

*Мазуренко Світлана Вікторівна,
кандидат юридичних наук, доцент,
доцент кафедри права інтелектуальної власності та корпоративного права
Національного університету «Одеська юридична академія»*

ТЕХНІЧНІ СПОСОБИ ЗАХИСТУ АВТОРСЬКИХ ПРАВ У МЕРЕЖІ ІНТЕРНЕТ

Широке розповсюдження у цифрових мережах копій об'єктів авторського права потребує їхньої ідентифікації, що зумовлено необхідністю виявлення легальних та нелегальних копій. Для правовласників та посередників (Інтернет- та хостинг-провайдерів) така ідентифікація полегшить протидію розповсюдженню піратського цифрового контенту, який необхідно виявляти.

Недостатня увага до використання засобів ідентифікації цифрового контенту призводить до ситуації, коли всі категорії зазначених суб'єктів зазначають певних втрат: правовласники не здатні оцінити реальні обсяги цифрового піратства, а також статистику використання об'єктів авторського права у мережі Інтернет; провайдери не в змозі сприяти правовласникам у протидії піратству, оскільки практично не можливо вести ефективний моніторинг не ідентифікованого контенту; користувачі не завжди усвідомлюють використання ними піратських музичних, відео- та текстових файлів.

Використання окремих технологічних засобів дозволяє ідентифікувати комп'ютер порушника. Важливо ідентифікувати піратські веб-сайти в Інтернеті та застосовувати до них певні обмеження у разі юрисдикційних та інших труднощів закриття або інші законні санкції. Так, нещодавно компанія Google оголосила про обмеження виведення пошукових результатів стосовно піратських сайтів та контенту не лише у власній пошуковій системі, але й у сервісі YouTube. Інше нововведення Google має позбавити ресурси з нелегальним вмістом основного джерела доходу – реклами. Тепер компанія відстежуватиме піратські сайти, на яких демонструється реклама AdSense, і розриватиме відносини з ними [1].

Щодо застосування передбачених міжнародним та вітчизняним законодавствами засобів ідентифікації та захисту цифрового контенту, який містить об'єктів авторського права, у відповідних правових актах застосовуються такі поняття, як засоби технологічного захисту (technical protection measures, TPM), інформація про управління правами (rights management information, RMI), цифрове управління авторськими правами (digital rights management, DRM).

Стаття 1 Закону України «Про авторське право і суміжні права» розкриває зазначені поняття, зокрема: інформація про управління правами – інформація, в тому числі в електронній (цифровій) формі, що ідентифікує об'єкт авторського права і (або) суміжні права і автора чи іншу особу, яка має на цей об'єкт авторського права і (або) суміжних прав, або будь-які цифри чи коди, у яких представлена така інформація, коли будь-який із цих елементів інформації прикладений до примірника об'єкта авторського права і (або) суміжних прав з його повідомленням до загального відома; технічні засоби захисту – технічні пристрої і (або) технологічні розробки, призначені для створення перешкоди порушенню авторського права і (або) суміжних прав при сприйнятті та (або) копіюванні захищених (закодованих) записів у фонограмах (відеограмах) і передачах організації мовлення чи для контролю доступу до використання об'єктів авторського права і суміжних прав.

Варто зазначити, що і традиційні засоби ідентифікації суб'єктів та об'єктів авторського права можуть успішно застосовуватись в Інтернеті. Так стаття 11 Закону України «Про авторське право і суміжні права» передбачає, що за відсутності доказів іншого автором вважається особа, зазначена як автор на оригіналі або примірнику твору (презумпція авторства) [1].

Особа, яка має авторське право (автор твору, чи будь-яка особа, якій на законних підставах передано майнове право на цей твір), для сповіщення про свої права може використовувати знак охорони авторського права. Цей знак складається з наступних елементів: латинська літера «с», обведена колом, – ©; ім'я особи, яка має авторське право; рік першої публікації твору.

