УДК 004.056.55 (043.3)

МЕТОДИ ВИРІШЕННЯ ЗАДАЧ АВТОРИЗАЦІЇ В СИСТЕМІ ЗАХИСТУ АВТОРСЬКИХ ПРАВ

В. І. Сабат, О. О. Богоніс

Національний університет «Львівська політехніка», вул. Під Голоском, 19, Львів, 79020, Україна

В роботі вирішуються задачі авторизації інтелектуальної власності у вигляді електронних видань чи програмного забезпечення за допомогою систем захисту авторських прав. Системи захисту авторських прав використовують засоби захисту електронних документів за допомогою впровадження в них цифрових водяних знаків, невидимих для людського ока, але таких, що проявляються за допомогою пристроїв зчитування скритої інформації.

Запропоновані в роботі алгоритми побудови моделі виявлення несанкціонованого інтелектуального продукту, за допомогою впровадження в нього цифрового водяного знаку, дозволяють виявляти нелегальні електронні видання та нелегальних власників інформації, які їх поширюють, порушуючи тим самим законні авторські права виробників інтелектуальної власності у вигляді електронних видань.

Наведений в роботі загальний алгоритм функціонування системи захисту авторських прав дозволяє розробляти інформаційні технології, що базуються на основі засобів захисту авторських прав з впровадженням у електронні видання невидимих водяних знаків та системах моніторингу таких видань в мережі Інтернет і на ринку поширення електронних видань. Такі моделі можуть бути ефективним засобом захисту інтелектуальної продукції від піратських копій і підробок електронних видань і рекомендуються до використання у системах захисту авторських прав.

Ключові слова: *цифровий водяний знак, системи захисту авторських прав, параметри цифрового середовища; моделі моніторингу; оцінювання ризику.*

Постановка проблеми. Сьогодні актуальною проблемою є захист авторських прав виробників електронних документів та авторів інтелектуального продукту, яким може бути програмне забезпечення чи електронне видання. Насамперед це пов’язано з вразливістю електронних видань до порушення їхніх основних параметрів, таких як конфіденційність, цілісність, модифікація. Але окрім вказаних параметрів, що потребують захисту від зовнішніх атак, важливим параметром в системі захисту є також параметр, який свідчить про авторство електронного видання. Порушуючи авторство електронного видання нелегальний власник може його підмінити, використати у своїх потребах з метою наживи чи поширення для вільного доступу. Тим самим зловмисники порушують авторські права на інтелектуальну продукцію і її захист, що потребує розроблення засобів виявлення

нелегальних електронних видань і, відповідно, нелегальних власників інформації. Такі засоби захисту використовують системи захисту авторських прав.

Крім використання криптографічних засобів захисту та розроблених на їх основі цифрового підпису, що засвідчують достовірність чи авторизацію електронного документа, існують ще механізми впровадження в цифрове середовище інтелектуального продукту цифрових водяних знаків. Дослідження, проведені в цій роботі, базуються на розробленні моделі системи захисту з впровадженням цифрових водяних знаків в електронні документи та на їх основі розв'язування проблем авторизації електронних видань.

Аналіз останніх досліджень та публікацій. Проблеми вирішення задач авторизації авторських прав є досить актуальними на сьогодні і висвітлені у працях багатьох вітчизняних та закордонних науковців. Так, наприклад, підвищення захисту відеоінформації від несанкціонованого копіювання і розповсюдження розглянуто в колективній статті вітчизняних науковців [1]. У роботі [2] автори досліджують різні підходи до вбудовування водяних знаків у зображення та проводять їх порівняльний аналіз з точки зору ефективності, стійкості до атак та вартості впроваджень. Інформаційні технології підтвердження прав власності на цифрові зображення розглянуто у роботі [3]. Використання криптографічних засобів захисту для приховування інформації розглянуто в роботі [4] і стенганографічні методи захисту інформації — в колективній монографії [5]. Юридичні аспекти та нормативні положення законодавства України, які регламентують правові аспекти захисту авторських прав розглянуті в роботі [7].

Сучасні розробки методів впровадження водяних знаків на цифрових зображеннях і визначення практики їх протидії з незаконним розповсюдженням авторської інформації та програмного забезпечення розглянуті в працях [8,9]. Захист інтелектуальної власності за допомогою використання штучного інтелекту розглянуті в колективній праці закордонних авторів [10].

