https://doi.org/10.31891/2219-9365-2025-83-5
УДК 004.056.55 (043.3)

САБАТ Володимир
Національний університет «Львівська політехніка»
https://orcid.org/0000-0001-8130-7837
e-mail: volodymyr.i.sabat@lpnu.ua
БОГОНІС Олександр
Національний університет «Львівська політехніка»
https://orcid.org/0009-0005-1341-6245
e-mail: oleksandr.o.bohonis@lpnu.ua

ОЦІКА РИЗИКІВ ЗБОЮ СИСТЕМИ ЗАХИСТУ АВТОРСЬКИХ ПРАВ ПІД ВПЛИВОМ ЗОВНІШНІХ НЕГАТИВНИХ ФАКТОРІВ

Функціонування системи захисту авторських прав для електронних видань тісно пов'язане із зовнішніми негативними факторами впливу, що можна представити у вигляді атак на вразливі параметри таких видань до яких насамперед можна віднести конфіденційність, модифікацію, доступність та ідентичність інформації, яка міститься у виданнях. Визначення авторства видання в системі захисту авторських прав може бути вирішено методом впровадження у них цифрових водяних знаків або за допомогою криптографічних алгоритмів, які з точністтю вказують на наявність у виданні авторських прав (цифровий підпис). Проте ще недостатньо розроблені методи моніторингу електронної продукції на ринку електронних видань на предмет легальності їхнього розповсюдження та недосліджені типи атак, які можуть вплинути на роботу системи захисту авторських прав. Тому метою дослідження у цій статті є аналіз атак на систему захисту авторських прав і визначення рівня безпеки для захисту електронних видань, який тісно пов'язаний із рівнем ризику виникнення атаки на електронне видання. Для вирішення задач, поставлених у меті дослідження, необхідно визначити найбільш критичні атаки на систему захисту авторських прав для електронного видання, ввести поняття ризику, вразливості, загрози і контролюючих засобів протидії загрозам. В статті проаналізовані сучасні засоби впровадження цифрових водяних знаків, їхні недоліки і переваги щодо протистояння зовнішнім атакам, введена шкала оцінювання основних параметрів, які визначають рівень ризику, що дозволяє нормалізувати рівень ризику у числових значеннях та в подальшому вдосконалювати систему захисту, за допомогою внесення тих чи інших засобів протидії атакам. Таким чином система захисту авторських прав на електронні видання може бути актуальною у кризових умовах впливу зовнішніх факторів атак та загроз на електронне видання і здатною адаптовуватись під такі зовнішні фактори. Це, в свою чергу, дозволяє контролювати необхідний оптимальний рівень безпеки для нормалізації функціонування системи моніторингу розповсюдження нелегальних видань та системи захисту авторських прав в цілому.

Ключові слова: авторське право, система захисту авторських прав, електронні вмдання, ризик, вразливість, загроза, контролюючі засоби захисту.

SABAT Volodymyr, BOHONIS Oleksandr
Lviv Polytechnic National University

FORMAL METHODS FOR DESCRIBING AND DETERMINING THE PARAMETERS OF COPYRIGHT PROTECTION SYSTEMS

The functioning of the copyright protection system for electronic publications is closely connected with external negative influencing factors, which can be represented as attacks on vulnerable parameters of such publications, which primarily include confidentiality, modification, availability, and identity of the information contained in the publications. The determination of authorship of a publication in the copyright protection system can be solved by the method of embedding digital watermarks into them or by means of cryptographic algorithms, which accurately indicate the presence of copyright in the publication (digital signature). However, the methods of monitoring electronic products in the electronic publications market for the legality of their distribution are still insufficiently developed, and the types of attacks that can affect the functioning of the copyright protection system remain unexplored. Therefore, the purpose of the research in this article is the analysis of attacks on the copyright protection system and the determination of the security level for protecting electronic publications, which is closely connected with the level of risk of an attack on an electronic publication. To solve the tasks set in the research objective, it is necessary to determine the most critical attacks on the copyright protection system for electronic publications, to introduce the concepts of risk, vulnerability, threat, and controlling countermeasures. The article analyzes modern means of embedding digital watermarks, their shortcomings and advantages in countering external attacks, introduces a scale for evaluating the main parameters that determine the risk level, which makes it possible to normalize the risk level in numerical values and further improve the protection system by introducing certain countermeasures against attacks. Thus, the copyright protection system for electronic publications may be relevant under crisis conditions of external factors of attacks and threats on an electronic publication and capable of adapting to such external factors. This, in turn, makes it possible to control the necessary optimal level of security for the normalization of the functioning of the monitoring system of illegal publication distribution and the copyright protection system as a whole.

