Технології захисту від підробок і піратства

Огляд Anti-Counterfeiting Technology Guide – посібника, підготовленого Європейською обсерваторією з питань порушення прав інтелектуальної власності EUIPO

IP OFFICE
Український національний офіс інтелектуальної власності та інновацій

IPRights
MONITORING CENTER
Ukrainian National Office for Intellectual Property and Innovations

Липень 2024

Цей документ ґрунтується на аналізі посібника з технологій захисту від підробок (Anti-Counterfeiting Technology Guide), що був розроблений у 2021 році Європейською обсерваторією з питань порушення прав інтелектуальної власності Європейського відомства інтелектуальної власності (EUIPO) за підтримки Експертної групи з технологій боротьби з підробками та Експертної групи з впливу технологій, і не відображає офіційну позицію УКРНОІВІ.

Огляд є результатом діяльності робочої групи Громадська обізнаність Центру спостереження з питань порушень прав інтелектуальної власності (далі – Центр спостереження IPR).

Центр спостереження IPR вітає будь-які подальші пропозиції або коментарі до теми цього Огляду з метою подальшого поглиблення розуміння тенденцій та проблем функціонування технологій захисту від підробок і піратства, а також найкращих практик для їх застосування.

Посилання:

- Посібник з технологій захисту від підробок
- Інтерактивний пошук та Інструкція з користування посібником

Технології боротьби з підробками і піратством надають інструменти, які допомагають визначити чи є продукт оригінальним, чи підробленим, або чи був він об'єктом шахрайських дій. Така діяльність може включати різні методи – від прикріплення дистанційних датчиків до вбудовування в продукт прихованих ідентифікаторів.

Центр спостереження IPR підготував огляд посібника з технології захисту від підробок і піратства (Anti-Counterfeiting Technology Guide), що був розроблений Європейською обсерваторією з питань порушення прав інтелектуальної власності EUIPO за підтримки Експертної групи з технологій боротьби з підробками та Експертної групи з впливу технологій і покликаний допомогти бізнесу, правовласникам і новаторам вирішити, які технології найкраще підходять для захисту.

Посібник з технологій захисту від підробок (далі – Посібник) був розроблений як дорожня карта боротьби з підробками і піратством. Кожна глава документа присвячена певному типу технології: глави 1–5 охоплюють окремі категорії технологій, класифіковані за методами; глави 6 і 7 охоплюють додаткові інструменти та галузеві стандарти, які можуть сприяти створенню більш ефективної комплексної стратегії боротьби з підробками:

I. Електронні технології для захисту від підробок
II.Технології маркування для захисту від підробок
III. Хімічні та фізичні технології для захисту від підробок
IV. Механічні технології для захисту від підробок
V. Технології захисту від підробок для цифрових медіа
VI. Технологія спільного реєстру для захисту від підробок (блокчейн)
VII. Стандарти ISO для технологій захисту від підробок

Посібник призначений для всіх підприємців та компаній, включаючи малі та середні підприємства, які зацікавлені в отриманні додаткової інформації про рішення для боротьби з підробками.

Цей огляд включає короткий перегляд та аналіз категорій і розділів технологій боротьби з підробками, що містяться в Посібнику.

I. ЕЛЕКТРОННІ ТЕХНОЛОГІЇ

Всі електронні технології боротьби з підробками передбачають зв'язок електронних пристроїв передачі даних з товарами в той чи інший спосіб. Ці пристрої дають змогу унікально ідентифікувати та відстежувати товари, або надаючи конкретну інформацію про товар, або надаючи доступ до бази даних, де зберігаються відповідні дані.