Проте не так багато є досліджень, які стосуються саме вирішенню задач авторизації інтелектуальної власності у вигляді електронних видань з подальшим їх несанкціонованим розповсюдженням та незаконним присвоєнням авторських прав. Такі задачі потребують як впровадження нових юридичних норм захисту інтелектуальної власності, так і розробок нових інформаційних технології в галузі захисту авторських прав.

Мета статті. Метою статті є розроблення алгоритмів та моделей захисту інтелектуальної власності у вигляді електронних видань та цифрових творів, які підлягають захисту авторських прав.

Виклад основного матеріалу дослідження. Проблеми захисту авторських прав передбачають дослідження та розв'язок задач, які в найбільшій мірі стосуються автентифікації. До них можна віднести:

- задачі виявлення несанкціонованої копії інформаційного продукту;
- задачі встановлення виробника несанкціонованого інформаційного продукту (*NIP*);
- задачі упередження можливості продукування *NIP* та інші задачі.

Одним із базових методів, який використовується для розв'язання вищевказаних задач, є метод, що передбачає використання цифрового водяного знаку (*ЦВЗ*). *ЦВЗ* впроваджуються у цифрове середовище інформаційного продукту (*ІР*), що потребує захисту і допомагають в подальшому виявляти їх та засвідчувати авторство того чи іншого електронного продукту. Задача виявлення екземплярів *NIP*, в більшості випадків, розв'язується шляхом маркування *IP* продуктів оригінальними маркерами, якими можна ідентифікувати кожний екземпляр *IP*. Але такий підхід в повній мірі дозволяє розв'язувати тільки задачу виявлення *NIP*. Для того, щоб можна було розв'язати задачу виявлення несанкціонованого виробника *IP*, необхідно створити деяку початкову структуру використання *IP* з впровадженням *ЦВЗ*. Крім того необхідно розширити за межі даних інформацію, яка може знаходиться в *ЦВЗ* і характеризує його тільки як маркер. Така інформація повинна бути узгоджена з методами функціонування початкової структури обслуговування *ЦВЗ*. При формуванні можливих методів розв'язку цієї задачі необхідно врахувати такі обмеження:

- процес продажу повинен забезпечувати анонімність покупця;
- інформація, що розміщується в *ЦВЗ* повинна визначатися на етапі технологічного процесу виготовлення окремого тиражу інформаційного продукту;
- управління процесом виготовлення кожного окремого тиражу інформаційного продукту повинно бути пов'язане з процесом управління системою обслуговування *ЦВЗ*;
- система обслуговування *ЦВЗ* повинна функціонувати у відповідності з певним варіантом, що визначається цілю використання *ЦВЗ*.

Така ціль може бути мінімальною і визначатися необхідністю встановлення факту виявлення *NIP*. Максимальна ціль використання *ЦВЗ* може полягати у забезпеченні, або у формуванні умов, при яких несанкціонований продукт не зможе бути використаним потенційним користувачем. Слід зауважити, що в цьому випадку, під інформаційним продуктом *IP* розуміється будь який продукт, що може являти собою інтелектуальну власність та цифрове електронне видання (*ЕВ*) одночасно.

Функціональна схема виявлення несанкціонованого інтелектуального продукту, який містить в своїй структурі *ЦВЗ* наведена на рис. 1.

На рис. 1 наведені наступні скорочення:

- *ZAP* — система захисту авторських прав;
- A(IP) — автор інтелектуального продукту;
- *IP* — інтелектуальний продукт, який потребує захисту;
- K_i — довільний неавторизований користувач, який хоче скористатись *IP*;
- *SKD (IP)* — система контролю доступу до *IP*;
- $K_i \rightarrow KI$ — ідентифікація системою контролю доступу неавторизованого користувача, де *KI* — користувач ідентифікований;
- $KI \rightarrow NVI$ — умови, при якій ідентифікований користувач порушує правила використання та поширення *IP*, переходячи тим самим у статус нелегального власника інформації;
- $IP \rightarrow NIP$ — інтелектуальна власність перетворюється в нелегальний інформаційний продукт;