Keywords: copyright, copyright protection system, electronic publications, risk, vulnerability, threat, controlling protection tools.

Стаття надійшла до редакції / Received 22.07.2025
Прийнята до друку / Accepted 24.08.2025

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Системи захисту авторських прав на електронні видання сьогодні потребують кардинальних вдосконалень, оскільки електронні видання, на відміну від паперових, все-більше починають заповнювати інформаційний мережний простір і як для автора цих видань так і для видавництва стає актуальною проблема їх ідентифікації і протидії незаконному нелегальному поширенню таких видань. Дослідження, які проводились у сфері захисту електронних видань, протидії атакам на їх індентичність і загрозам, пов'язаним з порушенням авторських прав, завжди є актуальними і з кожним днем зростатимуть. В цьому плані існує багато наукових публікацій і робіт, присвячених нормалізації авторського права і дотримання прав на інтелектуальну власність. Серед них необхідно насамперед зазначити вітчизняні законодавчі акти та інші напрацювання з метою запобігання таким негативним факторам [1,2]. Якщо електронні видання містять в собі растрові зображення (твори мистецтва, цифрові фотозображення, растрові рисунки тощо), то зазвичай розглядають методи та засоби ідентифікації та захисту растрових зображень. До таких досліджень можна віднести праці [3,4]. Відповідно до методів захисту таких зображень найкраще підходять стеганографія та криптографічні алгоритми захисту, що доведено у наукових дослідженнях [5, 6]. Захист авторських прав для цінних документів з формуванням графічних засобів захисту розглянуто у монографії [7]. У монографії [8] аналізуються методи захисту векторних зображень за допомогою впровадження в них цифрових водяних знаків. Методи оцінки ризику виникнення атак в технологічних процесах на поліграфічному виробництві запропоновані у праці [9]. Методи захисту електронних документів в системах документообігу для виробничих структур наведені у статті [10]. Але надалі актуальною проблемою є розпізнавання та протидія атакам на порушення авторських прав використання електронних видань та оцінка рівня ризику виникнення таких атак.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Визначення атак на систему захисту авторських прав електронних видань

Система захисту автрських (*ZAP*) прав з використанням методу впровадження *ЦВЗ* в цифрове інформаційне середовище потребує періодичної модифікації і виявлення вразливостей та загроз, які можуть виникнути внаслідок функціонування системи під дією негативних зовнішніх та внутрішніх факторів, що можуть призвести до збитків роботи системи, або до доступу зловмисників до алгоритмів впровадження *ЦВЗ* в *ЦІС*, що поставить роботу такої системи недоцільною.

Введемо поняття атаки на *ZAP*.

Означення 1. Під **атакою** на систему захисту авторських прав (A_{ZAP}) будемо розуміти усі негативні події, які призводять до збою функціонування системи, несанкціонованому доступу до алгоритмів впровадження *ЦВЗ* в *ЦІС* та нелегальної модифікації авторського твору з впровадженим у нього *ЦВЗ*.

Треба розуміти що усі негативні події пов'язані з A_{ZAP} з успішним розвитком атаки можуть призвести до значних збитків роботи системи захисту авторських прав і при отриманні зловмисником доступу до системи захисту роблять цю систему досить вразливою. Тому окрім розроблення самих алгоритмів впровадження ЦВЗ в цифрове інформаційне середовище електронного видання (ЕВ), необхідно також продумати про систему управління доступом до електронних видань. Для санкціонованих користувачів зазвичай розробляються відповідні методи ідентифікації, автентифікації та авторизації у базах даних чи електронних ресурсах, на яких планується впроваджувати *ЕВ* з *ЦВЗ*.

