

УДК 347.78:004.738.5

Ольга Рассомахіна,

кандидат юридичних наук,

доцент кафедри цивільного права і процесу

Юридичного інституту Національного авіаційного університету

ХАРАКТЕРИСТИКА ТЕХНІЧНИХ ЗАСОБІВ ЗАХИСТУ ОБ'ЄКТІВ АВТОРСЬКОГО ПРАВА І СУМІЖНИХ ПРАВ У МЕРЕЖІ ІНТЕРНЕТ

Стаття присвячена виявленню підходів до класифікації технічних засобів захисту авторського права і суміжних прав у мережі Інтернет та характеристиці окремих їх видів, що є актуальним у контексті дослідження питань їх правового регулювання.

Ключові слова: захист авторського права і суміжних прав, мережа Інтернет, правове регулювання, заходи і засоби захисту авторського права і суміжних прав, технічні засоби захисту.

На сьогоднішньому етапі розвитку техніки будь-яка особа може з легкістю і без значних витрат здійснювати порушення авторського права та суміжних прав у мережі Інтернет. У зв'язку із цим суб'єкти авторського і суміжних прав та інші особи використовують спеціальні технічні засоби захисту об'єктів авторського і суміжних прав у мережі, які є різноманітними. Останнім часом з'являється все більше нових таких засобів. Практика застосування даних засобів призвела до необхідності дослідження низки правових, технічних та організаційних питань, що з цим пов'язані. Одним з них є питання про види та характеристику технічних засобів захисту, підходи до їх класифікації та ефективність того чи іншого засобу, що має важливе значення для розуміння даного явища та визначення підходів до правової охорони технічних засобів захисту.

Дане питання було предметом дослідження багатьох зарубіжних та вітчизняних науковців, зокрема І. І. Ващинця [1; 2; 3], О. Недоруб [4], В. Б. Наумова [5], Е. Наумової [6], О. М. Пастухова [7] та інших. Частина із даних засобів охарактеризовано у Рекомендаціях щодо вдосконалення механізму регулювання цифрового використання об'єктів авторського права і суміжних прав через мережу Інтернет, розроблених Державною службою інтелектуальної власності [8]. Разом із тим, актуальним залишається формування системного уявлення про види технічних засобів захисту об'єктів авторського права і

суміжних прав у мережі Інтернет. Це питання є важливим у контексті дослідження питань їх правового регулювання.

Метою даної статті є виявлення підходів до класифікації засобів захисту авторського права і суміжних прав у мережі Інтернет та дослідження окремих видів технічних засобів захисту.

Заходи захисту авторського права і суміжних прав у мережі Інтернет різноманітні. Правові засоби захисту даних прав пов'язані із різного роду правочинами, встановленими законодавством способами захисту авторського права і суміжних прав, визначенням того, що є порушенням даних прав, встановленням відповідальності за відповідні правопорушення. Неправові засоби захисту авторського і суміжних прав у літературі поділяють на організаційні та технічні [9], які, в свою чергу, можуть бути організаційно-технічними, а також пов'язаними із правовими. Організаційно-правові заходи захисту авторського права і суміжних прав були розглянуті у окремій публікації автора. Слід також зазначити, що фахівці по-різному визначають приналежність заходів і засобів захисту до певного виду, тому віднесення того чи іншого засобу до певного виду може вирішуватися неоднозначно. Цікавим у цьому контексті є нещодавно запропонований пошуковою системою Google алгоритм, відповідно до якого сайти, зміст яких не порушує авторське право і суміжні права будуть з'являтися за результатами пошуку першими [10].

Поки що вітчизняні фахівці не розглядали зазначені засоби у системному вигляді, зважаючи на стрімкий розвиток технічних можливостей та появу нових засобів захисту прав у мережах. У цілому питання класифікації зазначених засобів ще не вирішено остаточно.

ВОІВ розглядає технічні засоби захисту як складову системи цифрового управління правами та виділяє серед них пристрої захисту від копіювання, контролю доступу, електронні конверти, оригінальне програмне забезпечення для перегляду, криптографічні засоби захисту, паролі, водяні знаки, системи ідентифікації користувача, системи контролю за використанням та отримання винагороди [11].

В. І. Ващинець виділяє підходи до класифікації систем, які мають на меті технічний захист об'єктів авторського права, і умовно поділяє їх на такі групи: 1) система, спрямована на захист дій, що підпадають під виключне право автора (передача публіці, зміна твору тощо), або система антикопіювання; 2) системи обумовленого доступу; 3) інструменти маркування і нанесення міток з метою вирішення проблеми розпізнавання легальних копій творів та полегшення виявлення піратської продукції; 4) електронні системи управління. І розглядає серед них не тільки ті технічні засоби, які застосовуються в мережі Інтернет [12].