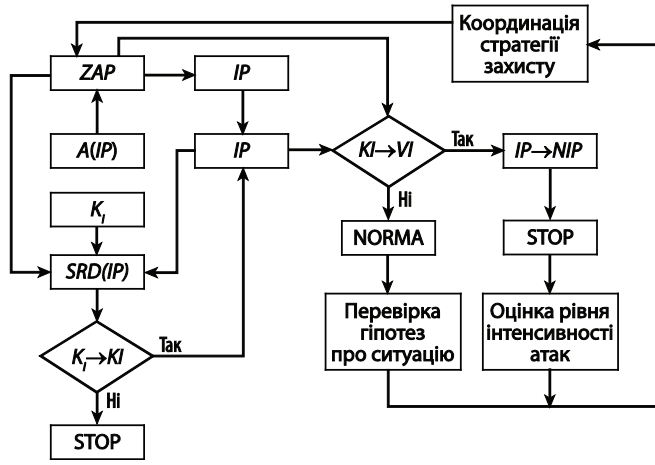

Рис. 1. Функціональна схема виявлення несанкціонованого інтелектуального продукту за допомогою системи *ZAP*

– *STOP* — зупинка надання послуг до *IP* системою *ZAP* несанкціонованому або нелегальному користувачеві;
– *NORMA* — позитивне завершення функціонування системи *ZAP*.

На рис. 1 зображено, як ідентифікований користувач *KI* стає нелегальним власником інформації, а це можливо лише при умовах невиконання усіх вимог, поставлених щодо дотримання авторських прав користування інтелектуальним продуктом. Якщо ж користувач порушує ті правила, наприклад, поширює *IP* без відповідного на це дозволу з боку автора інтелектуального продукту, то система виявлення та моніторингу переводить цей інтелектуальний продукт у статус нелегального інформаційного продукту та інформує *A(IP)* про порушення його авторських прав. Система контролю доступу до інтелектуального продукту *SKD (IP)* надає такий доступ для ідентифікованих користувачів, але не може контролювати розповсюдження ними цього *IP*, ті функції має виконувати підсистема моніторингу ринку, яка входить у структуру системи *ZAP*.

Оскільки на сьогодні досить чітко визначено поняття захисту авторських прав на ЕВ, що являє собою інтелектуальну власність, то основною ціллю використання ЦВЗ є по-перше виявлення несанкціонованого виробника *NIP* та по-друге доведення факту, що виявлена особа, чи організація є несанкціонованим виробником. Тоді необхідною умовою досягнення другої частини цілі є виявлення *NIP*.

Перше з вищенаведених обмежень, стосується тільки особистих даних покупця і не поширюється на реєстрацію всіх особливостей, що характеризують сам процес продажу. Це означає, що в процесі продажу можуть реєструватися індивідуальні дані проданого екземпляру ІР, час продажу, продавець, що здійснив продажу, об'єм проданого товару та інша інформація, яка стосується процесу продажу за винятком особистих даних покупця, що можуть його ідентифікувати. Для того, щоб можна було виявити *NIP*, необхідно, щоб цей продукт був офіційно представлений, що може бути реалізовано такими способами:

– на основі використання легальної реклами *IP*;
– на основі легального продажу відповідного *IP*;
– на основі офіційної передачі легального *IP* визначеним власникам та на основі використання інших засобів легалізації факту існування відповідного одного, або декількох екземплярів *IP*.

Анонімність покупця може мати різний характер, що можна описати наступними співвідношеннями покупця з факторами, які пов'язані з придбанням того чи іншого товару. Такі співвідношення анонімності покупця можуть бути наступними:
– анонімність покупця відносно продавця товару, яким є *EB*;
– анонімність покупця відносно довіреного посередника процесу придбання інтелектуальної власності;
– анонімність покупця відносно товару, або відносно *EB*;
– абсолютна анонімність покупця.

Перший тип анонімності є досить розповсюдженим і стосується більшості товарів, що можуть бути купленими покупцем. Ця анонімність гарантує свободу громадян у придбанні матеріальних цінностей, оскільки, виключає можливість несанкціонованого встановлення, шляхом моніторингу, рівня заробітку, або рівня достатку, яким володіє окремий потенційний покупець.

Зазвичай при реалізації процесів взаємодії користувача, що ідентифікується (*KI*) в інформаційній системі обслуговування і власника інформації (*VI*) використовуються залучення в систему обслуговування такої взаємодії третьої сторони. Основною задачею такого третього учасника є забезпечення необхідного рівня довіри між *KI* і *VI*. Для зручності, будемо позначати такого учасника символами *DI*. Найбільш поширеним прикладом використанням такого учасника є центр сертифікації системи обміну ключами [11]. Тому, анонімність покупця відносно довіреного посередника з формальної точки зору може розглядатися, хоча умови створення довірених третіх учасників обміну передбачають взаємну довіру двох сторін до довіреного посередника.