Зловмисник, отримавши доступ до будь-якого електронного видання (EB_i), у певній області їх поширень W_i, зможе здійснити одну із чотирьох атак, пов'язаних із вразливісттю EB_i, а саме:

1. Атака доступу до EB_i, — в результаті такої атаки зловмисник може зчитувати інформацію EB_i, яка є конфіденційною. Позначимо таку атаку $A_d(EB_i)$;

2. Атака модифікації інформації в EB_i, — в результаті атаки зловмисник може модифікувати інформацію, яка міститься в EB_i, або змінити параметри електронного видання, що відповідають за авторське право. Позначимо таку атаку $A_m(EB_i)$;

3. Відмова в обслуговуванні EB_i. В цьому випадку EB_i стає недоступним для користувачів, зазвичай зловмисники його зашифровують і вимагають оплату за дешифрацію документа, або знищують. Такі атаки відносяться до DoS-атак (Denial-of-service), позначимо їх як $A_{dos}(EB_i)$.

4. Відмова від зобов'язань щодо певного EB_i. Ця атака направлена проти можливості ідентифікації інформації в EB_i, іншими словами, це спроба дати невірну інформацію про реальну подію, трансакцію або авторство твору. Позначимо такі атаки як $A_z(EB_i)$.

З вищенаведених атак до атак на систему захисту авторських A_{ZAP} для EB_i можна віднести: атаку на порушення доступу до інформації, а саме $A_d(EB_i)$ і атаку на відмову від зобов'язань $A_z(EB_i)$, або іншими словами на порушення індентичності твору щодо його авторства. Тому в нашому дослідженні будемо аналізувати лише ті дві атаки, що стосуються безпосередньо роботи системи ZAP. Протидія іншим атакам, наприклад, таким, які пов'язані з доступом до інформації належать до служб забезпечення конфіденційності та ідентифікації в системі безпеки, а протидія DoS-атакам належить службі доступності [11].

Якщо провести аналіз системи захисту електронних видань $ZS(EB_i)$ і системи захисту їх авторських прав $ZAP(EB_i)$, то систему ZAP можна віднести до служби, яка забезпечує цілісність інформації та до служби ідентифікації користувачів, яким надається доступ до інформації в системі $ZS(EB_i)$.

Служба забезпечення цілісності стежить за достовірністю інформації в EB_i. При належному рівні організації ця служба дає користувачам впевненість в тому, що інформація є вірною, і її ніхто не змінив. Подібно до служби конфіденційності, служба забезпечення цілісності повинна працювати спільно із службою ідентифікації, щоб здійснювати надійну перевірку достовірності користувачів. Дана служба є «щитом» від атак модифікації.

Одним із засобів захисту електронних видань від атак модифікації та відмову від зобов'язань, окрім цифрового електронного підпису, є впровадження в EB_i цифрового водяного знаку.

Розглянемо поняття ризику, вразливості та загрози, в контексті наших досліджень системи захисту авторських прав.

Оцінка ризику виникнення атак на систему захисту авторських прав

Перед тим як перейти до методів оцінки ризику виникнення атак на систему захисту авторських прав введемо поняття ризику, загрози і вразливості.

Згідно з класичними уявленнями ризик — це основоположна концепція, що формує фундамент того, що ми називаємо «безпекою».

Означення 2. **Ризик** — це вірогідність втрат, яка вимагає захисту.

Для більш точного формулювання поняття ризику необхідно також навести означення основних компонент, з яких складається ризик — загрози та вразливості.

Означення 3. **Загроза** — це дія, або подія здатна порушити безпеку інформаційних систем. Загрози існують як ззовні так і всередині інформаційної системи і чим вищий рівень загроз, тим вищий ризик виникнення на систему атак.

Означення 4. **Вразливість** — це здатність об'єктів, які підлягають захисту протидіяти можливим загрозам. Іншими словами висолка вразливість — це це потенційний шлях для виконання атаки на об'єкт захисту.

З означення 4 випливає, що вразливість — це характерна особливість об'єкта захисту. Якщо він не може протидіяти загрозам виникнення небезпеки, то й зростає ризик здійснення атаки на цей об'єкт. Таким чином можна узагальнити наведені поняття тим, що ризик виникнення атаки R_i на *i*-тий об'єкт захисту формується на основі рівня вразливості цього об'єкта до загроз і рівня загроз, які можуть виникнути щодо об'єкта захисту, тобто:

$$R_i = V_i + Z_i, \tag{1}$$

де V_i — вразливості *i*-того об'єкту захисту відносно загроз на цей об'єкт Z_i.

