірити легітимність доступу до контенту. Якщо з'єднання заблоковане (наприклад, через брандмауер або антивірус), активація може не відбутися, що призведе до помилок у доступі до книги. Для вирішення таких проблем рекомендується



налаштувати брандмауер або антивірус так, щоб вони дозволяли з'єднання з сервером активації [21].

Стосовно електронних книг це працює *наступним чином* [22]:

1. **Придбання:** Користувач купує електронну книгу через онлайн-магазин (наприклад, Amazon Kindle Store, Google Play Books, Apple Books).
2. **Завантаження:** Книга завантажується на пристрій користувача (рідер, планшет, смартфон, комп'ютер) у певному форматі (часто EPUB або власний формат магазину).
3. **Активация (перша спроба відкриття):** При першій спробі відкрити книгу програма для читання (наприклад, додаток Kindle, Google Play Books, Apple Books) може вимагати підключення до інтернету.
4. **Перевірка ліцензії:** Програма зв'язується із сервером магазину, передаючи інформацію про покупку (наприклад, обліковий запис користувача, ідентифікатор пристрою).
5. **Підтвердження:** Сервер перевіряє, чи дійсно користувач придбав цю книгу і чи не перевищено ліміт пристроїв, на яких її можна використовувати.
6. **Доступ:** У разі успішної перевірки користувачеві надається доступ до вмісту книги.

Переваги онлайн-активації для електронних книг [23]:

- **Захист авторських прав** ускладнює несанкціоноване копіювання та розповсюдження електронних книг, прив'язуючи покупку до облікового запису та/або пристрою.
- **Керування ліцензіями** дозволяє постачальникам контролювати кількість пристроїв, на яких може бути відкрита книга.
- **Можливість відкликання доступу.** У разі виявлення порушень авторських прав або інших проблем постачальник може відкликати доступ до книги.
- **Зручність для покупців (в певних межах).** Після одноразової активації книга зазвичай доступна для читання в офлайн-режимі на авторизованих пристроях.

Недоліки онлайн-активації для електронних книг:

- **Залежність від інтернету.** Для першого відкриття книги та іноді для періодичної перевірки ліцензії потрібне інтернет-з'єднання.
- **Проблеми при зміні пристроїв.** Перенесення книги на новий пристрій може вимагати повторної активації і може бути обмежено кількістю дозволених пристроїв.
- **Ризик втрати доступу.** Якщо магазин припинить роботу або змінить політику, користувачі можуть втратити доступ до своїх придбаних книг.
- **Обмеження прав користувачів.** Обмежує можливість вільно розпоряджатися придбаною книгою (наприклад, дарувати, передавати у спадок).
- **Незручність.** Процес активації може бути незручним, особливо при першому знайомстві з платформою або при виникненні технічних проблем.

Щоб краще зрозуміти, чому питання зручності активації та доступу до цифрового контенту є настільки важливим, варто згадати один із найвідоміших випадків, який наочно продемонстрував недоліки онлайн-активації та контролю з боку платформи. Йдеться про інцидент із Amazon Kindle [24], коли компанія без попередження видалила у користувачів придбані електронні книги, зокрема твори Джорджа Орвелла, що



викликало широкий резонанс і підкреслило вразливість користувачів у подібних ситуаціях.

У 2009 році Amazon віддалено видалив копії книг Джорджа Орвелла «1984» та «Колгосп тварин» зі своїх пристроїв Kindle користувачів, які їх законно придбали. Це сталося через суперечку щодо авторських прав з видавцем.

Дану неефективність можна пояснити наступним чином:

- **Законні покупки постраждали** — користувачі, які заплатили за книги, втратили до них доступ без попередження та без їхньої згоди. Це підірвало їхнє право власності на придбаний контент.
- **Обхід захисту не допоміг** — онлайн-активація та DRM, які мали б захищати авторські права, не змогли запобігти видаленню контенту з пристроїв користувачів. Фактично, вони дали Amazon централізований контроль над контентом навіть після його продажу.
- **Піратство залишається невідкладним** — люди, які б захотіли отримати ці книги нелегально, могли б легко знайти їхні копії в інтернеті без будь-яких обмежень DRM.