Електронні технології для захисту від підробок	
Radio Frequency Identification (RFID)	RFID – використовує радіочастотні технології для дистанційного розпізнавання об'єктів, тварин або людей. Три ключові елементи : 1. Бірки – вони прикріплюються до товару і включають в себе антену та мікрочіп, який містить дані про товар (наприклад, унікальні ідентифікатори або URL-адреси веб-сайтів, які містять додаткову інформацію). 2. Зчитувачі – використовуються для запиту тегу, отримання відповіді, інформації та передачі її до системи обробки даних. 3. Система обробки даних – підключається до зчитувача через Інтернет. Система використовує ідентифікаційні коди з міток для отримання та управління всією доступною інформацією, пов'язаною з об'єктами.
Near Field Communication (NFC)	Мітки NFC можуть використовуватися з різноманітними продуктами та матеріалами. Вони дозволяють користувачам зв’язати кредитну картку зі своїм пристроєм і здійснювати платежі, коли пристрій знаходиться достатньо близько до платіжної машини з підтримкою NFC. Оскільки багато смартфонів вже мають вбудований зчитувач міток NFC, споживачі можуть використовувати цю технологію для перевірки автентичності самих продуктів.
Electronic Seals	Електронні печатки надають додатковий рівень безпеки, записуючи розширену інформацію про товар і дозволяючи відстежувати та контролювати його в режимі реального часу. Дані, що містяться в електронній печатці, можуть передаватися, зчитуватися і перевірятися сторонніми програмами, наприклад під час митних перевірок.
Magnetic Stripes	Магнітні смуги найчастіше використовуються на фінансових картках. Однак вони також можуть бути нанесені безпосередньо на цінний об'єкт (якщо фізичні характеристики та умови використання дозволяють), щоб гарантувати його автентичність та відстежувати його.
Contact Chips	Ця технологія працює шляхом вбудовування мікрочипа в пластикову картку. Мікрочип містить унікальні дані про продукт, які зчитуються шляхом вставляння частини картки з мікрочипом у зчитувальний пристрій.

Тож, існує п'ять типів електронних технологій захисту від підробок, але найпоширенішими є ті, що базуються на радіо частотної ідентифікації (RFID) і ближнього радіозв'язку (NFC), які здійснюють дистанційне розпізнавання об'єктів.

II. ТЕХНОЛОГІЇ МАРКУВАННЯ

Технології маркування працюють шляхом позначення продуктів унікальними елементами захисту, переважно графічними візерунками або кодами.

Існує декілька різних типів технологій маркування. Найбільш широко використовуються ті, які можна перевірити візуально через їх різноманітність, низьку вартість за одиницю та прості процедури перевірки – у багатьох випадках перевірку можна виконати візуальним оглядом або за допомогою смартфона.

Технології маркування для захисту від підробок	
Optical Memory Stripe	Оптична стрічка пам'яті – фактично лазерний зчитувальний пристрій, який здатний зберігати дані та зображення до відносно великої місткості.
Machine-Readable Codes	Машинозчитувані коди, також відомі як штрих-коди – ідентифікаційні коди, які призначені для зчитування за допомогою оптичного сканування.
One-Dimensional Barcodes	Одновимірні штрих-коди складаються з одного ряду штрихів, в яких дані закодовані горизонтально, можуть бути використані на майже всіх видах товарів. Кожен тип штрих-коду має певний набір дозволених символів (наприклад, цифри, буквено-цифрові символи, спеціальні символи) і, в деяких випадках, максимальну кількість символів або цифр.
Two-Dimensional Barcodes	Двовимірні штрих-коди можуть зберігати різноманітні дані та мають більшу місткість, ніж одновимірні штрих-коди. Дані зберігаються як по горизонтальних та вертикальних осях графічного зображення, яке можна видрукувати, вставити на цифровий екран або іншим чином представити для сканування та аналізу.
INKS	Технології на основі чорнила зазвичай використовуються для автентифікації продукту, але вони також можуть використовуватися для ідентифікації та відстеження, якщо унікальний ідентифікаційний код продукту міститься в маркуванні.
IR-Sensitive Inks (Infrared)	Чорнила, чутливі до інфрачервоного випромінювання, абсолютно невидимі неозброєним оком і повинні бути виявлені спеціальним інфрачервоним зчитувачем. Вони застосовні до всіх типів матеріалів і використовуються для захисту від підробок, щоб запобігти несанкціонованому фотокопіюванню. Одне з найпоширеніших застосувань чутливих до інфрачервоного випромінювання чорнил — це приховування штрих-кодів або запобігання їх відтворенню.

Anti-Counterfeiting Technology Guide містить й інші технології маркування для захисту від підробок, які не продемонстровано в цьому Огляді.

III. ХІМІЧНІ ТА ФІЗИЧНІ ТЕХНОЛОГІЇ

Хімічні та фізичні технології боротьби з підробкою використовують спеціальні речовини для маркування та перевірки об'єктів. Вони використовують притаманну випадковість візерунків, які утворюються, коли певні хімічні процеси або речовини застосовуються до матеріалів, які служать маркерами.