Атаки на об'єкти захисту, до яких у нашому дослідженні можна віднести електронні видання, що підлягають виконання процедур дотримання авторських прав, здійснюються через загрози порушення цих авторських прав. Якщо нелегальний дилер поширює електронні видання (*ЕВ*), які підлягають захисту авторських прав, або інтелектуальної власності на них, без згоди власника авторських прав чи фірми виробника цього продукту, з якою автор підписав відповідну угоду, то тим самим нелегальний дилер порушує авторські права на *ЕВ*. В результаті таких дій фірма виробник і автор *ЕВ* можуть зазнати значних збитків, отже згідно з означенням 1 такі дії, які порушують авторські права і призводять до збитків називаються атакою.

Для того, щоб зменшити рівень ризику на порушення авторських прав щодо *ЕВ*, необхідно ввести засоби захисту, що зменшують вразливість *ЕВ* відносно існуючих загроз та атак. Це можна здійснити за допомогою таких механізмів: 1) криптографічних засобів, або шифрування *ЕВ*; 2) введенням в *ЕВ* цифрового підпису (*ЦП*), що також є одним із різновидів шифрування; 3) за допомогою стеганографічних засобів впровадження у *ЕВ* цифрового водяного знаку. Методи шифрування та *ЦП* не завжди підходять для масового розповсюдження електронних видань. Зокрема на ринку цифрової продукції для захисту авторських прав у більшості випадків використовують *ЦВЗ* для захисту авторських прав. Тому в нашій роботі розглядатимемо вразливості *ЕВ*, у яких впроваджено *ЦВЗ*.

Для того, щоб оцінити ризик a_{irisk} виникнення атаки A_{ZAP} на EB_i, яка стосується порушення авторських прав, необхідно оцінити рівень захисту EB_i, а саме впровадженого у EB_i цифрового водяного знаку.

Однією із ознак *ЦВЗ* є його скритість для користувача або будь-якої іншої системи моніторингу, окрім системи моніторингу, яка входить у систему захисту авторських прав *ZAP*. Тому розглянемо різні відомі методи впровадження *ЦВЗ* у цифрове середовище і визначемо рівень їхньої стійкості відносно виявлення у них скритого *ЦВЗ*.

З аналізу впровадження *ЦВЗ* у цифрове інформаційне середовище (*ЦІС*) сьогодні відомо два методи впровадження таких водяних знаків: видимі ЦВЗ і невидимі ЦВЗ. Хоча поняття видимого ЦВЗ і суперечить ознаці скритості *ЦВЗ*, але й надалі такі *ЦВЗ* є поширеними. Це насамперед пов'язано через їхню не складність

програмної реалізації і у деяких випадках важкість позбутись таких напівпрозорих водяних знаків, особливо при друці електронних видань. Але з аналізу методів створення таких водяних знаків, наприклад, для найбільш поширених електронних pdf-документів, видимий цифровий водяний знак створюється програмно шляхом накладання на електронну сторінку шару з напівпрозорим текстовим підписом. Такі *ЦВЗ* реалізуються також у програмному середовищі, зокрема в останніх версіях програми Adobe Acrobate Pro. Відповідно, недоліком створення таких *ЦВЗ* є те, що маючи доступ до pdf-файлу, в програмному середовищі можна легко видалити будь-який видимий *ЦВЗ*. Наприклад, у програмі Adobe Acrobate Pro достатньо виділити цей водяний знак інструментом редагування тексту і видалити його. Тому такі *ЦВЗ* у нашій роботі ми розглядати не будемо, хоча для простого захисту електронних документів видимі ЦВЗ можна використовувати, але тоді необхідно виставляти обмеження для редагування таких документів за допомогою системи парольного захисту.

До скритих водяних знаків впроваджених у *ЦІС* можна віднести *ЦВЗ* створені на основі метаданих, які додаються до документу на основі атрибутів доповнення *ЦВЗ* до фалу, який необхідно захистити. ЦВЗ на основі метаданих, це найпростіший спосіб захистити EB_i, але через свою простоту він є і найбільш вразливим, бо метадані, також як і видимий ЦВЗ, можна легко видалити у програмі, яка сворювала цей ЦВЗ. Наприклад, для pdf-документа достатньо зайти у програмі Adobe Acrobate Pro в діалогове вікно параметри документа, де усі супровідні атрибути стануть доступними для редагування і для їх видалення. Отже, через свою вразливість до будь-яких модифікацій, такі ЦВЗ також не розглядатимемо.