Інформаційні ресурси, що являють собою інтелектуальний продукт, можуть ідентифікуватися власником цього ресурсу, після його покупки. Такий ідентифікатор власника найчастіше використовуються в тому випадку, коли власник передбачає надавати у тимчасове використання відповідне *EB*. Така ідентифікація зазвичай не здійснюється в цифровій формі, тому, цей тип анонімності розглядатися не буде. Абсолютна анонімність покупця об'єднує всі вищезазначені види анонімності. Всі інші обмеження безпосередньо пов'язані з конкретною організацією системи обслуговування ЦВЗ, як засобів захисту авторських прав.

Оскільки порушення авторських прав повинно каратися у відповідності з нормами закону, то механізми, що використовуються для доведення порушення права, повинні бути визначеними в рамках законів.

Цифровими механізмами, що уже визначені в рамках юридичного права, і які використовуються для доведення факту порушення авторських прав є механізми цифрового підпису [12].

Розглянемо можливі засоби, за допомогою яких можна забезпечувати виконання обмежень, що накладаються на систему підтримки обслуговування *ЦВЗ* та

які, одночасно, забезпечують можливість досягнення цілі використання *ЦВЗ* і забезпечують одну з базових умов анонімності покупця *ЕВ*. Для розв'язку цих задач введемо наступні обмеження. Несанкціонований дистриб'ютор може появитися тільки в результаті здійснення операції продажу санкціонованим дистриб'ютором *ЕВ*. Таким чином, неуповноваженим дистриб'ютором може бути покупець, який легально купує певне *ЕВ*, або особа, яка тим, чи іншим чином скористалася з легально купленого екземпляру *ЕВ*. На ринку розповсюдження *ЕВ* існують механізми перевірки продажу легальних і нелегальних *ЕВ*, які діють незалежно від того, чи появилися на ринку нелегальні електронні видання (*NEB*) [13].

Приймемо, що виявлення несанкціонованого *ЕВ* може здійснюватися тільки у випадку продажу такого видання. З цього випливаю, що тільки легальний *КІ* може переходити у статус нелегального власника інформації (*NVI*). Якщо б дилер не наймав продавців, то визначення *NVI* можна було б здійснювати за ідентифікатором дилера, який має право продавати *ЕВ* певного тиражу. Приймемо також, що для кожного тиражу, або типу *ЕВ* визначається час $\Delta T_i(EB_i)$ актуальності авторських прав для даного EB_i. Параметр $\Delta T_i(EB_i)$, в межах функціонування системи захисту авторських прав (*ZAP*), може змінюватися незалежно від встановлених початкових границь мінімального ΔT_i і максимального ΔT_j значень. Таким чином, одним з параметрів *ZAP* є параметр ΔT_i, який може бути забезпечений у межах певної системи *ZAP*.

У випадку виявлення *NEB*, необхідно розв'язати задачу виявлення нелегального власника інформації *NVI*. В ідеальному випадку, така задача могла б бути розв'язана на основі даних ЦВЗ, нелегального екземпляру *ЕВ* та даних про безпосереднього *КІ*, що перейшов у стан *NVI*. Але через вимоги забезпечення анонімності *КІ*, реалізація таких процедур є досить складною. Розв'язок відповідної задачі вимагає організації деякої послідовності етапів, або кількість етапів функціонування системи *ZAP*, що приймемо як параметр *NE*.

Оскільки процес визначення нелегального власника інформації є досить складним, то при необхідності термінового встановлення конкретної особи, яка являє собою *NVI*, система *ZAP* повинна мати можливість розв'язувати цю задачу з різною мірою наближення. Для того, щоб говорити про наближене визначення потенційного *NVI*, необхідно визначити параметри *NVI* з різною мірою наближення. Приймемо, що захист авторських прав може здійснюватися наступними способами, або діями зі сторони *ZAP*:

- виявлення ідентифікаційних даних потенційного *NVI* з ціллю компенсації за його рахунок втрат автора, до яких призвело нелегальне використання *ЕВ*, при цьому, кінцевою ціллю встановлення особистих даних є виявлення місця знаходження відповідного *NVI*;
- виявлення об'ємів *NEB* та їх знищення з ціллю запобігання втратам автора від реалізації *NEB* передбачає визначення місця продукування екземплярів *NEB*.

Таким чином, параметр, який може визначитися з певним наближенням, являє собою адресу *NVI*, завдяки якій можна реалізувати наведені вище способи захисту авторських прав. Цей параметр, згідно з прийнятою системою адресації може мати різну міру наближення.