У одній із робіт наводиться 24 види технологій захисту веб-сторінок та їх елементів, які застосовуються в Інтернеті [13].

Більш ґрунтовні класифікації технологічних заходів наводяться у публікаціях зарубіжних фахівців. В одному із досліджень Інституту інформаційного права Амстердамського університету з даної тематики наведено чотири категорії таких заходів: 1) ті, що контролюють доступ, зокрема технології, що контролюють доступ до мережі; технології, що контролюють доступ на рівні користувача або одержувача інформації; технології, що контролюють доступ до набутої копії твору; заходи, що запобігають подальшому доступу; 2) технології, які контролюють використання інформації; 3) технології, які захищають цілісність роботи; 4) технології, які дозволяють здійснювати облік доступу до інформації або її використання. При цьому зазначено, що вони можуть бути розмежовані і

за іншими критеріями, що на практиці дані категорії часто перетинаються і що в майбутньому можуть з'являтися інші види технологій з іншими функціями. Окремо виділяють електронні системи управління правами, які полегшують торгівлю об'єктами авторського права в мережах. Деякі фахівці розмежовують такі технологічні заходи на дві категорії: 1) ті, які запобігають незаконному перехопленню творів неуповноваженими одержувачами; 2) ті, які обмежують використання та/або наступне розповсюдження творів. Також існує поділ даних заходів на 1) ті, які можуть бути застосовані до моменту порушення прав, 2) заходи щодо стягнення плати до або в момент використання твору та 3) технології виявлення правопорушення та захисту прав після їх порушення [14].

В одній із робіт канадських фахівців зазначається, що в основі класифікації технічних засобів захисту є їх функція і що зазвичай їх поділяють на заходи контролю доступу до твору та ті, які контролюють використання творів. Разом з тим, зазначається, що дані засоби часто виконують обидві функції, що створює певні труднощі для юристів, які намагаються визнати правову охорону технічних засобів за якоюсь однією групою, а не за іншою, та вказує на недосконалість класифікації. Зокрема серед першої групи наводять паролі та технології криптографічного захисту, зокрема цифрові підписи та сертифікати [15].

Технічні засоби захисту авторського права та суміжних прав у мережі Інтернет різноманітні. Зупинимось на характеристиках деяких з них. Серед них можна виділити використання веб-депозитаріїв, які є своєрідними веб-архівними об'єктами інтелектуальної власності. Слід зазначити, що деякі автори відносять даний захід до організаційних [16]. Схеми веб-депозитаріїв використовуються у багатьох країнах для захисту авторського права у різноманітних сферах. Даний захід заснований на принципах явочної системи та презумпції авторства. Механізм застосування даного засобу такий: є сховище, куди депонуються у безумовному порядку усі можливі твори, в тому числі CD-ROM з веб-сторінками. Для цього особа подає заяву про те, що вона є автором (правоволодільцем) твору, із зазначенням його назви та коротким описом. Фіксується дата прийому твору,

оформлюється свідоцтво про те, що певний об'єкт прийнято, яке видається заявнику. Дата депонування буде доказом факту того, що у вказаний час заявник володів копією об'єкта [17]. Позитивне значення даного заходу полягає в тому, що він дає можливість довести наявність авторського права, порівняти твори, визначити справжнього автора. Проте даний спосіб має недоліки: є випадки, коли особа вже опублікувала свій твір в Інтернеті, тоді використання такого засобу є непотрібним; даний засіб не захищає від недобросовісної реєстрації твору у веб-депозитарії іншою особою, тобто від зловживання правом; даний засіб не дає захисту від публікації твору, взятого в оф-лайн, у мережі Інтернет; процедура депонування також може бути недоступною кожному. У зв'язку із зазначеним у законодавстві досі не передбачено застосування такого технічного засобу захисту, хоча спроби правового регулювання застосування такого засобу існують, зокрема у Російській Федерації [18].