Скриті ЦВЗ, які не підпадають під означення метаданих, тобто інформацію про які неможливо визначити, без відповідного на це програмного забезпечення, і які безпосередньо вшивають інформацію у зображення чи сторінку з текстом, також можна поділити на дві категорії: 1) ЦВЗ, які створюються шляхом маніпуляції бітів цифрового середовища і 2) ЦВЗ, які створюються за допомогою впровадження у ЦІС векторних форм, або прозорих символів тексту, які стають невидимими для користувача. Розглянемо ці два випадки впровадження у цифрове інформаційне середовище скритих ЦВЗ.

До найбільш поширених методів впровадження ЦВЗ у графічні зображення можна віднести такі алгоритми:

— DCT (Discrete Cosine Transform) — як у JPEG, MPEG;
— DWT (Discrete Wavelet Transform) — для ще більш стійкого захисту.

Недоліком таких методів впровадження є те, що, наприклад, текстовий, матеріал у векторній формі необхідно спочатку перетворити у графічне зображення і лише після цього можна буде використовувати методи DCT чи DWT впроваджування *ЦВЗ.* Незважаючи на високу стійкість таких EB_i до атак і важкість визначення в електронних документах наявність *ЦВЗ*, використання методів DCT та DWT впроваджень *ЦВЗ* для тектових документів є не зовсім доцільним. Насамперед це пов'язано з тим, що зростає розмір файлу, особливо, якщо це багатосторінкова публікація, де кожна сторінка перетворюється на її графічний растровий скан. А також зростає час на зчитування *ЦВЗ* з таких документів і, відповідно, зменшується якість визначення ЦВЗ, якщо ПК не задовольняє високим вимогам для видобутку *ЦВЗ* з кожної растрової сторінки EB_i. Хоча алгоритми впровадження *ЦВЗ* у EB_i досить непогано себе зарекламували для публікацій у яких є невеликий відсоток зображень поруч з тектсовим масивом інформації. В цьому випадку ЦВЗ впроваджується не для кожної сторінки EB_i а лише для зображень, які містяться на сторінках тексту. Тому такий варіант, як альтернативний, можна враховувати і через особливості того чи іншого EB_i з наявними у них зображеннями, досить ефективно використовувати на практиці.

Якщо розглядати *ЦВЗ* на основі впровадження у сторінки EB_i невидимого тексту або елементів у векторну структуру файлу, то це буде найкращим варіантом для зменшення вразливості таких документів до атак на виявлення в EB_i *ЦВЗ.* Правда, якщо це стосується невидимого для користувача тексту, наприклад за допомогою надання йому кольору паперу (білий колір), то такий текст також також можна буде легко виявити, за допомогою інструментів редагування тексту в документі, тому цей метод не дуже підходить для впроваджень у електронні документи *ЦВЗ*. Проте впровадження у *ЦІС* електронних документів замаскованих векторних структур робить їх дійсно стійким для виявлення цифрового водяного знаку, без необхідного програмного забезпечення. Окрім того такі алгоритми практично не збільшують розмір файлу з *ЦВЗ* і досить добре себе зарекомендували для EB_i з великими обсягами тексту.

Метод оцінки ризику виявлення ЦВЗ у цифровому інформаційному середовищі електронного документа

Для оцінки і формалізації ризику впровадження і виявлення ЦВЗ на основі вищенаведених методів введемо для понять вразливості, загрози і ризику певні рівні.

Так, наприклад, для нашого випадку досліджень введемо наступні поняття вразливості, загрози та ризику для захисту авторських прав на основі впроваджень ЦВЗ.

Означення 5. Вразливість цифрового водяного знаку (V) — це його рівень стійкості до будь-яких загроз, який можна поділити на три рівні:

— 1 — низька (мала вразливість);
— 2 — середня вразливість;

— 3 — висока вразливість.