Цей випадок викликав великий скандал та обурення серед користувачів, підкресливши недоліки системи, де онлайн-активація та DRM дають постачальнику надмірний контроль над придбаним контентом на шкоду споживачам. Він показав, що замість ефективної боротьби з піратством ці методи можуть призвести до втрати законно придбаного контенту через рішення постачальника [25].

Обфускація коду — це метод ускладнення структури програмного коду з метою унеможливлення або значного ускладнення зворотної інженерії, при цьому функціональність програми залишається незмінною. Суть полягає в тому, щоб зробити вихідний код важким для розуміння та аналізу, застосовуючи різноманітні техніки, які ускладнюють дослідження внутрішньої логіки, алгоритмів і потенційних вразливостей. Важливо пам'ятати, що жоден технічний захід не є абсолютно надійним, оскільки зловмисники постійно шукають способи обходу захисту. Тому для ефективного захисту часто використовують поєднання кількох методів і постійно вдосконалюють [26].

Основні методи обфускації коду:

- **Перейменування ідентифікаторів.** Змінюються імена змінних, функцій, класів на короткі, беззмістовні або навіть оманливі послідовності символів. Це ускладнює розуміння призначення різних частин коду. Наприклад, змінна `userPassword` може бути перейменована на `aBcD12`.
- **Видалення зайвої інформації.** З коду видаляються коментарі, налагоджувальна інформація, невикористані змінні та функції, що робить його більш компактним та менш зрозумілим.
- **Зміна структури коду.** Складні логічні блоки можуть бути розбиті на менші, перемішані або переписані з використанням менш очевидних конструкцій (наприклад, використання умовних операторів замість циклів або навпаки).
- **Вставка «мертвого» коду.** До коду додаються фрагменти, які ніколи не виконуються, але ускладнюють його аналіз та розуміння справжньої логіки.
- **Шифрування рядків та інших констант.** Текстові рядки, ключі, URL-адреси та інші важливі константи можуть бути зашифровані та розшифровуватися лише під час виконання програми.
- **Використання віртуальних машин.** Частина коду може виконуватися у віртуальній машині зі складною для аналізу архітектурою.



- **Контроль потоку виконання.** Порядок виконання коду може бути штучно ускладнений за допомогою різних технік, таких як «спагетті-код» (надмірне використання операторів переходу goto) або складні системи умовних переходів.

Хоча обфускація традиційно застосовується для захисту виконуваного коду програм, її принципи можуть бути використані і для ускладнення аналізу деяких форматів електронних книг [27], особливо якщо вони включають інтерактивні елементи, сценарії (наприклад, JavaScript у веб-сторінках або EPUB) або є частиною спеціалізованого програмного забезпечення для читання.

Наприклад, якщо електронна книга є веб-додатком, її JavaScript-код може бути обфускований, щоб ускладнити розуміння логіки відображення контенту або перевірки ліцензії.

Переваги обфускації: ускладнення зворотної інженерії; захист інтелектуальної власності; ускладнення пошуку вразливостей;

Недоліки обфускації: може впливати на продуктивність; ускладнює налагодження та підтримку; може бути неефективним проти досвідчених зловмисників;

Підтвердження **неефективності обфускації** [28]:

В екосистемі Android дуже поширене використання обфускації коду (через такі інструменти, як ProGuard або DexGuard) для захисту додатків від зворотної інженерії та несанкціонованого копіювання. Проте, незважаючи на це, регулярно з'являються модифіковані (зламани) версії платних додатків, які безкоштовно розповсюджуються в інтернеті. Якщо електронні книги розповсюджуються через спеціалізовані мобільні додатки (що є поширеною практикою), і ці додатки для захисту від копіювання використовують лише обфускацію коду (без надійного DRM на рівні файлів або онлайн-активації), то зловмисники можуть зламати додаток, обійти перевірку ліцензії та отримати доступ до вмісту книг без необхідності їх купувати.