Іншим засобом захисту є цифрові водяні знаки, що наносяться за допомогою спеціального програмного забезпечення, яке вбудовує прихований код певного формату у файли. Під час звичайного сприйняття документа користувач не бачить яких-небудь закодованих позначень — знака копірайту, імені автора, року видання. Але згодом під час застосування певного програмного засобу можна довести, що файли містять додаткову інформацію, що вказує особу, яка її записала. Інколи інформація вбудованого файла може відобразитися у вигляді напівпрозорих символів — «водяних знаків» — під час перегляду. Таким чином, «видимі» та «невидимі» водяні знаки ускладнюють або роблять неможливим протиправне комерційне використання об'єкта і можуть бути складовою доказів порушення прав. При цьому важливою особливістю водяних знаків є стійкість до будь-яких операцій над документом — стиснення, зміна розмірів, формату, кольору, які їх не знищують, а лише трохи змінюють їх вигляд [19]. Сьогодні таких програмних продуктів дуже багато, серед них, зокрема, Photo Watermark Professional, Easy Batch Watermark, Watermark Factory тощо.

Це можуть бути методи криптографічного перетворення матеріалів, зокрема криптографічні конверти — програмне

забезпечення, яке зашифрує твори так, що доступ до них може бути отриманий лише із застосуванням належного ключа до шифру. Ці методи дозволяють обмежити або повністю виключити можливість копіювання творів. Серед таких, наприклад, програмні продукти Cryptolore фірми IBM. Суб'єкти авторського права можуть розповсюджувати твори із використанням технології криптографічного конверта, вимагаючи від користувачів плати за ключ, за допомогою якого твір можна «вийняти» з конверта [20].

У цілому за допомогою спеціальних комп'ютерних програм об'єкт можна зробити обмежено функціональним, коли автор подає лише частину інформації, приміром, зміст книги чи деякі її розділи. Цей метод широко використовується для передплати інтернет-видань. Можна обмежувати кількість копіювання творів. Можна зберігати твір у файлі формату PDF таким чином, щоб його неможливо було копіювати взагалі або навіть друкувати. Разом із тим можна використовувати коди доступу, які надаються за плату, за допомогою яких можна знімати захисні механізми, функціональні обмеження для використання твору [21].

Можливим є також використання електронно-цифрового підпису, який надійно засвідчує належність документа певній особі. Файл-носії з вбудованим електронно-цифровим підписом має усі ознаки документа і може являти собою доказ для суду. Таким чином, електронно-цифровий підпис дозволяє пов'язати зміст документа разом з його реквізитами у єдиний електронний документ і підтвердити його юридичну силу. Так, відповідно до ст. 3 Закону України «Про електронний цифровий підпис» від 22.05.2005 р. № 852-IV за відповідності встановленим вимогам електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки). Стаття 1 даного Закону визначає електронний цифровий підпис як вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Слід підкреслити, що в українському законодавстві під час визначення

призначення даного засобу спеціально не вказується, що електронний цифровий підпис призначений для захисту електронного документа від підробки, хоча це було би бажаним.

Слід зазначити, що цифрові сертифікати, які використовуються у технології цифрового підпису, можуть використовуватися для посвідчення більшої інформації, ніж просто особи тих, кому їх було видано, зокрема права, що належать певній особі. Продавці можуть користуватися цифровими сертифікатами для контролю доступу до системних ресурсів, у тому числі файлів, що містять твори, надаючи доступ до файлів користувачам, які можуть пред'явити цифровий сертифікат із зазначеними в ньому правами (наприклад права на доступ, завантаження, перегляд тощо). Отримати такий сертифікат можна як у продавця, так і у третьої особи [22].

Також за допомогою спеціальних комп'ютерних програм можна обмежувати доступ до творів, зокрема встановлювати строк, протягом якого твір буде доступним для загального доступу в Інтернет (наприклад прийом «годинникова бомба»). Це можуть бути також інші мережеві технології, які наділяють електронний документ можливістю саморуйнування у випадку його незаконного використання [23].

Існують спеціальні технічні засоби, які надають можливість контролювати кількість випадків використання творів, розміщених в Інтернеті, а також у певних випадках стягувати плату за їх використання [24]. З цією метою суб'єкти авторського права і суміжних прав можуть розповсюджувати свої твори в мережі із використанням кодів доступу, які надаються за плату, за допомогою яких можна знімати захисні механізми, функціональні обмеження для використання твору. Такі коди можуть час від часу змінюватися. Це можуть бути також конверти управління правами, які періодично зв'язуються із сервером продавця для перевірки дотримання ним параметрів використання твору. Наприклад, програмні продукти компанії Wave Interactive Networks, які дозволяють зашифрувати твори у файл з розширенням wxp, які під час активації викликають встановлення зв'язку між комп'ютером користувача і сервером фірми з метою дебе-

тування рахунку користувача на сайті цієї фірми [25].