Пояснення рівнів вразливості:

— *висока вразливість* — ЦВЗ можна легко виявити або видалити без спеціалізованих знань (наприклад, через редактор або очищення метаданих);

— *середня вразливість* — ЦВЗ частково захищений, але за наявності базових знань або програм може бути виявлений;

— *низька вразливість* — ЦВЗ є глибоко інтегрованим у структуру документа/зображення, потребує високих знань та інструментів для виявлення чи модифікації.

Введемо означення для загрози системі захисту авторських прав.

Порівняльний аналіз вразливостей вищеописаних типів ЦВЗ у ЦІС наведений у табл. 1.

Таблиця 1.

Порівняльна таблиця типів цифрових водяних знаків (ЦВЗ) у ЦІС

№	Тип впровад-ження	Вид ЦВЗ	Мета впровад-ження	Приклад застосування	Рівень вразливості	Коментар / рекомендації
1	Метадані файлу	Прихований у атрибутах	Вбудоване маркування, авторизація	PDF, DOCX, JPG (EXIF), MP3 (ID3)	Висока	Метадані легко змінити або видалити у звичайних редакторах.
2	Візуальний	Видимий знак або логотип	Демонстрація авторства/ прав	Скановані документи, фотографії	Середня	Захищає від несанкціонованого друку/копій. Легко прибрати в графічних редакторах.
3	Структура ЦІС – DCT/ DWT	Невидимий (на основі зображень)	Стеганографічне вбудовування у зображення	PDF з вбудованими зображеннями, JPEG, PNG	Низька	Стійкий до базового редагування. Потребує спеціалізованого ПЗ для виявлення/видалення.
4	Структура ЦІС – векторні	Невидимий (векторні об'єкти)	Приховані векторні позначки в документі	PDF, SVG, AI, текстові шари у CAD	Середня/ Низька	Може бути ефективним для PDF з текстом. Важко виявити без знання структури.
5	Гібридні методи	Комбіновані ЦВЗ	Поєднання візуального та прихованого знаку	Високозахищені публікації, ліцензійні документи	Низькаа	Рекомендується для критичних документів. Складний для атаки через комбіновану структуру.

Означення 6. Загроза для системи захисту авторських прав на основі цифрового водяного знаку (Z) — це інтенсивність зовнішнього негативного впливу з боку зловмисника, яку можна поділити на три рівні:

— 1 — низька ймовірність атаки або обмежені можливості зловмисника;

— 2 — середня загроза через малу вразливість ЦВЗ;

— 3 — висока (висока мотивація/доступ до ПЗ, слабкість захисту ЦВЗ).

В нашому дослідженні використовується адитивна модель оцінки ризику, яка передбачає зменшення вразливості V через впровадження контрзаходів (C), пов'язаних з впровадженням стійких до зовнішніх атак та спотворень ЦВЗ. В контексті інформаційної безпеки — така модель зустрічається в методиках STRIDE, CVSS та ISO/IEC 27005, де ризик може бути модифікований впливом захисних заходів.

Введемо уточнену формулу (1) для оцінки величини ризику з врахуванням контрзаходів C_i для i-того об'єкту:

$$R_i = (V_i - C_i) + Z_i, \tag{2}$$

для уточнної формули (2) рівні ризику визначаються на основі:

— V_i — рівня вразливості *ЦВЗ* (1 – низька, 2 – середня, 3 – висока);

— C_i — ефективність контрзаходів (0–3), які зменшують вразливість ЦВЗ;

— Z_i — рівень загрози (1 – низький, 2 – середній, 3 – високий).

Тоді рівень ризику захисту авторських прав у EB_i на основі впровадження у них ЦВЗ буде визначатись на основі нормованої оцінки ризику (в межах: 1–6). Якщо $(V_i - C_i)$J 0, тоді вважається, що вразливість ЦВЗ у EB_i нейтралізована.

На основі наведених нами припущень змоделюємо схему оцінки ризику для системи захисту авторських прав на видання EB_i (рис. 1).

Проведені в роботі дослідження з впровадження контрзаходів доволяють зменшувати ризик здійснення атак на систему ZAP. Нормалізована оцінка ризику для різних ЦВЗ наведена в табл. 2.

Таблиця 2.