Іншим параметром, що визначається з різними мірами наближення, може бути величина об'єму екземплярів *NEB*, яка також може використовуватися для реалізації процедур пов'язаних із захистом авторських прав. Наприклад, в залежності від кількості екземплярів *NEB* можна визначити величину втрат, через порушення авторських прав і, відповідно, прийняти рішення про використання різних засобів протидії, вартість яких є різною.

Отже, система *ZAP* може визначати параметри, необхідні для реалізації процесів захисту з різною мірою наближення. Тому міра наближення (*MB*) може характеризувати систему *ZAP*, як один з її параметрів.

Наступний параметр, яким можна характеризувати систему *ZAP*, є параметр, що визначає величину втрат, яких не вдасться уникнути при використанні певної версії системи захисту. Якщо система *ZAP* виявляє *NVI* на першому етапі функціонування, то можна прийняти величину параметра втрат (*VT*), рівною нулю. Це означає, що виявлено *NEB*, яке випродуковано в рамках одного тиражу, об'єм якого можна визначити. На основі цього визначається величина втрат, яку отримав *VI* від продажі *NEB*, та обчислювати необхідну величину компенсації, яку повинен виплатити виявлений *NVI*. Якщо процес виявлення *NEB* складається з цілого ряду етапів, або $NE > 1$, то на кожному із етапів залишається певна кількість *NEB*, які були продані, і стосовно яких існує значно менше можливостей по встановленню величини відповідного тиражу. З цього випливає, що етапи виявлення та ідентифікації нелегального власника інформації синхронізуються з окремими тиражами видання *NEB*. Кількість етапів (*NE*) є параметром, що характеризує втрати, яких не вдається уникнути.

Важливим параметром системи *ZAP* також є параметр, що відображає швидкість визначення або ідентифікації *NVI* з моменту виявлення *NEB*. Слід зазначити, що процес активного функціонування *ZAP* починається з цього моменту. Тому можна стверджувати, що процес функціонування *ZAP* складається з таких періодів:

– періоду пасивного функціонування (*Tp*),
– періоду активного функціонування (*TA*),
– періоду не ініційованого функціонування (*TI*).

Пасивний період функціонування *ZAP* починається з моменту запиту *VI* на його обслуговування для захисту авторських прав. Цей момент починається з передачі тиражу *EB*, який визначається власником авторських прав *VI*, у торгівельну мережу. Він також може співпадати з часом випуску тиражу, або визначатися співвідношенням:

$$t_p\left(EB\right) = t_i + \Delta t_j\left(VI_j\right), \tag{1}$$

де t_i — поточний момент функціонування системи *ZAP*, який визначається незалежно від типу частини циклу функціонування *ZAP*; $\Delta t_j\left(VI_j\right)$ — інтервал часу, що починається з моменту t_i, який у більшості випадків, визначається моментом передачі тиражу *EB*, або *MB*, в торгівельну мережу та моментом часу, починаючи з якого замовляється перехід системи *ZAP* з $T_i \to T_j$. В найпростішому випадку $\Delta t_j\left(VI_j\right) = 0$.

Частина часу функціонування *ZAP*, або період T_p відводиться на моніторинг ринку EB_i, що проводиться з ціллю виявлення *NEB* і, відповідно, *NVI*. Цей період

не може тривати нескінченно і тому обмежується параметром ΔT_i, який характеризує період актуальності охорони авторських прав. З цього випливає, що параметр $\Delta T_i(EB)$ є обов'язковим параметром для обґрунтування доцільності використання послуг *ZAP* довільним *VI*(*EB*).

Період активного функціонування T_A може складатися з одного, або цілого ряду етапів реалізації процесу виявлення та ідентифікації *NVI*. Цей період закінчується після ідентифікації *NVI* для даного EB_i. Якщо період $T_A(EB_i)$ завершився, то починається період $T_p(EB_i)$, який триває до моменту завершення , або до моменту виявлення нового *NEB* на ринку продаж.

Період T_i визначається відносно зареєстрованих в *ZAP* авторів *EB*, або власників інформації *VI*. Необхідність виділення цієї частини часу функціонування обумовлена тим, що забезпечення існування *ZAP* потребує певних затрат і, якщо виникає період, коли зареєстровані *VI* не ініціюють періодів T_p для *ZAP* протягом певного критичного часу T_I, то функціонування *ZAP* припиняється.