Це повідомляє користувачу певні реквізити (найменування) правовласника, що спрощує його пошук, або, попереджає про те, що об'єкт в Інтернеті є об'єктом авторського права та, теоретично, стримує від його незаконного використання. Що стосується використання засобів технічного захисту, то тут не припиняються суперечки щодо ефективності та, в окремих випадках, правомірності їх застосування.

Було б ідеально, якби наприклад, усі електронні копії музичних (mp3, ogg, FLAC тощо), аудіовізуальних (avi, mkv, divx тощо), літературних (doc, pdf, rtf тощо) творів мали обов'язкові ідентифікатори, які засвідчували б правомірність та умов використання, тоді боротьба з піратством у цифровому середовищі була б набагато ефективнішою. Але обов'язку застосування в Інтернеті таких ідентифікаторів за аналогією з контрольними марками на фізичних примірниках законодавством (як міжнародним, так і національним не передбачено) (хоча пропозиції щодо введення «електронних контрольних марок лунають»). Тобто застосування RMI, DRM, TPM залишається на розсуд

правовласників. На початку цифрової ери неналежна увага з боку правовласників призвела до невігідних для них тенденцій. Зокрема, під час появи ефективного щодо співвідношення розмір/якість формату «mp3» менеджери музичної індустрії вважали його піратським, але за популярністю він став де-факто стандартом для музичних плеєрів. Цей формат має програмні засоби ідентифікації (текстова частина ID3 Tag), але позбавлений засобів жорстокого обмеження від неконтрольованого копіювання.

Варто зазначити, що кожний потужний бізнес цифрової дистрибуції прагне запровадити власні захищені формати файлів, які, крім того, пов'язані з конкретним обладнанням. Наприклад, компанія Apple використовує у своїх плеєрах (iPod) та онлайн-сервісі (iTunes) власні аудіо- та відеоформати, захищені від копіювання. Варто відмітити, що в свій час iTunes разом з iPod виступили свого роду «панацеєю» музичної індустрії, яка сильно страждала від Інтернет-піратства, зокрема Napster [2]. На ринку електронних книг «захищені» формати також розвивають деякі сервіси (наприклад сервіс Amazon та програмно-апаратний засіб для читання Kindle).

Деякі правовласники віддають перевагу захисту не контенту, а носіїв інформації. Так, для DVD-дисків діє регіональна система захисту, яка покликана вирішити проблему розповсюдження дисків у країнах, де прем'єра фільму ще не завершилася та він не вийшов на DVD. Ідея полягає в тому, що кожен диск кодується певним номером регіону (наприклад, 1 для США та Канади). Також аналогічний код встановлюється на оптичні прилади, які продаються в даному регіоні. При розбіжності кодів DVD не буде зчитуватись. Окрім засобів DRM, можна зазначати ще й інші, більш побутові засоби захисту та контролю за авторськими правами.

Перш за все, автор може банально в рядку пошуку ввести певне словосполучення чи речення. В результаті буде отримано список веб-сторінок, що містять даний фрагмент тексту, включаючи і сторінку-першоджерело. Далі, можуть застосовуватись спеціальні засоби (програмні та апаратні, які або зовсім не дозволяють скопіювати та/або зберегти ресурс, або обмежують можливості копіювання, якщо не виконуються умови використання ресурсу, визначені його власниками).

До них можна віднести: блокування правої кнопки миші. Це є найбільш класичним засобом захисту контенту сайту. Він полягає в тому, що при натисненні правої кнопки миші, завдяки спеціальному скрипту, видається попереджувальне повідомлення; заборона видалення об'єкта за допомогою миші. Ці два засоби виступають базовими, оскільки зазвичай для копіювання використовується саме миша; заборона копіювання. Оскільки копіювання

можливо не лише завдяки миші, але й завдяки комбінації клавіш на клавіатурі (наприклад, ctrl+c), то блокування копіювання взагалі, може служити в певній мірі безпечним заходом.

Для захисту зображень додатково можна застосовувати такі заходи як: створення «листкової» картинки. Ідея полягає в тому, щоб дозволити користувачу копіювати зображення, але не що він бачить, а, наприклад, прозору, що знаходиться зверху неї; розміщення на зображенні будь-якого текст або інформації про автора/власника зображення (на усіх фотографіях Лондона на сайті www.picturesoflondon.com є фоновий текст: «Порушення авторських прав, будь ласка, звернутись за адресою www.picturesoflondon.com«).