Оцінка ризику з врахуванням контрзаходів для ЦВЗ

№	Тип ЦВЗ	Вразливість (*V*)	Загроза (*Z*)	Контрзаходи (*C*)	Ризик (*R*)	Інтерпретація
1	Метадані	3	3	1	5	Високий ризик
2	Видимий	2	2	1	3	Середній ризик
3	DCT/DWT	2	2	2	2	Низький ризик
4	Векторний (SVG/об'єкт)	2	1	2	1	Дуже низький ризик
5	Гібридний (видимий + DWT)	2	1	3	0 + 1 = 1	Мінімальний ризик

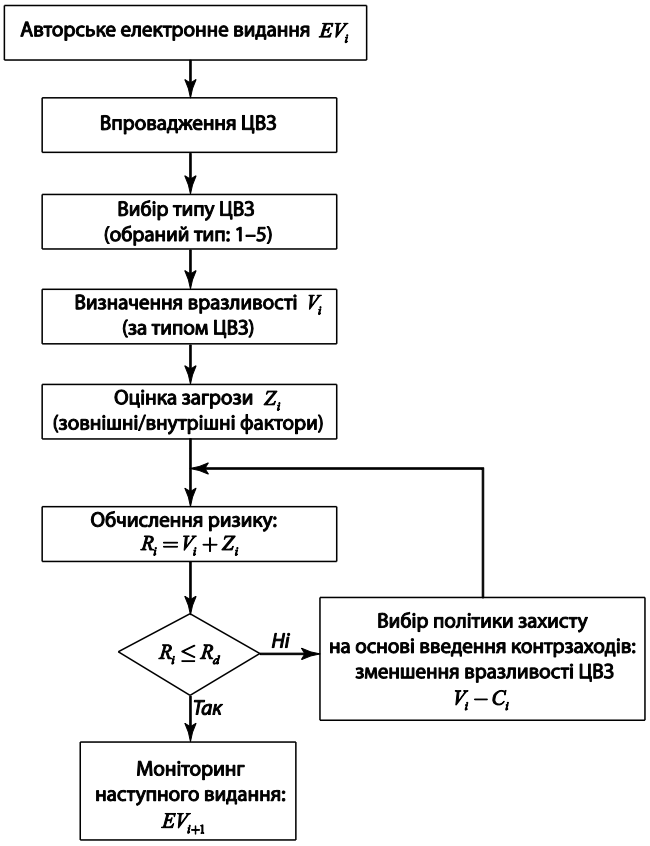

Рис. 1. Функціональна схема оцінки рівня ризику в системі захисту авторських прав на авторські електронні видання з використанням ЦВЗ

У табл. 3. наведений опис контрзаходів для зменшення вразливості *ЦВЗ*, впроваджених у EB_i до атак на систему захисту авторських прав.

Таблиця 3.

Приклади контрзаходів (С) і їх ефективність:

Контрзахід	Значення С
Немає активних заходів	0
Простий контроль (пароль, повідомлення про авторство)	1
Впровадження криптографії, виявлення змін (хеш, цифровий підпис)	2
Комбінована технологія: криптографія + невидимий ЦВЗ + моніторинг	3

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

Розглянуті в роботі типи критичних атак, які можуть бути використані зловмисниками для порушення системи захисту авторських прав для електронних документів дозволяють створювати відповідні методи та засоби протидії таким атакам. Введені поняття ризику, загрози, вразливості електронного документа, який має ідентифікатор авторства, на основі яких можна розробляти методи оцінки ризику виникнення атак і створювати відповідні контрзаходи для зменшення таких вразливостей до відповідних існуючих загоз виявлення цифрового водяного знаку. Проведений аналіз сучасних методів впровадження цифрових водяних знаків у цифрове середовище електронних документів та їхнє порівняння згідно з критеріями запоропонованих у статті рівнів

шкал. Таким чином змодельовані та запропоновані у роботі алгоритми і проведені досліження оцінки ризику захисту електронних видань з впровадженими у них ЦВЗ дозволяють зробити висновок, що найкращого результату можна досягти завдяки використанню комбінованих технологій контрзаходів на основі криптографічних методів захисту ЦВЗ, розміщення його у невидимих для користувача зонах і проведенням постійного моніторингу на вразливість ЦВЗ до зовнішніх атак.