У зв'язку з цим вводиться параметр *ZAP*, який характеризує міру пропускної здатності для послуг захисту авторських прав (*NP*). Цей параметр означає, скільки одночасно періодів T_p і особливо періодів T_A може бути ініційовано в рамках системи *ZAP* на даний момент часу t_i. Таким чином, модель *ZAP* формально можна описати:

$$ZAP = F\left(\Delta T, NE, MB, LP\right). \quad (2)$$

Для побудови моделі захисту авторських прав на інтелектуальну власність необхідно проаналізувати усі вищевказані параметри, наведені у формулі (2), їхні взаємозв'язки у системі захисту авторських прав та розробити алгоритм функціонування *ZAP*.

На основі виявлення параметрів, які впливають на систему захисту авторських прав наведених у співвідношенні (2), в роботі були проведені експериментальні дослідження з побудови моделі захисту авторських прав, яка враховує засоби авторизації інтелектуального продукту за допомогою введення у цифрове середовище невидимих для людського ока цифрових водяних знаків. Модель системи захисту авторських прав базується на процедурах моніторингу інтелектуального продукту, що представлений у вигляді електронного видання. Власник інтелектуального продукту (електронного видання) зацікавлений у тому, щоб дотримувались його авторські права, щодо реалізації його *IP* на ринку і отримання на основі цього прибутку від його реалізації для санкціонованих користувачів *KI*. Якщо його права на інтелектуальну власність порушуються, що вдається визначити за допомогою системи *ZAP*, тоді він може звертатись до відповідних виконавчих служб для захисту своїх авторських прав, що передбачається законодавчими актами про захист приватної інтелектуальної власності.

Загальний алгоритм моделі функціонування системи *ZAP*, наведений на рис. 2.

На рис. 2 наведені наступні скорочення:

- PT_i – період не ініційованого функціонування системи;
- *ZOVI* – запит на обслуговування від власника інформаційного продукту у вигляді *EB*;

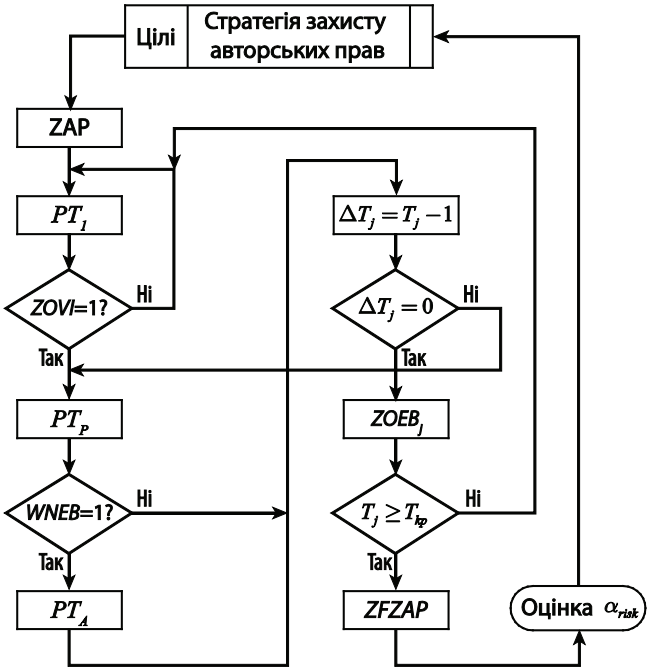

Рис. 2. Загальний алгоритм модлі функціонування системи *ZAP*

– PT_p – період моніторингу системи цифрових водяних знаків та виявлення несанкціонованого електронного видання, що належить автору інформаційного продукту, який замовив обслуговування;
– *VNEB* – перевірка, чи виявлено *NEB* в період моніторингу системою *NEB*;
– PT_A – період активного функціонування *ZAP* з ідентифікації *NVI*, визначенню тиражу *NEB* та по здійсненню функцій захисту авторських прав;
– $ZOEB_i$ – завершення обслуговування *AIP*, що замовив обслуговування по захисту авторських прав на EP_i;
– $T_i \geq T_{KP}$ – визначення чи час перевірки не ініційованого функціонування системи *ZAP* перевищив критичне значення;
– *ZFZAP* – завершення функціонування системи *ZAP*.