Слід звернути увагу, що зображення неможливо захистити від копіювання завдяки кнопки PrintScreen, яка робить копію усього екрана на момент натиснення. Тому рекомендується публікувати зображення у якість, задовільній для ознайомлення, але неприйнятним для комерційного використання. Наприклад, карикатурист Олександр Зудін на своєму сайті на усіх малюнках спеціально додав тінь та обрав невеликий розмір зображення, та запропонував для придбання зображення звернутися до автора (<http://cartoon.ru/about/copyright>)

Для більш складних об'єктів цифрового авторського права як, наприклад, комп'ютерні програми чи ігри також використовують технічність засоби захисту, зокрема, DRM. Так, вони можуть вимагати наявність диска у оптичному приводі комп'ютера, вимагають введення ключа або реєстрації через Інтернет. Наприклад, компанія Edios, видавець відеогри Batman: Arkham Asylum, вигадала новий спосіб боротьби з піратами – у неліцензійній версії Бетмен не вміє літати. У результаті, як повідомляє PC Advisor, з проекту зникає можливість доступу до деяких частин ігрового світу, оскільки до них можливо дістатись за допомогою польоту головного героя на своїх штучних крилах, а без них він гине. У відповідь на скарги гравців компанія Edios зробила офіційну заяву, у якій відзначила, що це не програмна помилка, а спеціально створений захист. Один з працівників Edios зазначив: «Це помилка не в грі, а у вашому моральному відношенню до авторського права». На сьогодні, як правило, технічні засоби захисту авторських прав у цифровому середовищі вважають більш ефективними ніж юридичні, в силу свого превентивного характеру та тим, що, як правило, вимагає спеціальних знань та навичок для здійснення несанкціонованої копії.

Не зважаючи на це, було б несправедливим не зазначити про існування певної критики цих засобів захисту, зокрема DRM. Так, вважається що ці

обмеження в певній мірі звужують права в перш за все чесних споживачів. Прикладом може виступати музика, придбана у магазині Apple iTunes, яку неможливо прослухати на інших плеєрах окрім iPod. Також, в певних випадках засоби захисту від взлому можуть негативно вплинути на роботу операційної системи користувача. Як вже зазначалось, деякі DRM вимагають Інтернет-з'єднання з контролюючою системою (на сьогодні це один з ефективних засобів). Проблема полягає в тому, що компанія може припинити підтримку серверу, контент стає марним. Наприклад, у 2008 році Microsoft вирішила закрити більш не дійсний MSN Music Store та вимкнути сервери, необхідні для отримання ключів до раніше придбаних музичних творів, після чого користувачі були б не в змозі відтворювати їх після заміну комп'ютера. Однак, після численних скарг, Microsoft продовжила строк дії серверів до 2011.

ЛІТЕРАТУРА:

1. Google посилює боротьбу з піратством [Електроний ресурс]. – Режим доступу до ресурсу: <http://intelpro.ua/uk/google/google-posylyue-borotbu-z-piratstvom>
2. Закон України «Про авторське право і суміжні права» // Відомості Верховної Ради України (ВВР)// – 1994. – N 13. – ст.64
3. The Audienceis in formed [Электронный ресурс] – Режим доступа: <http://id3.org/>
4. Авторские права в Интернете [Электронный ресурс] – Режим доступа к ресурсу: http://www.itlt.edu.nstu.ru/copyright_internet.php.
5. Как техническими способами защитить авторские права на сайт (контент, дизайн и т.д.) [Электронный ресурс] – Режим доступа к ресурсу: <http://www.seonews.ru/masterclasses/detail/29849.php>.
6. Антіпіратські заходи / Інтелектуальна власність – № 6 – 2009 р. – с. 46.

Ключові слова: мережа Інтернет, технічні способи захисту, авторське право, ідентифікація користувачів.

Keywords: Internet, technicalprotection, copyright, useridentificatio