Хімічні та фізичні технології для захисту від підробок	
DNA Coding	DNA Coding імплантує унікальний ДНК-код у продукт або упаковку, роблячи його відстежуваним, ідентифікованим та перевіреним. Ця технологія сумісна з усіма типами матеріалів і тому може застосовуватися до найрізноманітніших продуктів.
Chemical Encoding and Tracers	Ця технологія захисту від підробок використовує мініатюрні частинки зі специфічними хімічними або фізичними властивостями для автентифікації та захисту продуктів і упаковки. Ці частинки можуть бути прикріплені до будь-якого типу поверхні та невидимі неозброєним оком.
Glue Coding	Клейове кодування – це процес нагрівання полімеру, що призводить до утворення в ньому спонтанних, випадкових і унікальних бульбашок. Конкретне розташування, розмір і форма полімерних бульбашок щоразу різні, що робить кожну конкретну комбінацію унікальною. Кожен набір бульбашок записується в базу даних до якої має доступ лише власник продукту. Тому ці унікальні тривимірні візерунки практично неможливо повторити, що робить їх ідеальними для захисту та виявлення підробок.
Surface Fingerprint & Laser Surface Analysis	Поверхня кожного продукту може бути унікальною завдяки мікроскопічним структурним відмінностям, викликаним фізичними процесами або використанням хімічних речовин. Ця технологія використовує ці відмінності, призначаючи кожному код у випадковій і стабільній формі, як відбиток пальця, який ідентифікує продукт. Коди записуються в бази даних, на які можна посилатися, щоб перевірити автентичність продукту.

Таким чином, існує чотири типи хімічних і фізичних технологій. Їхня основна мета – автентифікація без одночасної унікальної ідентифікації продукту.

Слід зауважити, що для зчитування та перевірки маркерів, які вони створюють, потрібне спеціалізоване обладнання або лабораторні тести. Це дуже ускладнює відтворення подібних маркувань третіми особами. Витрати, пов'язані зі створенням і нанесенням хімічних і фізичних маркерів, як правило, невеликі. Однак спеціалізовані автоматичні зчитувальні пристрої, коли вони потрібні, можуть бути дорогими. Тому варто мати на увазі, що негайна перевірка на місці часто неможлива. Замість цього тестування доводиться проводити в лабораторіях, що вимагає більше часу.

IV. МЕХАНІЧНІ ТЕХНОЛОГІЇ

Механічні технології працюють з фізичними властивостями матеріалів, щоб запобігти підробці та створити ефективні бар'єри для захисту від несанкціонованого доступу.

Механічні технології для захисту від підробок	
Labels	Ідентифікаційна етикетка – це будь-який фізичний елемент, що містить ідентифікаційні дані та інформацію про товар і розміщується на товарі або його упаковці. Вони є ефективним способом ідентифікації продуктів, особливо в поєднанні з іншими елементами безпеки, такими як штрих-код або голограма.
Laser Engraving	Ця технологія використовує особливий тип лазера для вирізання дуже близько розташованих канавок різної глибини на будь-якому типі опори чи поверхні. Зображення, логотипи, текст або ідентифікаційні коди можуть бути накладені поверх гравіювання, де вони набудуть нових кольорів при розгляді під різними кутами. Основною перевагою цієї технології є те, що маркування невіддільне від продукту, тому його дуже важко підробити.
Anti-Alteration Devices	Пристрої захисту «механічно» запобігають зміні продукту в його оригінальній упаковці. Хоча специфічні пристрої потенційно можуть бути виготовлені для всіх типів продукції, найпоширенішим прикладом є кришка, що запобігає переливанню, або кришка, що запобігає повторному наповненню.
Seals	Пломба або печатка – це будь-який пристрій, який герметично закриває упаковку, щоб захистити вміст від несанкціонованого доступу. Зазвичай їх легко встановлювати та знімати, але рівень безпеки, який вони пропонують, значною мірою залежить від досвіду та здібностей особи, яка їх перевіряє.
Security Threads	Захисні нитки – це нитки з різних матеріалів (металу, тканини, полімерів), які вплітаються у вироби або прикріплені до них іншим чином, щоб уможливити автентифікацію та запобігти несанкціонованому доступу до них.
Security Film	Основна мета цієї технології – захистити дані, надруковані на документах та упаковці. Для цього використовується тиск або тепло для нанесення пластикової плівки на сторінки або інші поверхні, які потрібно захистити. Для додаткового захисту поліетиленова плівка має спеціальні захисні елементи, вбудовані в процес її нанесення, наприклад, друковані, тактильні або кольорові елементи – для додаткового захисту.