Ще одним із ефективних технічних засобів захисту є використання мережевих павуків та пошукових роботів — програм, які працюють в Інтернет та здатні за допомогою певного набору пошукових реквізитів, які містяться у вбудованому файлі, відшукати конкретний об'єкт або посилання на нього [26]. Аналогічні програми ще називають детекторами плагіату, при використанні яких створюється цифровий образ усього документа, який перевіряється, після чого він порівнюється з матеріалами, розміщеними в Інтернеті та спеціалізованих базах даних, у тому числі на академічних ресурсах і каталогах матеріалів засобів масової інформації [27].

Існують також виконувані програми, наприклад Java applets, Active X scripts, які є частками інформації, що передається із сервера продавця на комп'ютер користувача, виконується під час конкретного сеансу зв'язку та стирається з оперативної пам'яті комп'ютера із його закінченням. Випадки використання виконуваних програм, а відтак й інформації з сервера користувача, легко піддаються обчисленню, оскільки ці програми завантажуються у комп'ютер користувача під час кожного сеансу зв'язку [28].

Також можна використовувати механізм централізованого обчислення, за якого всі виконувані програми, що не є частиною інтерфейсу комп'ютера користувача, залишаються на сервері продавця. Комп'ютер користувача повинен встановлювати контакт із сервером щоразу, як використовується виконувана програма, що дозволяє центральному комп'ютеру обчислювати кількість сеансів доступу [29].

Слід зазначити, що частину з даних засобів охарактеризовано у Рекомендаціях щодо вдосконалення механізму регулювання цифрового використання об'єктів авторського права і суміжних прав через мережу Інтернет, розроблених Державною службою інтелектуальної власності. Доцільно було би викласти положення щодо технічних засобів захисту у більш системному вигляді.

У літературі вже висвітлювалися питання про технічні засоби захисту таких об'єктів, як фотографічні твори. Зокрема найбільш простими і саме тому не досить ефективними є наступні. Техноло-

гія «низького рівня вирішення» полягає у розміщенні в мережі об'єкта з вирішенням не вище 72 пікселів на дюйм. У результаті на екрані об'єкт відображається цілком задовільно, проте друківана версія має низьку якість. Технологія «багатошарового зображення» передбачає створення таблиці з однією коміркою, що співпадає за розмірами з об'єктом, далі розміщення об'єкта в комірку у якості фону, формування ще однієї таблиці-комірки, яку поміщають зверху, формування спеціального прозорого файлу, який розміщують у якості верхнього шару. В результаті об'єкт можна продивитися, проте результатом копіювання буде лише прозорий шар, власне пустий файл. Технологія «сегментування» передбачає автоматичну «нарізку» об'єкта на безліч сегментів, створення таблиці з кількістю комірок, що дорівнюють кількості сегментів, кожен з яких розміщується у відповідну комірку. В результаті об'єкт не може бути скопійований як єдине ціле (подібну «мозаїку» можна прикрити зверху прозорим шаром) [30].

У результаті проведеного дослідження можна зробити такі висновки. По-перше, необхідним є вироблення системного підходу до класифікації технічних засобів захисту авторського права і суміжних прав, у тому числі в мережі Інтернет, та його відображення на рівні відповідних рекомендацій. Разом з тим, це ускладнено технічними характеристиками зазначених засобів та постійною появою нових засобів. По-друге, у зв'язку із швидким розвитком технологій необхідним є постійний моніторинг заходів і засобів захисту об'єктів інтелектуальної власності в мережі Інтернет на рівні відповідного уповноваженого органу. По-третє, жоден із вказаних засобів не може гарантувати стовідсоткової охорони об'єкта у мережі Інтернет. На думку фахівців, найбільш ефективними вважаються технології, засновані на принципах криптографії, які задувалися раніше, а доцільним вважається комплексне використання різних технічних засобів захисту.