Отож дослідивши наведені вище технічні методи захисту електронних книг, ми дійшли висновку, що вони не забезпечують максимального захисту та ефективності. Тому пропонуємо новий інноваційний спосіб запобігання піратству та захисту авторських прав електронних книг.

Пропонований нами метод захисту електронних книг базується на поєднанні динамічного цифрового підпису та блокчейн-технологій, що забезпечує високий рівень безпеки, прозорості та незмінності даних. Суть методу полягає в тому, що під час отримання електронної книги кожен користувач отримує унікальну зашифровану копію. Цифровий підпис формується на основі хешу контенту книги, ідентифікатора користувача та мітки часу, що гарантує цілісність та автентичність даних. Згенерований підпис разом із контрольним хешем книги записується у блокчейн — децентралізований реєстр, який забезпечує незмінність і доступність цих даних для подальшої перевірки.

Під час відкриття книги спеціальне програмне забезпечення автоматично звіряє цифровий підпис із даними, записаними в блокчейні. У разі збігу підтверджується автентичність книги та відсутність несанкціонованих змін. Для виявлення джерел можливого нелегального поширення у цифровий підпис інтегруються приховані ідентифікатори (водяні знаки), які дозволяють ідентифікувати конкретну копію без розкриття персональних даних користувача. Такий підхід дає змогу ефективно виявляти витoki контенту, не порушуючи конфіденційності.

Технічно метод використовує сучасні криптографічні алгоритми, зокрема RSA або ECDSA, для створення цифрових підписів, а також блокчейн як надійний реєстр транзакцій, стійкий до змін та підробок завдяки механізмам розподіленого консенсусу та



доказів роботи. Система блокчейну забезпечує стійкість до збоїв і атак, адже будь-яка спроба змінити запис вимагатиме колосальних обчислювальних ресурсів, що робить підробку фактично неможливою.

Серед основних переваг даного методу варто відзначити неможливість підробки або зміни електронних книг без втрати їхньої легітимності, високу прозорість і довіру між авторами, видавцями та користувачами, а також ефективний захист від витоків завдяки можливості ідентифікувати джерело незаконного розповсюдження. Крім того, автоматизація процесів перевірки через інтеграцію із додатками-читалками та використання смарт-контрактів спрощує управління ліцензіями та підвищує зручність для кінцевих користувачів.

Однак метод має і певні обмеження. Впровадження та підтримка блокчейн-рішень і криптографічних протоколів вимагають значних технічних і фінансових ресурсів, що може стати серйозною перешкодою для масового застосування, особливо для невеликих видавництв чи окремих авторів. Крім того, існують ризики обходу захисту, наприклад, шляхом копіювання контенту у нові файли або використання спеціалізованого програмного забезпечення для зняття захисту. Також не всі пристрої та платформи підтримують складні криптографічні механізми, що може обмежити доступність контенту для широкого кола користувачів.

Прикладом реального впровадження подібних ідей є стартап Po.et [29], який у 2018 році запропонував платформу для реєстрації цифрового контенту з використанням блокчейн-технологій для захисту авторських прав на тексти та книги. Подібні концепції сьогодні також активно розвиваються у сфері NFT та електронної дистрибуції цифрового контенту.

Ефективність інноваційного методу базується на кількох ключових факторах. По-перше, блокчейн забезпечує децентралізовану, незмінну та прозору систему зберігання даних, що унеможливорює підробку чи несанкціоновану зміну інформації. Цифрові підписи, записані в блокчейні, захищені криптографічними алгоритмами, що гарантує цілісність електронних книг. По-друге, використання унікальних ідентифікаторів користувачів і міток часу дозволяє підтвердити легітимність копії книги та виявити джерела незаконного поширення без порушення конфіденційності. По-третє, автоматизація перевірок за допомогою смарт-контрактів і інтеграція із додатками для читання електронних книг підвищують ефективність системи та рівень довіри на ринку.

