ОСОБЛИВОСТІ ЗАХИСТУ ГРАФІЧНИХ ЗОБРАЖЕНЬ

Катерина Євгенівна МАКАРУК,

головний судовий експерт відділу комп'ютерно-технічних та телекомунікаційних досліджень Харківського науково-дослідного експертно-криміналістичного центру МВС України

Використання засобів пошуку Google. Google дуже уважно ставиться до захисту інтелектуальної власності і 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-акаунтом [1, 2].

Алгоритми індексування пошуковими роботами при створенні анкор-посилань, або анкор-аркушів 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 роботи Google при індексації відзначають матеріал веб сторінок, як першоджерело.

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 та час створення знімка, витримки та діафрагму. Ці дані створюються автоматично при перетворенні необробленого "RAW-формату" цифрової фотоапарата в будь-який інший графічний формат, наприклад, "JPEG формат", "TIFF формат" та наступного 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 редактором IPTC, 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 метадані, що вже існують, на будь-які інші, що сильно ускладнює встановити оригінал графічного файлу.

Накладення водяного знака на зображення. Прозоре накладення водяного знака на зображення у вигляді підпису, напису чи 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 [3, 4].

Такий програмний додаток, як Digimarc, кодує водяний знак у візуальний шум, який можна розглянути тільки за допомогою спеціального програмного забезпечення.

Досить важко позбутися зображення від водяного знака, навіть маючи досвід роботи з професійними графічними редакторами. У деяких випадках складність видалення водяного знака із 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 картинку як..." або "Копіювати URL-адреси картинки".

Змінюючи код веб-сторінки за допомогою JavaScript, jQuery, CSS, плагінів AntiCopy (для Joomla) або No Right Click Images Plugin (для WordPress), можна вимкнути контекстне меню для всіх унікальних зображень на сайті або в цілому веб порталі [2].

Зазначений метод захисту зображень 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 для завантаження чужих графічних зображень з Інтернету. Недосвідченого в інформаційних технологіях користувача такий захист може зупинити та переконає його відмовитися від ідеї завантажити графічне зображення, авторство якого захищене 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 картинки за допомогою засобів "html редакторів" або "стилів css". Згодом, використовуючи контекстне меню графіки, зберігається лише прозорий верхній шар без авторського зображення [3, 4].

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

Досвідчені користувачі можуть обійти зазначені захисту шляхом завантаження контенту сайту з використанням стороннього програмного забезпечення або вилучити необхідне графічне зображення з кешу веб-браузера, або просто зробити екран екрана з необхідним графічним зображенням і обробити його графічним редактором при необхідності.

Анонсування чи кроспостинг. Розміщення анонсів за допомогою спеціальних програм Best Persons, Piston Poster або анонсування вручну на інших сайтах, соціальних мережах або веб-ресурсах своїх майбутніх публікацій допомагає захистити авторство ще до створення унікальних сторінок із зображеннями [2].

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

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

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 чи системи безпеки, завжди рекомендується одночасно вибирати кілька методів захисту [5].

Виходячи з викладеного вище, зауважимо, що до захисту авторського права графічних зображень рекомендується створення сервісу, принцип роботи якого полягає у тому, що автор зображення завантажує до сервісу графічне зображення, безпосередньо сервіс розраховує хеш-суму файлу з відомими хеш-алгоритмами (наприклад, MD5, SHA1, SHA256 і т.д.). Потім публікує в базі даних розрахований хеш графічного зображення, дату публікації та відомості про авторів, що надалі зможе виступати як додаткове джерело встановлення авторства графічного зображення.

Список використаних джерел:

1. Каневский Сергей. Защита авторских прав в сети Интернет/ЛитРес: Самиздат, 2019. 97 с.

2. Игорь Ашманов, Андрей Иванов. Оптимизация и продвижение сайтов в поисковых системах/3-е издание, 2012. 463 с.

3. Божко А.Н. Photoshop CS. Ретушь и коррекция изображений/ М. “ДЕСС КОМ”, 2002, 400 с., ил

4.Айсманн К., Палмер У. Ретуширование и обработка изображений в Photoshop/ М.: Издательский дом "Вильямс", 2008. 560 с. + 40 с. цв. ил. (3-е изд.)

5. Макарук К.Є. Бичков С.О. Захист графічних зображень від копіювання в мережі Інтернет. Міжнародний науковий журнал “Інтернаука” №18 (98)/2020, 1 том, 75 с.