При самостійному використанні механічні технології виконують прості функції автентифікації. У поєднанні з іншими технологіями, вони також можуть виконувати функції ідентифікації та відстеження. Наприклад, унікальні ідентифікаційні коди можуть бути включені в етикетку, щоб можна було відстежити продукт.

V. ТЕХНОЛОГІЇ ЗАХИСТУ ВІД ПІДРОБОК ДЛЯ ЦИФРОВИХ МЕДІА

Технології захисту від підробок, призначені для використання з цифровими носіями, по суті, складаються з різних методів вбудовування та ідентифікації інформації в цифрові файли, комп'ютери та електронні пристрої з метою захисту, ідентифікації та відстеження їхнього змісту, що є об'єктом інтелектуальної власності.

Технології захисту від підробок для цифрових медіа	
Digital Rights Management (DRM) Systems	Системи DRM контролюють, хто отримує доступ до цифрового контенту та використовує його.
Digital Watermarks	Водяні знаки – один з найстаріших методів автентифікації, добре відомий завдяки використанню на фізичних продуктах, таких як паперові гроші. Тепер водяні знаки існують і в цифровому світі. Наприклад, відео, придбане на вебсайті відео на вимогу (VOD), матиме персоналізований водяний знак, який містить ідентифікатор клієнта, що дозволяє відстежувати несанкціоноване розповсюдження захищеного авторським правом контенту.
Hashing	Хешування – це процес, який використовує алгоритм для створення унікального ідентифікатора – «хешу», для файлу на основі його даних. Два однакових файли завжди матимуть однаковий хеш. Аналогічно, два різних файли завжди матимуть різні хеші, навіть якщо різниця між ними мінімальна. Хеші файлів, які порушують авторські права, можуть бути додані до «чорних списків», які можуть використовуватися хмарними сервісами для виявлення, блокування та видалення несанкціонованих файлів.
Fingerprinting	Цифрові відбитки фіксують та реєструють ідентифікаційні ознаки, які є унікальними для конкретного цифрового файлу. Цей метод був прийнятий на сайтах для обміну відео, щоб дозволити авторам створювати цифрові відбитки своїх оригінальних відео. Ці відбитки потім зберігаються в довідковій базі даних. За допомогою спеціального програмного забезпечення аналізується кожен новий або невідомий контент, генеруються відбитки, які порівнюються з усіма, що зберігаються в базі даних, щоб виявити збіг і виявити незаконне використання.

Отже, існує чотири типи технологій захисту від підробок для цифрових медіа, які поділяються на дві основні категорії: системи управління цифровими правами (DRM) та технології автоматичного розпізнавання контенту.

VI. ТЕХНОЛОГІЯ СПІЛЬНОГО РЕЄСТРУ ДЛЯ ЗАХИСТУ ВІД ПІДРОБОК (БЛОКЧЕЙН)

Технологія спільного реєстру для захисту від підробок забезпечує надійний засіб відстеження всіх транзакцій, які відбуваються по всьому ланцюгу постачання, від виробництва до торгового залу. Вона побудована на основі децентралізованої однорангової системи і є, по суті, базою даних (реєстром) перевірених обмінів активами, яка зберігається одночасно на всіх комп'ютерах, підключених до мережі. Блокчейн – найвідоміша форма технології спільного реєстру.

Слід зауважити, що блокчейн все ще є досить новою технологією, однак деякі рішення вже використовуються для боротьби з підробками. Такі рішення дозволяють компаніям створювати власні ідентифікатори продукції та контролювати власні ланцюги постачання.

Єдиного стандарту використання блокчейну для боротьби з підробками не існує, але приклади можна знайти в таких секторах, як предмети розкоші, діаманти, агропродовольча галузь, електроніка та фармацевтика.

Блокчейн-системи класифікуються за доступністю (публічні або приватні) та можливістю редагування (з дозволом або без дозволу).