Також варто зазначити, що ефективність методу значною мірою залежить від якості технічної реалізації та доступності для кінцевих користувачів. Впровадження блокчейн-рішень потребує значних ресурсів, а складність криптографічних протоколів може зменшувати сумісність із різними пристроями. Соціально-економічні чинники, зокрема висока вартість легальних електронних книг та низький рівень обізнаності користувачів щодо авторських прав, також можуть негативно впливати на загальний рівень захисту.

Проте, незважаючи на ці певні недоліки, інноваційний метод захисту електронних книг на основі динамічного цифрового підпису та блокчейн-технологій є перспективним і ефективним інструментом для забезпечення безпеки, прозорості та довіри у сфері цифрової дистрибуції. Його впровадження дозволяє суттєво знизити ризики підробки та нелегального поширення контенту. Проте для досягнення максимальної ефективності необхідно поєднувати технічні рішення з інформаційно-просвітницькою діяльністю, спрямованою на підвищення обізнаності користувачів щодо авторських прав, а також розвивати доступні моделі ціноутворення, які зроблять легальні електронні книги більш привабливими для широкої аудиторії. Лише комплексний підхід, що об'єднує технічні, економічні та освітні



заходи, дозволить суттєво зменшити рівень порушень авторських прав у цифровому середовищі та сприятиме сталому розвитку ринку електронної дистрибуції.

Хоча запропонований метод динамічного цифрового підпису на основі блокчейн-технологій має значні переваги, жоден технічний засіб захисту не можна вважати абсолютно ефективним. З результатів опитувань користувачів видно, що однією з основних причин порушення авторських прав є не тільки технічна доступність піратських копій, а й соціально-економічні чинники.

Однією з головних проблем є висока вартість легальних електронних книг, що часто спонукає користувачів шукати безкоштовні або нелегальні альтернативи. Водночас багато споживачів не мають достатньої обізнаності про суть авторських прав, наслідки їх порушення та вплив таких дій на авторів і видавців. Відсутність розуміння правових аспектів сприяє поширенню нелегального контенту.

Також існують технічні бар'єри, що впливають на ефективність захисту. Складність використання захисних технологій, обмеження сумісності із деякими пристроями чи безкоштовним програмним забезпеченням можуть знижувати комфорт користування легальним контентом і підштовхувати споживачів до обходу захисту.

Нижче наведена порівняльна таблиця (табл. 3) основних методів захисту з урахуванням ключових критеріїв.

Таблиця 3

Порівняння основних методів захисту електронних книг

Критерій	Електронний підпис	Блокчейн	DRM	Водяні знаки	Контроль доступу	Інноваційний метод (підпис + блокчейн)
Ідентифікація користувача	Так	Ні	Так	Ні	Так	Так (на основі підпису)
Прозорість транзакцій	Ні	Так	Ні	Ні	Частково	Так
Захист від підробки	Частково	Так	Ні	Ні	Ні	Так
Простеження витоку	Обмежена	Частково	Ні	Так	Ні	Так (по ланцюгу підписів)
Незмінність записів	Ні	Так	Ні	Ні	Ні	Так (через блокчейн)
Автоматична валідація	Так	Ні	Частково	Ні	Ні	Так
Захист у відкритому середовищі	Ні	Частково	Ні	Ні	Частково	Так
Масштабованість	Обмежена	Так	Обмежено	Так	Ні	Так
Стійкість до злоумисників	Частково	Так	Ні	Ні	Частково	Так
Складність реалізації	Низька	Середня	Висока	Низька	Середня	Вища (але виправдана)

Підсумовуючи варто зазначити, що лише інтеграція технічних, економічних та освітніх заходів дозволить суттєво знизити рівень порушень авторських прав у цифровому середовищі та забезпечити сталий розвиток ринку електронної дистрибуції.