Наведений на рис. 2 алгоритм моделі функціонування *ZAP* відображає процес виконання функцій захисту авторських прав на рівні передачі управління між функціональними компонентами, що відображають окремі періоди моніторингу системи *S*. Функціональний блок PT_A, в цьому випадку, реалізує мінімальні функції протидії, які полягають в інформуванні системи *ZAP* про результат роботи блоку PT_p. Стратегія захисту авторських прав розробляється на основі аналізу та оцінки рівня ризику порушення авторських прав на інтелектуальну власність електронного видання, після чого виробляються цілі та додаткові засоби для системи захисту авторських прав, що наведено на рис. 2.

Висновки. Сьогодні надзвичайно актуальними є проблеми захисту авторських прав, особливо серед розробників програмного забезпечення та електронних

видань, які можуть поширюватись за допомогою глобальної мережі Інтернет. На жаль ефективних засобів, які б реалізували захист прав власників електронного продукту або інтелектуальної власності, дуже мало і зловмисники знаходять методи злому будь-якого захисту електронної інформації. В деяких випадках важко навіть доказати авторство того чи іншого інтелектуального продукту, якщо він не пройшов усі офіційні процедури ліцензування та патентування, які також у більшості випадків зловмисники можуть порушувати. Проблеми на інтелектуальну власність і на відкриття кримінальних справ за фактами її порушення можуть бути вирішені лише при розв'язуванні задач авторизації інтелектуального продукту. Впровадження систем захисту авторських прав із використанням цифрових водяних знаків забезпечує захист приватної власності на інтелектуальний продукт як виробників так і їхніх авторів.

Запропоновані в роботі алгоритми побудови моделі для системи захисту авторських прав дозволяють виявляти нелегальні електронні видання та нелегальних власників інформації, які їх поширюють, порушуючи тим самим законні авторські права виробників інтелектуальної власності у вигляді електронних видань. Такі моделі можуть бути ефективним засобом захисту інтелектуальної продукції від піратських копій і підробок електронних видань.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Яремчук Ю. Є., Карпінець В. В., Зоря І. С., Козак Д. О. Підвищення стійкості цифрових водяних знаків у потокових відеозаписах на основі диференціального вбудовування енергії (DEW). Вінниця : Вісник ВПІ, 2023. Вип. 1. С. 55–64.
2. 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. https://doi.org/10.26906/SUNZ.2024.3.121.
3. 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.
4. 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.
5. Megías, D.; Mazurczyk, W.; Kuribayashi, M. Data Hiding and Its Applications: Digital Watermarking and Steganography. Appl. Sci. 2021, 11, 10928. https://doi.org/10.3390/app112210928.
6. Дурняк Б. В., Сабат В. І., Музика Д. В. Стеганографічні методи захисту документів. Монографія. Л. : УАД, 2013. 160 с.
7. Тарасенко Л. Авторське право у цифрову епоху: Основні тенденції і зміни. Вісник Львівського національного університету. Серія юридична. 2022. Вип. 75. С. 61–72.
8. Ray A., Roy S. Recent trends in image watermarking techniques for copyright protection: a survey. Int J Multimed Info Retr 9, 249–270 (2020). doi: 10.1007/s13735-020-00197-9.
9. Megías, D.; Mazurczyk, W.; Kuribayashi, M. Data Hiding and Its Applications: Digital Watermarking and Steganography. Appl. Sci. 2021. Vol. 11:10928, Pp. 1–6. https://doi.org/10.3390/app112210928.

10. Regazzoni F., Palmieri P., Smailbegovic F., Cammarota R. and Polian I. Protecting artificial intelligence IPs: A survey of watermarking and fingerprinting for machine learning. CAAI Trans. on Intellig. Techn., 2021. Vol. 6. No. 2. Pp. 180–191.
11. Recommendation X.509 (2019) Corrigendum 2 (10/23) URL: https://www.itu.int/rec/T-REC-X.509-202310-I!Cor2/en.
12. Subramanya S. R. Digital signatures. IEEE Potentials. 2006. Vol. 25(2). Pp. 5-8. doi: 10.1109/MP.2006.1649003.
13. Сабат В. І. Богоніс О. О. Побудова математичної моделі моніторингу для системи захисту авторських прав. Наука і техніка сьогодні. К. : Наукові перспективи, 2025. № 6(47). 1537–1553 с.