ПРИМІТКИ

1. Ващинець І. Поняття технічних засобів захисту авторського права та їх правовий статус у чинному законодавстві України / І. Ващинець // Підприємництво, господарство і право. — 2005. — № 3. — С. 95—100.
2. Ващинець І. І. Цивільно-правова охорона авторських прав в умовах розвитку інформаційних технологій : дис. ... канд. юрид. наук : 12.00.03 / І. І. Ващинець ; НАН України, Ін-т держави і права ім. В. М. Корецького. — К., 2006. — 179 с.
3. Ващинець І. І. Деякі питання правового статусу технічних засобів захисту авторського права і суміжних прав / І. І. Ващинець // Часопис Київського університету права. — 2009. — № 2. — С. 186—192.
4. Недоруб О. Особенности использования и охраны фотографических произведений в сети Интернет / О. Недоруб // Интеллектуальная собственность. Авторское право и смежные права. — 2008. — № 9. — С. 22—33.
5. Наумов В. Б. Проблемы реализации авторских прав в сети Интернет [Електронний ресурс] / В. Б. Наумов // Мир медиа XXI. — 1999. — № 1. — Режим доступу : <http://www.russianlaw.net/law/ip/copyright/a09/>.
6. Наумова Е. Технические средства защиты авторского права / Е. Наумова // Интеллектуальная собственность. Авторское право и смежные права. — 2009. — № 2. — С. 60—66.
7. Пастухов О. М. Авторське право в Інтернеті : монографія / О. М. Пастухов. — К. : Школа, 2004. — 144 с.
8. Рекомендації щодо вдосконалення механізму регулювання цифрового використання об'єктів авторського права і суміжних прав через мережу Інтернет, розроблені Державною службою інтелектуальної власності [Електронний ресурс]. — Режим доступу : sips.gov.ua/ua/gesomnet.html.
9. Недоруб О. Зазнач. праця. — С. 26—30.
10. Google будет бороться с интернет-пиратами [Електронний ресурс]. — Режим доступу : http://news.zn.ua/TECHNOLOGIES/google_budet_borotsya_s_internet-piratami_106880.html.
11. Managing intellectual property online. What are digital rights management and technological protection measures//DL-202E Electronic Commerce and Intellectual Property, Session 2, 2007. — WIPO/OMP. — P. 39.

12. Ващинець І. Поняття технічних засобів захисту авторського права та їх правовий статус у чинному законодавстві України / І. Ващинець // Підприємництво, господарство і право. — 2005. — № 3. — С. 95—96.
13. Michael Sonntag. Securing webpages. An Overview [Electronic resource]. I-Society 2010, 28-30.6.2010, Institute for Information Processing and Microprocessor Technology, London. — Mode of Access: http://www.sonntag.cc/fileadmin/Downloads/Publications/Securing_webpages.pdf. — P. 7—9.
14. Protection of technological measures. Institute for Information Law, Amsterdam, University of Amsterdam, November 1998. — P. 2—5.
15. Dr. Ian R. Kerr, Alana Maurushat, Christian S. Tacit. Technological protection measures: tilting at copyright's windmill//Ottawa Law Review. — 2002—2003. — Vol. 34. — № 1. — P. 13—14.
16. Недоруб О. Зазнач. праця. — С. 28.
17. Наумов В. Б. Зазнач. праця.
18. Возможно, будет создан web-депозитарий [Електронний ресурс]. — Режим доступу : <http://www.cy-pr.com/news/3199/>; Web-депозитарий и авторское право [Електронний ресурс]. — Режим доступу : <http://www.exler.ru/blog/item/10035/>.
19. Наумов В. Б. Зазнач. праця.
20. Пастухов О. М. Зазнач. праця. — С. 94.
21. Там само.
22. Наумова Е. Зазнач. праця. — С. 61.
23. Мамон З. Захист авторських прав у мережі Інтернет [Електронний ресурс] / З. Мамон, О. Дроздов // Юридичний вісник. — 2007. — № 7. — Режим доступу : http://www.yurinc.com.ua/legal_bulletin_of_Ukraine/archive/?jid=203.
24. Пастухов О. М. Зазнач. праця. — С. 97.
25. Там само. — С. 97—98.
26. Недоруб О. Зазнач. праця. — С. 32.
27. Германова О. Межі копірайту в безмежжі Інтернету / О. Германова // Вісник податкової служби України. — 2007. — № 31. — С. 38—41.
28. Пастухов О. М. Зазнач. праця. — С. 98.
29. Там само.
30. Недоруб О. Зазнач. праця. — С. 30—31.

Рассомахина Ольга. Характеристика технических средств защиты объектов авторского права и смежных прав в сети Интернет.

Статья посвящена определению подходов к классификации технических средств защиты авторского права и смежных прав в сети Интернет и характеристике отдельных их видов, что актуально в связи с проведением исследования вопросов их правового регулирования.

Ключевые слова: защита авторского права и смежных прав, сеть Интернет, правовое регулирование, меры и средства защиты авторского права и смежных прав, технические средства защиты.

Rassomakhina Olga. Characteristics of technological protection measures of copyright and related rights on the Internet.

This article describes approaches to the classification of technological protection measures of copyright and related rights on the Internet and characteristics of certain types of them, that is important in connection with the examination of issues concerning their legal regulation.

Key words: protection of copyright and related rights, the Internet, legal regulation, measures and means of protection of copyright and related rights, technological protection measures.