ВИСНОВКИ

На основі проведеного аналізу можна зробити кілька ключових висновків. По-перше, проблема піратства електронних книг залишається актуальною через легкість копіювання та розповсюдження цифрового контенту, що завдає значних збитків авторам і видавцям. По-друге, існуючі технічні засоби захисту, такі як DRM, шифрування, водяні знаки та онлайн-активація, мають як переваги, так і недоліки: вони підвищують рівень захисту, але можуть ускладнювати доступ для легальних користувачів і не гарантують абсолютної безпеки. По-третє, результати опитування свідчать, що більшість користувачів все ще віддають перевагу безкоштовним джерелам, а основними причинами піратства є висока вартість легального контенту та обмежена доступність книг. По-четверте, для ефективної боротьби з піратством необхідно поєднувати технічні, правові, економічні та освітні заходи, а не покладатися лише на технології. Запропонований нами метод захисту електронних книг, що базується на поєднанні динамічного цифрового підпису та блокчейн-технологій забезпечує високий рівень безпеки, прозорості та незмінності даних та дозволяє здійснювати ефективний контроль за розповсюдженням електронних книг. Комплексний підхід забезпечить баланс між захистом прав авторів і доступністю знань для суспільства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. On Copyright and Related Rights, Law of Ukraine No. 3792-XII (2023) (Ukraine). <https://zakon.rada.gov.ua/laws/show/3792-12#Text>
2. Civil Code of Ukraine, Code of Ukraine No. 435-IV (2025) (Ukraine). <https://zakon.rada.gov.ua/laws/show/435-15#Text>
3. Melnyk, I. V. (2022). Protection of Copyright in the Digital Environment. *Information Law of Ukraine*, 2, 45–52.
4. Khoina, A. (n. d.). *Copyright Agreement*. https://essuir.sumdu.edu.ua/bitstream-download/123456789/92570/1/Khoina_copyright_agreement.pdf
5. *Copyright: Collection of Scientific Papers*. (n. d.). <http://baltijapublishing.lv/omp/index.php/bp/catalog/download/223/5968/12487-1?inline=1>
6. *Monolith Law. Protection of Copyright Abroad*. (n. d.). <https://monolith.law/uk/general-corporate/overseas-copyright>
7. Hugenholtz, P. B. (2020). The Copyright Wars – Seen from the Netherlands. *Journal of Intellectual Property Law & Practice*, 15(2), 85–87. <https://doi.org/10.1093/jiplp/jpaa004>
8. *Ukrainian Agency for Copyright and Related Rights*. (n. d.). <https://uacrr.org.ua/about-us.html>
9. Pakhomova, I. I. (2023). Technical Means of Protecting E-books from Copying. *Bulletin of the National University "Lviv Polytechnic"*, 894, 112–117.
10. Kozlov, V. A. (2021). DRM Technologies: Current State and Development Prospects. *Information Security*, 3, 34–38.
11. Sydorenko, O. V. (2020). Anti-Piracy Methods in the Field of Digital Content. *Legal Ukraine*, 5, 67–72.
12. *Digital Rights Management (DRM) Explained*. (2023). Electronic Frontier Foundation.
13. *DRM and E-books: How Digital Rights Management Works*. (2024). HowStuffWorks.
14. *Data Encryption: Principles, Algorithms, Applications*. (2023). *IT Security Journal*, 9.
15. *Kindle to Discontinue USB Download Option for Books*. (2025). Good e-Reader.
16. *Encryption in eBooks: How It Works and Why It Matters*. (2024). EpubSecrets.
17. *Advantages and Disadvantages of Encryption for eBooks*. (2023). Cybersecurity Magazine.
18. *Risks of Weak Encryption in Digital Publishing*. (2022). InfoSec Today.
19. *Watermarking Techniques for Digital Content Protection*. (2021). Springer.
20. *Watermarks in Publishing: Current State and Prospects*. (2023). *Publishing Affairs*, 4, 99–104.
21. *Online Activation and License Management for eBooks*. (2024). BookNet Canada.
22. *How eBook Activation Works on Major Platforms*. (2024). The Digital Reader.
23. *Pros and Cons of Online Activation for Digital Books*. (2023). Publishing Perspectives.



