

ГРИГОР'ЯНЦЬ Г. І.

Національний університет «Одеська юридична академія»,
асистент кафедри права інтелектуальної власності та корпоративного права

ТЕХНІЧНІ СПОСОБИ ОХОРОНИ АВТОРСЬКИХ І СУМІЖНИХ ПРАВ ВІД ПІРАТСТВА В МЕРЕЖІ ІНТЕРНЕТ

Розвиток технічного прогресу, на жаль, має не лише позитивні наслідки, а й стає для порушників надійним помічником у незаконному відтворенні об'єктів авторського права і суміжних прав. І якщо раніше незаконно виготовлені примірники творів були продуктом не вищого гатунку, то сучасні технології дозволяють порушникам виготовляти цифрові примірники, які є ідеальними копіями оригіналів, та розповсюдження звичайних примірників, наприклад книг, аудіо- або відеоносіїв, вартість творів, що розміщені в Інтернеті, а також витрати пов'язані з їх доставкою у мережі, є незначними. Здатність порушників діяти в Інтернеті анонімно та неосвіченість більшості користувачів всесвітньої мережі з питань захисту авторського права і суміжних прав має наслідком наполегливі вимоги міжнародного співтовариства щодо активізації України у боротьбі з Інтернет-піратством [1, с. 141].

Основними та найбільш дієвими заходами захисту об'єктів авторського права і суміжних прав в мережі Інтернет ми вважаємо технічні. Позитивними моментами такого захисту є: превентивний характер – можливість захищати твір до того як правопорушення буде скоєно; ефективність – технічний захист найбільш надійний, оскільки складний у розшифруванні та цим створює перепону для піратської діяльності; вільний вибір – автори та правоволодільці самі вирішують питання надавати своїм творам такий захист чи ні. Негативними сторонами є: необхідність звертатися до осіб, які розбираються у технічних питаннях; не безкоштовний, а в деяких випадках достатньо дорогий спосіб; з появою нових способів захисту, з'являються нові способи обходити такий захист.

Програмні методи захисту є перспективними, оскільки для них характерні гнучкість у проектуванні, адаптованість до алгоритмів програм-об'єктів захисту та, порівняно з апаратними засобами, нижча вартість реалізації. До програмних методів захисту належать шифрування та заплутування, або обфускація (obfuscation) програмного коду. Такі методи ускладнюють структуру програми і, тим самим, процес зворотного або реверс-інжинірингу (reverseengineering). Не менш ефективними у боротьбі з піратством є стеганографічні методи, а саме цифрові водяні знаки, які впроваджують в коди програм для підтвердження авторських прав. Наприклад, якщо в кожен примірник програми

додати водяний знак у вигляді ідентифікаційного номера, то у випадку незаконного копіювання і розповсюдження програми можна визначити недобросовісного користувача [2, с. 82].

Характерною тенденцією у сфері захисту інформації є впровадження криптологічних методів. Однак на цьому шляху ще багато невирішених проблем, зв'язаних з руйнівним впливом на криптозасоби таких складових інформаційної зброї як комп'ютерні віруси, логічні бомби, автономні реплікативні програми, т.п. Об'єднання методів комп'ютерної стенографії і криптографії є гарним виходом з положення, що створилося. У цьому випадку можна усунути слабкі сторони відомих методів захисту інформації і розробити більш ефективні нові нетрадиційні методи забезпечення інформаційної безпеки [3, с. 108].

Для попередження піратських дій щодо об'єктів авторського права і суміжних прав в мережі Інтернет пропонується використовувати метод авторизації через Інтернет, ліцензійні угоди, цифрові водяні знаки, надання безоплатної версії програми на певний строк та програмні методи охорони (такі як шифрування та заплутування програмного коду). Більшість названих прийомів може слугувати також спрощенню процесу доказування у суді.

Можливим варіантом майбутнього регулювання відносин розповсюдження легальних примірників творів може бути система оплати безлімітного доступу до творів, яка включається до суми сплати за користування Інтернетом. Однак такий метод пов'язаний із складнощами розподілу гонорарів між правовласниками та авторами, та технічними методами захисту, які необхідно використовувати для подальшої охорони продукту.

Список використаної літератури:

1. Кетрарь А.А. Правові проблеми захисту авторських та суміжних прав від піратства в мережі Інтернет / А.А. Кетрарь // Часопис цивілістики. – 2013. – № 14. – С. 141–145.
2. Стороженко А.О. Методика захисту програмного забезпечення шляхом впровадження ЦВЗ в асемблерний код програми / А.О. Стороженко, А.Я. Горпенюк, Н.М. Лужецька // Автоматика, вимірювання та керування: [збірник наукових праць] / відповідальний редактор В.Б. Дудикевич. – Львів: Видавництво Львівської політехніки. – Вісник Національного університету «Львівська політехніка». – 2013. – № 753 – С. 80–84.
3. Навроцький Д.О. Методи комп'ютерної стеганографії / Д.О. Навроцький // Вісник Національного технічного університету України «КПІ». – 2007. – № 35. – С. 105–108.