REFERENCES

1. Yaremchuk, Y. Ye., Karpinets, V. V., Zorya, I. S., & Kozak, D. O. (2023). Enhancing the robustness of digital watermarks in streaming video using differential energy embedding (DEW). Herald of VPI, (1), 55–64.
2. Zubko, I., Martovitskyi, V., Punchenko, A., & Karachevtsev, D. (2024). A review 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.
3. Ruban, I. V., Bologova, N. M., & Martovytskyi, V. O. (2022). Information technology for ownership verification of digital images. Modern Information Systems, 6(1), 118–123.
4. Bodnia, M., Yesina, M., & Ponomar, V. (2024). Research on the use of steganographic and cryptographic algorithms for information hiding. Computer Science and Cybersecurity, (2), 43–57.
5. Megías, D., Mazurczyk, W., & Kuribayashi, M. (2021). Data hiding and its applications: Digital watermarking and steganography. Applied Sciences, 11(10928), 1–6. https://doi.org/10.3390/app112210928.
6. Durnyak, B. V., Sabat, V. I., & Muzyka, D. V. (2013). Steganographic methods for document protection (Monograph). Lviv: Ukrainian Academy of Printing.
7. Tarasenko, L. (2022). Copyright in the digital age: Key trends and changes. Bulletin of the Lviv National University. Legal Series, (75), 61–72.
8. Ray, A., & Roy, S. (2020). Recent trends in image watermarking techniques for copyright protection: A survey. International Journal of Multimedia Information Retrieval, 9, 249–270. https://doi.org/10.1007/s13735-020-00197-9.
9. Megías, D., Mazurczyk, W., & Kuribayashi, M. (2021). Data hiding and its applications: Digital watermarking and steganography. Applied Sciences, 11(10928), 1–6. https://doi.org/10.3390/app112210928.
10. Regazzoni, F., Palmieri, P., Smailbegovic, F., Cammarota, R., & Polian, I. (2021). Protecting artificial intelligence IPs: A survey of watermarking and fingerprinting for machine learning. CAAI Transactions on Intelligence Technology, 6(2), 180–191.
11. International Telecommunication Union. (2023). Recommendation X.509 (2019), Corrigendum 2 (10/23). https://www.itu.int/rec/T-REC-X.509-202310-I!Cor2/en.
12. Subramanya, S. R. (2006). Digital signatures. IEEE Potentials, 25(2), 5–8. https://doi.org/10.1109/MP.2006.1649003.

13. Sabat, V. I., & Bohonis, O. O. (2025). Development of a mathematical monitoring model for a copyright protection system. Science and Technology Today, (6)47, 1537–1553.

doi: 10.32403/0554-4866-2025-1-89-21-32

METHODS FOR SOLVING AUTHORIZATION TASKS IN COPYRIGHT PROTECTION SYSTEMS

V. I. Sabat, O. O. Bohonis

Lviv Polytechnic National University
19, Pid Holoskom, St., Lviv, 79020, Ukraine
volodymyr.i.sabat@lpnu.ua, oleksandr.o.bohonis@lpnu.ua

This paper addresses a pressing issue in the field of copyright protection—namely, the detection of illegal copies of digital information products that fall under the intellectual property rights of their developers and authors. This problem is particularly significant for software developers and publishers of electronic content, whose products are often distributed via the global Internet. Unfortunately, effective mechanisms for protecting the rights of electronic product owners or intellectual property holders are scarce, and malicious actors are continuously discovering new ways to circumvent digital protection systems. In many cases, it is even difficult to prove the authorship of a given intellectual product if it has not undergone official licensing or patenting procedures—which, in turn, can also be violated or bypassed by infringers. The challenge of asserting intellectual property rights and initiating legal action against violations can only be addressed by solving the problem of intellectual product authorization. The implementation of copyright protection systems that employ digital watermarking offers a robust method for safeguarding private ownership of intellectual products—both for manufacturers and their original authors. The algorithms proposed in this paper provide a model for detecting unauthorized use of intellectual products through the embedding of digital watermarks. These algorithms enable the identification of pirated electronic publications and the individuals or entities distributing them, thereby enforcing the legitimate copyrights of intellectual property holders. The general algorithm presented herein for the operation of a copyright protection system lays the foundation for the development of information technologies that utilize invisible digital watermarks embedded in electronic documents, along with monitoring systems for tracking their distribution online and in the digital marketplace. Such models are recommended for use in copyright protection systems as effective tools to combat piracy and counterfeit digital content.

Keywords*: digital watermark, copyright protection systems, parameters of the digital environment, monitoring models, risk assessment.*

Стаття надійшла до редакції 03.04.2025.
Received 03.04.2025.