

УДК 343.9:343.533

**Шишка Роман Богданович,**

доктор юридичних наук, професор, професор кафедри інтелектуальної власності та права Київського Інституту інтелектуальної власності та права Національного університету «Одеська юридична академія»

## ПРАВОВІ ОСНОВИ ПРОТИДІЇ ПІРАТСТВУ В ІТ СФЕРІ

**Постановка проблеми.** З появою цифрових технологій у суспільстві появилось чимало нових нагальних проблем сучасності, зокрема в сфері права: забезпечення недоторканності честі та гідності людини, свободи її волевиявлення, ділової репутації юридичної особи; збереження таємниці свого приватного життя, інших видів таємниць та персональних даних; забезпечення недоторканності майна та майнових прав, втручання у належне користувачам програмне забезпечення їх гаджетів і використання їх контенту, безпеки грошового обігу та безготівкових розрахунків тощо.

Принаймні, види, форми та наслідки порушень у сфері ІТ технологій постійно зростає як і небезпеки від того. Справа не стільки в самих порушеннях, які визначені такими чинним законодавством, скільки у нейтралізації їх наслідків, виявленні порушників доведення їх причетності та вини, протидії цим порушенням та порушникам, як правило високоінтелектуальним особам, які є фахівцями і можуть мати доступ до мережі через різні гаджети та різні місця. Здебільше це вчиняється для неправомірного отримання вигоди або від безкоштовного використання чийогось ресурсу, або отримання прибутку від віддаленого майнінгу чи іншої майнової вигоди. Зі встановленням неліцензійних програм на ПК користувачів, що є масовим в Україні, пірати-розповсюджувачі порушують закони України, піддають ризику своїх клієнтів, не гарантують якісної технічної підтримки. Реалізація піратських продуктів за низькими цінами позбавляє клієнтів законослухняних продавців ліцензійного, безпечного та надійного програмного забезпечення та перешкоджає для розвитку чесного бізнесу в українській ІТ індустрії.

Відповідно ведеться пошук засобів та способів протидії піратству. Тут недостатньо формального визначення піратства у ст. 50 Закону України «Про авторське право та суміжні права» [2], а необхідно

встановити витоки, прояви, небезпеки та їх наслідки, виробити стратегію і тактику такої протидії і на їх основі сформулювати форми, засоби та способи такої протидії. Поки що за конструкцією чинного законодавства йдеться про намагання протидіяти наслідкам, зокрема користувачам піратських контентів і апелювати до їх совісті та намагатися виписувати проти них санкції. Проте проблема у поширювачах піратського контенту, які власне забезпечують відповідний інформаційний ресурс, розробникам програмного забезпечення доступу до контенту з обмеженим доступом.

**Стан дослідження теми.** Можна погодитися щодо різноманітного впливу на ІТ-сферу в Україні з боку як урядів окремих країн, так і неурядових об'єднань компаній-виробників інтелектуального контенту як виправданій складової державної політики у цій сфері, напряду правового визначення, впливу, регулювання та охорони суб'єктивних прав та інтересів, яка в Україні тільки становиться. Цей напрям розробляється кафедрами інтелектуальної власності та корпоративного права Національного університету «Одеська юридична академія» та Львівського національного університету ім. І. Франка. Є й інші гідні уваги розробки та навіть фундаментальні роботи (Г.О. Улянова).

**Виклад основного матеріалу.** Наразі виділено 4 види напрямів політики держави щодо протидії піратству: 1) посилення законодавства для підняття рівня ризику для порушників при порушенні закону; 2) фіксація верхнього порогу цін до прийнятого для середніх доходів рівня; 3) стандартизація, сертифікація та ліцензування з метою переведення ринку програмного забезпечення з нинішнього «дикого» стану в урегульований і нав'язування користувачам культури уникнення контрафактів, зокрема введення сертифікатів безпеки/відповідності програмних продуктів і ліцензій на право займатися діяльністю з виробництва ПЗ; 4) пропаган-

да правомірності діяльності в сфері ІТ та добитися у піратів і користувачів протиправного програмного забезпечення докорів совісті та почуття дискомфорту. В їх узагальнюючому декларативно постановочному формулюванні можна лише сподіватися, що це позитивно відобразиться на практиці. Проте сподівання не завжди себе виправдовують, особливо надія на порядність та нормопослушання.

Водночас виробники інтелектуального контенту програмними засобами намагаються протидіяти як порушенням так і його прояву – піратству. Так корпорація Microsoft спрямовує такі заходи, насамперед, щодо розповсюджувачів піратських копій. Тут само собою напрошується рішення: карати їх тією зброєю: обмеженням чи заборонаю доступу до інформаційних мереж, як прояву звуження прав людини через блокування доступу до мереж. Проте наразі віртуальні технології – невід’ємна складова сучасності, без чого неможливе забезпечення гідного людини рівня життя (безготівкові розрахунки, цифрове телебачення, мобільний зв’язок тощо). Вони стали середовищем поширення об’єктів авторського права і не тільки своїх і правомірно. Під їх натиском традиційне використання окремих його об’єктів (друк, прокат кінофільмів) в економічному плані втратили комерційну складову, стали не вигідними і фактично не забезпечують майнових прав авторів та володільців. Особливо прикро, що значна частина наукових публікацій не вартують більше чим витрачений на їх друк папір, і їх відбір для оприлюднення не витримує критики і стає загрозою для самої науки.