24. *Kindle Ownership Controversy*. (2010). TechCrunch. <https://techcrunch.com/2010/02/25/amazon-kindle-ownership-controversy/>
25. *Amazon Deletes Orwell Books from Kindle*. (2009). The New York Times.
26. *DRM Use in Ukrainian Law*. (n. d.). <https://ir.kneu.edu.ua/server/api/core/bitstreams/ffd51b6b-0084-4bbc-bfe4-4273f8ad4fce/content>
27. *What is Blockchain and How Does It Work*. (n. d.). Zfort Group. <https://www.zfort.com.ua/blog/sho-take-blokchein-yak-vin-pracyuye>
28. *Copyright Law in Ukraine*. (n. d.). BukLib.net. <https://buklib.net/books/26254/>
29. *Legal IT Group. Blog on IT Law*. (n. d.). <https://legalitgroup.com/blog-z-it-prava/>

**Iryna Feshchak**

Student of the Department of Information Protection
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0009-0008-6827-1049
iryna.feshchak.kb.2023@lpnu.ua

Solomiia Onofriichuk

Student of the Department of Information Protection
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0009-0004-7047-2828
solomiia.onofriichuk.kb.2023@lpnu.ua

Oleh Harasymchuk

Ph.D., Associate Professor at the Department of Information Protection,
Lviv Polytechnic National University, Lviv, Ukraine
ORCID ID: 0000-0002-8742-8872
oleh.i.harasymchuk@lpnu.ua

TECHNICAL MEANS OF COPYRIGHT PROTECTION AS TOOLS TO COMBAT E-BOOK PIRACY

Abstract. With the development of digital technologies, the issue of copyright protection is becoming increasingly relevant, especially in the field of electronic books. This is due to the relentless growth of content, the convenience of distribution via the Internet, and technological capabilities for copying without quality loss. Consequently, there is a need to develop effective means of protecting copyright. The article discusses the main aspects of copyright protection, including legal foundations, technical methods to combat piracy, and their effectiveness. In particular, it analyzes the current situation regarding user assessments of existing protection systems and their attitudes toward piracy, which remains one of the main obstacles to the development of the electronic book market. Special attention is given to the study of technical methods such as DRM, encryption, watermarks, online activation, and code obfuscation, along with their advantages and disadvantages. For example, DRM can restrict legitimate use of content, provoking negative reactions from users, whereas watermarks allow identification of the original source without loss of quality or content. The article notes that no single method provides full guarantees of protection, which necessitates a comprehensive approach. Based on the analysis of existing problems, an innovative method of protecting electronic books is proposed, based on the combination of a dynamic digital signature and blockchain technology. The dynamic signature allows changing authorization data depending on the user, while blockchain ensures tamper-proof records and traceability of all operations related to the content. The article also discusses challenges and limitations associated with implementing new protection methods and emphasizes the importance of a comprehensive approach that combines technical, economic, and educational measures for effective fight against piracy in the digital environment. The piracy problem cannot be solved solely through technical means — effective cooperation between rights holders, technology developers, and users is essential. Only through joint efforts at national and international levels can sustainable and effective copyright protection in the digital age be achieved.