Публічний блокчейн	У публічних блокчейнах, що не потребують дозволу, будь-хто може брати участь у мережі, читати і записувати дані без необхідності отримання дозволу. Ці блокчейни за своєю суттю є прозорими, оскільки всі дії в мережі повинні бути підтверджені всіма учасниками і бути видимими для них. Будь-яка дія, невидима для всіх учасників, не може бути належним чином підтверджена. У публічних блокчейнах з дозволом будь-хто може читати дані, але тільки обрані учасники можуть їх записувати.
Приватний блокчейн	У приватних блокчейнах для приєднання та участі в мережі потрібен дозвіл. Учасникам можуть бути надані дозволи на читання та запис. Така можливість надавати учасникам мережі різноманітні дозволи особливо корисна в таких сферах, як охорона здоров'я, де певні дії та інформація повинні залишатися приватними, але де учасники отримують вигоду від безпеки спільної інфраструктури.

Щодо витрат, то основними факторами, що впливають на них, є тип використовуваної мережі блокчейн (публічна чи приватна), а також обсяг і розмір транзакцій. Блокчейн дозволяє економити гроші в інших сферах. Оскільки рішення на основі блокчейну забезпечують безперебійне та безпечне виконання контрактів і платежів без залучення третіх осіб, вони усувають витрати на перевірку третьою стороною та транзакційні витрати, пов'язані з поточними фізичними процедурами укладання контрактів і здійснення платежів.

VII. СТАНДАРТИ ISO ДЛЯ ТЕХНОЛОГІЙ ЗАХИСТУ ВІД ПІДРОБОК

International Organization for Standardization, ISO – це Міжнародна організація зі стандартизації. Вона базується в Женеві і є найбільшим у світі міжнародним органом зі стандартизації, що видає технічні стандарти, які охоплюють майже всі галузі. Її членами є національні органи стандартизації більшості країн світу.

Стандарти ISO – це набори правил і критеріїв, які були узгоджені експертами на міжнародному рівні. Вони бувають різних форм (наприклад, стандарти на продукцію), але за своєю суттю стандарти ISO – це фактично формули, які описують «найкращий спосіб зробити щось». Вони нумеруються у форматі «ISO nnnn:yyyy – назва», де nnnn – номер стандарту, yyyy – рік публікації, a title – назва стандарту.

Існує низка стандартів ISO, спрямованих на забезпечення відповідності технологій захисту від підробок поставленим цілям. Більшість з них орієнтовані на постачальників технологій і містять критерії щодо розробки та впровадження рішень. Однак є два стандарти ISO, які призначені для користувачів.

- ISO 22383:2020 – набір настанов, які допомагають підприємствам вирішити, яке рішення для автентифікації підходить саме їм, визначаючи критерії продуктивності та надаючи методи оцінки ефективності;
- ISO 22384:2020 – набір настанов, що допомагають брендам розробити та контролювати план захисту своєї продукції від різних видів шахрайства, таких як підробка, копіювання, сірий ринок тощо.

При цьому більшість стандартів ISO щодо технологій боротьби з підробками містять настанови, орієнтовані на постачальників технологій, а не на користувачів. Два стандарти, які є найбільш актуальними для цілей Посібника, мають на меті встановити загальні правила та критерії, щоб сприяти розробці та впровадженню рішень, які є сумісними, а отже, мають ширше застосування.

Підсумовуючи, зазначимо, що з появою нових можливостей, які відкриваються завдяки глобалізації, для підприємств будь-якого розміру стає все більш важливим розуміння повного спектра інструментів, які вони мають у своєму розпорядженні для захисту від порушень у сфері інтелектуальної власності.

Ринок технологій для боротьби з підробками і піратством є широким і складним. Технології швидко розвиваються, а інформація про них не є легкодоступною. Саме тому Центр спостереження з питань порушень прав інтелектуальної власності вбачає актуальність та цінність у проаналізованому Посібнику з технологій боротьби з підробками (Anti-Counterfeiting Technology Guide) і рекомендує правовласникам, новаторам, бізнесу звертатися до нього у своїй практичній діяльності.

Адже Посібник охоплює основні типи технологій захисту від підробок на ринку, дає чітке визначення кожного з них, описує їхні основні характеристики та стисло викладає практичні вимоги до впровадження.