Література

1. Закон України «Про авторське право і суміжні права». (Відомості Верховної Ради (ВВР), 2023, № 57, ст.166.
2. Закон України «Про електронну ідентифікацію та електронні довірчі послуги» № 2801-IX від 01.12.2022. Відомості Верховної Ради (ВВР), 2017, № 45, ст.400. [Електронний ресурс] посилання на ресурс: https://zakon.rada.gov.ua/laws/show/2155-19#Text
3. Зубко І. Мартовитський В., Пунченко А., Карачевцев Д. Огляд методів нанесення цифрових водяних знаків для захисту зображень. Системи управління, навігації та зв'язку. Полтава, 2024. Т. 3. № 77. С. 121–125. doi: 10.26906/SUNZ.2024.3.121
4. Рубан І. В., Бологова Н. М., Мартовицький В. О. Інформаційна технологія підтвердження права власності на цифрові зображення. Сучасні інформаційні системи. 2022. Т. 6. № 1. С. 118–123.
5. Бодня М., Єсіна М., & Пономар В. Дослідження можливостей застосування стеганографічних та крипто-графічних алгоритмів для приховування інформації. Комп'ютерні науки та кібербезпека, Київ: 2024. Вип. 2. С. 43–57.
6. Дурняк Б. В., Сабат В. І., Музика Д. В. Стеганографічні методи захисту документів. Монографія. Л. : УАД, 2013. 160 с.
7. Дурняк Б. В., Сабат В. І., Пашкевич В. З., Тимченко О. В. Інформаційна технологія формування графічних засобів захисту документів. Монографія. Л. : УАД, 2011. 152 с.
8. Карпінець В. В., Яремчук Ю. Є. Методи захисту векторних зображень цифровими водяними знаками. Монографія. Вінниця : ВНТУ, 2013. 156 с.
9. Дурняк Б. В., Петріашвілі Г. Г., Сабат В. І., Майба Т. М. Визначення рівня безпеки технологічних процесів на основі оцінювання ризику. Монографія. Л. : УАД, 2019. 160 с.
10. Сабат В. І. Обґрунтування методів захисту документів в системах документообігу для виробничих структур. Комп'ютерні технології друкарства. 2022. № 1(47). С. 176–190.
11. Зубок М. І. Інформаційна безпека в підприємницькій діяльності. К. : ГНОЗІС, 2015. 216 с.

References

1. Law of Ukraine "On Copyright and Related Rights". (Vedomosti Verkhovna Rada (VVR), 2023, No. 57, p. 166.
2. Law of Ukraine "On Electronic Identification and Electronic Trust Services" No. 2801-IX dated 01.12.2022. Vedomosti Verkhovna Rada (VVR), 2017, No. 45, p. 400. [Electronic resource] link to the resource: https://zakon.rada.gov.ua/laws/show/2155-19#Text
3. Zubko I., Martovytskyi V., Punchenko A., & Karachevtsev D. (2024). Overview of digital watermarking methods for image protection. Control, Navigation and Communication Systems, 3(77), 121–125. https://doi.org/10.26906/SUNZ.2024.3.121
4. Ruban I. V., Bologova N. M. & Martovytsky V. O. (2022) Information technology for confirming ownership of digital images. Modern information systems. 6(1), 118–123.
5. Bodnya M., Yesina M., & Ponomar V. Research into the possibilities of using steganographic and cryptographic algorithms for hiding information. Computer science and cybersecurity, Kyiv: 2024. Vol. 2. P. 43–57.
6. Durnyak B. V., Sabat V. I. & Muzyka D. V. (2013) Steganographic methods for document protection. Monograph. L.: UAD, 160 p.
7. Durnyak B. V., Sabat V. I., Pashkevych V. Z. & Tymchenko O. V. (2011) Information technology for forming graphic means of document protection. Monograph. L.: UAD, 152 p.
8. Karpinets V. V., Yaremchuk Yu. Ye. (2013) Methods of protecting vector images with digital watermarks. Monograph. Vinnytsia: VNTU, 156 p.
9. Durnyak B. V., Petriashvili G. G., Sabat V. I. & Mayba T. M. (2019) Determining the security level of technological processes based on risk assessment. Monograph. L.: UAD, 160 p.
10. Sabat V. I. (2022) Substantiation of document protection methods in document management systems for production structures. Computer printing technologies. 1(47), 176–190.
11. Zubok M. I. (2015) Information security in business activities. K.: GNOZIS, 216 p.