

Технические науки

УДК 004.6

Бичков Сергій Олександрович

судовий експерт

Харківський науково-дослідний

експертно-криміналістичний центр МВС України

Бычков Сергей Александрович

судебный эксперт

Харьковский научно-исследовательский

экспертно-криминалистический центр МВС Украины

Bychkov Sergey

Forensic Expert

Kharkiv Research Forensic Center of the

Ministry of Internal Affairs of Ukraine

Макарук Катерина Євгенівна

судовий експерт

Харківський науково-дослідний

експертно-криміналістичний центр МВС України

Макарук Екатерина Евгеньевна

судебный эксперт

Харьковский научно-исследовательский

экспертно-криминалистический центр МВС Украины

Makaruk Ekaterina

Forensic Expert

Kharkiv Research Forensic Center of the

Ministry of Internal Affairs of Ukraine

**ЗАХИСТ ГРАФІЧНИХ ЗОБРАЖЕНЬ ВІД КОПІЮВАННЯ В МЕРЕЖІ
ІНТЕРНЕТ**

ЗАЩИТА ГРАФИЧЕСКИХ ИЗОБРАЖЕНИЙ ОТ КОПИРОВАНИЯ В СЕТИ ИНТЕРНЕТ

PROTECTION OF GRAPHIC IMAGES FROM COPYING ON THE INTERNET

Анотація. Рекомендації щодо методів захисту від копіювання авторських графічних зображень, що розміщуються в мережі Інтернет.

Ключові слова: захист від копіювання, авторські зображення, анкор-листи, метадані, водяний знак, контекстне меню, кросспостінг.

Аннотация. Рекомендации по методам защиты от копирования авторских графических изображений, размещаемых в сети Интернет.

Ключевые слова: защита от копирования, авторские изображения, анкор-листы, метаданные, водяной знак, контекстное меню, кросспостинг.

Summary. Recommendations on methods of copy protection of copyright graphic images posted on the Internet.

Key words: copy protection, copyright images, anchor lists, metadata, watermark, context menu, cross-posting.

Постановка проблеми. Проблема захисту авторства при розміщенні графічних елементів на сторінках в мережі Інтернет виникла при багаторазових крадіжках зображень з унікальних інтернет ресурсів, які мають високий рейтинг і позиціонують себе в пошукових системах по цільових запитах авторських зображень і дизайнерських проектів [1].

Високоякісні авторські фото, отримані при використанні професійних камер, картинки з додатковими елементами обробки в спеціальних дорогих програмах для роботи з зображеннями, необхідно захищати від копіювання для запобігання їх використання на інших ресурсах.

Мета дослідження. Огляд деяких способів захисту графічних зображень від копіювання, які розміщуються в мережі Інтернет. Плюси і мінуси кожного з методів захисту.

Основний матеріал.

Використання засобів пошукових систем Google

Компанія Google дуже уважно ставиться до захисту інтелектуальної власності та пропонує користувачам сервісу кілька методів захисту свого контенту на сторінках Інтернет. Наприклад, використання оптимізації сайтів за допомогою створення анкор-посилань для фіксації унікального контенту сайту або використання зв'язки з Google бізнес - аккаунтом [4].

Алгоритми індексування пошуковими роботами при створенні анкор - посилань, або анкор-листів для опису зображення, ефективно фіксують джерело походження інформації. Для створення анкор-посилань необхідно написати унікальні частини тексту на сторінках сайту, відзначити їх як анкор-посилання. Пошукові боти Google при індексації відзначають матеріал веб сторінок, як першоджерело.

Бізнес-акаунт в системі Google допомагає зв'язати будь-яке зображення з корпоративними авторськими підписами. В налаштуваннях профілю вказуються посилання на джерела для підтвердження авторства. Відповідно, на веб сторінках, які потребують захисту авторства зображень, повинні бути посилання на профіль Google аккаунта.

Однак, сервіси Google працюють над захистом авторського права через бізнес-профіль тільки для корпоративних клієнтів, а не для простих фізичних осіб.

Захист авторства за допомогою фіксації метаданих зображень

Метадані EXIF (Exchangeable Image File Format), які прив'язані до властивостей графічного файлу, містять відомості про модель камери, її виробника, про дату і час створення знімка, витримки і діафрагми. Ці дані створюються автоматично при перетворенні необробленого «RAW-формату»

цифрового фотоапарата в будь-який інший графічний формат, наприклад, «JPEG формат», «TIFF формат» і подальшого запису файлу фотозображення. Автору необхідно лише мати певні навички роботи з графічними редакторами, щоб додати до метаданих унікальну інформацію про себе.

Якщо автор знімка має досвід роботи з IPTC редактором, він може зробити пакетну обробку необробленого фотоматеріалу, без вказівки основних технічних параметрів, а лише відзначаючи своє авторство на кожному знімку.

Однак, слід враховувати, що існує безліч редакторів метаданих, і досвідчений користувач може легко змінити вже існуючі метадані на будь-які інші, що сильно ускладнює встановити оригінал графічного файлу.