Keywords: copyright; e-books; piracy; digital protection; DRM (Digital Rights Management); watermarking; encryption; online activation; code obfuscation; blockchain; digital signature; content protection.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. On Copyright and Related Rights, Law of Ukraine No. 3792-XII (2023) (Ukraine). <https://zakon.rada.gov.ua/laws/show/3792-12#Text>
2. Civil Code of Ukraine, Code of Ukraine No. 435-IV (2025) (Ukraine). <https://zakon.rada.gov.ua/laws/show/435-15#Text>



3. Melnyk, I. V. (2022). Protection of Copyright in the Digital Environment. *Information Law of Ukraine*, 2, 45–52.
4. Khoina, A. (n. d.). *Copyright Agreement*. https://essuir.sumdu.edu.ua/bitstream-download/123456789/92570/1/Khoina_copyright_agreement.pdf
5. Copyright: Collection of Scientific Papers. (n. d.). <http://baltijapublishing.lv/omp/index.php/bp/catalog/download/223/5968/12487-1?inline=1>
6. Monolith Law. *Protection of Copyright Abroad*. (n. d.). <https://monolith.law/uk/general-corporate/overseas-copyright>
7. Hugenholtz, P. B. (2020). The Copyright Wars – Seen from the Netherlands. *Journal of Intellectual Property Law & Practice*, 15(2), 85–87. <https://doi.org/10.1093/jiplp/jpaa004>
8. Ukrainian Agency for Copyright and Related Rights. (n. d.). <https://uacrr.org.ua/about-us.html>
9. Pakhomova, I. I. (2023). Technical Means of Protecting E-books from Copying. *Bulletin of the National University “Lviv Polytechnic”*, 894, 112–117.
10. Kozlov, V. A. (2021). DRM Technologies: Current State and Development Prospects. *Information Security*, 3, 34–38.
11. Sydorenko, O. V. (2020). Anti-Piracy Methods in the Field of Digital Content. *Legal Ukraine*, 5, 67–72.
12. *Digital Rights Management (DRM) Explained*. (2023). Electronic Frontier Foundation.
13. *DRM and E-books: How Digital Rights Management Works*. (2024). HowStuffWorks.
14. Data Encryption: Principles, Algorithms, Applications. (2023). *IT Security Journal*, 9.
15. *Kindle to Discontinue USB Download Option for Books*. (2025). Good e-Reader.
16. *Encryption in eBooks: How It Works and Why It Matters*. (2024). EpubSecrets.
17. *Advantages and Disadvantages of Encryption for eBooks*. (2023). Cybersecurity Magazine.
18. *Risks of Weak Encryption in Digital Publishing*. (2022). InfoSec Today.
19. *Watermarking Techniques for Digital Content Protection*. (2021). Springer.
20. Watermarks in Publishing: Current State and Prospects. (2023). *Publishing Affairs*, 4, 99–104.
21. *Online Activation and License Management for eBooks*. (2024). BookNet Canada.
22. *How eBook Activation Works on Major Platforms*. (2024). The Digital Reader.
23. *Pros and Cons of Online Activation for Digital Books*. (2023). Publishing Perspectives.
24. *Kindle Ownership Controversy*. (2010). TechCrunch. <https://techcrunch.com/2010/02/25/amazon-kindle-ownership-controversy/>
25. *Amazon Deletes Orwell Books from Kindle*. (2009). The New York Times.
26. *DRM Use in Ukrainian Law*. (n. d.). <https://ir.kneu.edu.ua/server/api/core/bitstreams/ffd51b6b-0084-4bbc-bfe4-4273f8ad4fce/content>
27. *What is Blockchain and How Does It Work*. (n. d.). Zfort Group. <https://www.zfort.com.ua/blog/sho-take-blokchein-yak-vin-pracyuye>
28. *Copyright Law in Ukraine*. (n. d.). BukLib.net. <https://buklib.net/books/26254/>
29. *Legal IT Group. Blog on IT Law*. (n. d.). <https://legalitgroup.com/blog-z-it-prava/>