Накладення водяного знаку на зображення

Прозоре накладення водяного знаку на зображення у вигляді підпису, напису або логотипу - один із зручних способів захисту зображення від копіювання на веб порталі.

Водяний знак можна накласти за допомогою різних графічних редакторів, таких як: Adobe Photoshop, Watermark [2; 3].

Таке програмне забезпечення, як Digimarc, кодує водяний знак у візуальний «шум», який можна розглянути тільки за допомогою спеціального програмного забезпечення.

Досить важко позбутися на зображенні від водяного знаку, навіть маючи досвід роботи з професійними графічними редакторами. У деяких випадках складність видалення водяного знаку з зображення може перевищити цінність самого зображення.

Однак, останнім часом зазначений метод захисту графічних зображень в Інтернеті стає менш популярним через те, що водяний знак псує саме зображення і автори намагаються уникати такого захисту.

Заборона контекстного меню, прозоре зображення або порожній файл замість картинки

Контекстне меню картинки дає кілька варіантів для копіювання фото, а саме: «Зберегти зображення як ...» або «Копіювати URL картинки».

Змінюючи код веб сторінки за допомогою JavaScript, jQuery, CSS, плагінів AntiCopy (для Joomla) або No Right Click Images Plugin (для WordPress), можна відключити контекстне меню для всіх унікальних зображень на сайті або цілому веб порталі [4].

Зазначений метод захисту зображень дуже часто зустрічається на сайтах інтернет-магазинів відомих брендів.

Такий захист авторства досить надійний і для користувача з невеликим досвідом роботи з програмами може стати серйозною перешкодою при завантаженні чужих графічних зображень з Інтернету. Недосвідченого в інформаційних технологіях користувача такий захист може зупинити і переконає його відмовитися від ідеї завантажити графічне зображення, авторство якого захищено таким чином.

Автори унікальних творчих зображень часто використовують спеціальний графічний редактор Adobe Photoshop, який дозволяє створити прозоре зображення одного розміру, що і оригінал і накласти цей шар-зображення на передній план картини за допомогою засобів «html-редакторів» або «стилів css». В результаті чого, використовуючи контекстне меню графіки, зберігається лише верхній прозорий шар без авторського зображення [2; 3].

За допомогою плагіна Photo Protect зображення можна покрити невидимим шаром (накладенням) і при збереженні картини з сайту сторінки відкривається лише порожній файл.

Досвідчені користувачі можуть обійти зазначені методи захисту шляхом завантаження контенту сайту з використанням стороннього програмного забезпечення або вилучити необхідне графічне зображення з кешу веб-браузера,

або просто зробити «скріншот» екрану з необхідним графічним зображенням і обробити його графічним редактором при необхідності.

Анонсування або кросспостінг

Розміщення анонсів за допомогою спеціальних програм Best Persons, Piston Poster або анонсування вручну на сторонніх сайтах, соціальних мережах або веб-ресурсах своїх майбутніх публікацій допомагає захистити авторство ще до створення унікальних сторінок із зображеннями [4].

Такий метод захисту підходить для зображень, які мають художню цінність, смислове навантаження і не використовуються в комерційних цілях.

З точки зору на захист авторських прав графічних зображень, що несуть художнє смислове навантаження, цей метод є одним з істотних і може діяти на попередження крадіжки контенту сайту.

Висновки, рекомендації. Оглядом наведених методів можна зробити висновок, що всі наведені засоби захисту авторських прав графічних зображень мають як переваги, так і недоліки, крім того, деякі методи можна застосувати до графічних зображень в мережі Інтернет, а інші безпосередньо до самого графічного файлу.

Як і у всіх сучасних системах, захисту авторського права або системи безпеки, завжди рекомендується одночасно вибирати декілька методів захисту.

Від авторів статті, з приводу захисту авторського права графічних зображень, рекомендується створення сервісу, принцип роботи якого полягав би в тому, що автор зображення завантажує до сервісу графічне зображення, безпосередньо сервіс розраховує хеш-суму файлу за відомими хеш-алгоритмами (наприклад, MD5, SHA1, SHA256 і т.д.) і публікує в базі даних розрахований хеш графічного зображення, дату публікації, відомості про авторів та безпосередньо оригінал файлу. Що в подальшому зможе виступати як додаткове джерело встановлення авторства графічного зображення.

Література

1. Каневский Сергей. Защита авторских прав в сети Интернет. ЛитРес: Самиздат, 2019. 97 с.
2. Божко А.Н. Photoshop CS. Ретушь и коррекция изображений. М. «ДЕСС КОМ», 2002. 400 с., ил
3. Айсманн К., Палмер У. Ретуширование и обработка изображений в Photoshop. М.: Издательский дом "Вильямс", 2008. 560 с. + 40 с. цв. ил. (3-е изд.)
4. Ашманов Игорь, Иванов Андрей Оптимизация и продвижение сайтов в поисковых системах / 3-е издание, ISBN: 978-5-459-00737-4, 2012. 463 с.