Проблеми, що з’явилися із запровадженням ІТ, привернули увагу фахівців різних галузей права і не дарма: можливість вічності для збереження особистості в цифровому середовищі як вічне прагнення людства до безсмертя, форма існування особи та прояву її особистості і професійності. Визнаний високий рівень піратства в Україні завдав шкоди її репутації та здатності навести лад. Недарма торгове представництво США (USTR) визнало її «піратом N1» та ініціювало спеціальне розслідування стосовно нелегального використання програмного забезпечення, недолугих спробах уряду закрити піратські ресурси.

Законодавство України у сфері ІТ-права, зокрема, з протидії піратству, формування концепту розвитку нормативно-правової бази в сфері кібербезпеки на державному рівні, окремих локальних систем та користувачів бажає кращого: воно не системне, роздроблене, полишено єдиного підходу. Наразі це як загальні закони України «Про основи національної безпеки», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», щодо піратства – Закон

України «Про авторське право та суміжні права». Заслугує уваги ухвалений Верховною Радою України законопроект 3081-д «Про державну підтримку кінематографії в Україні», який передбачає окремі напрямки протидії неправомірного використання кінофільмів, зокрема засоби та способи протидії піратству в Інтернеті.

Ряд з них по своїй природі є оперативними заходами, які не передбачені цивільним законодавством. Відповідно ми маємо або визнати допустимість оперативних заходів стосовно недобросовісних споживачів, або надалі ігнорувати їх і тим не бачити в них перспектив. Тож якщо ми визнали чи маємо визнати відносини ІТ-права правовими та приватними, то йдеться про рівень їх визначення чи навіть визнання, глобальну ідею, яка можлива тільки в рамках концепції цивільно-правового регулювання. Звідси йдеться про потребу розширення його предмету, визнання віртуального простору як сфери здійснення цивільних прав та виконання юридичних обов’язків, нових їх носіїв – за ідентифікаційними ознаками ПК та інших гаджетів, через які було вчинене піратство та визнання оперативних засобів протидії, в тому числі, через самозахист.

В іншому разі, згідно ієрархії правового регулювання цивільних правовідносин, що передбачені у ст. 4 ЦК України [4], стає незрозумілим поява в спеціальних актах зазначених правовідносин, значення програмного забезпечення безпеки Інтернет-правовідносин як нормативного впливу на них, допустимість окремих заходів протидії правопорушенням, можливе припинення вільного доступу до Інтернет-ресурсу тощо.

Йдеться про блокування сайту, блокування контенту, а іноді й пересилка «черв’яків» на сайти, з яких вчинено піратство тощо. Разом із блокуванням платіжних карток це, по суті, новий спосіб захисту порушених прав, що потребує позитивізації в ЦК України, зокрема його ст. 16. Зокрема стосовно цієї статті не зрозуміло: чому вона відразу акцентована на судову форму захисту порушених прав, що проведено у її назві «Захист цивільних прав та інтересів судом», а також ч.1, 2 та 3? Принаймні тут проігноровані: можливість самозахисту та співвідношення названої статті із ст. 19 ЦК, захисту прав іншою стороною, що забезпечує здійснення цивільних прав та інтересів, зокрема в даній сфері провайдерами, можливі примирні процедури при порушенні цивільних прав та інтересів. Видається розумним змістити акценти згідно послідовності стадій розвитку правового конфлікту та сучасних уявлень про його вирішення, зокрема:

1) У назві цієї статті вилучити слово «судом».

2) Частину 1 викласти у редакції «Потерпілі від порушення їх суб'єктивних цивільних прав та інтересів вправі їх захищати у формі, порядку, засобами та способами, що передбачені цим кодексом та іншими актами цивільного і процесуального законодавства».

3) Частину 3 викласти у редакції «Форми захисту (неюрисдикційна та юрисдикційна обираються потерпілими на їх власний розсуд з урахуванням виду порушення, потреби його припинення та відновлення прав, засобів впливу на порушника».

4) Частину 3 викласти у редакції «Засоби захисту цивільних прав: усне звернення до порушника, письмові заява, рекламація, скарга, позов, апеляція, касація, оперативні дії обираються потерпілими чи іншими учасниками правовідносин на їх власний розсуд».

5) Нинішню частину 2 слід визначити ч. 4 і у ній окремим абзацом 11 серед способів захист порушених прав та інтересів передбачити в редакції «оперативний захист (блокування платіжної та іншої картки, скасування бонусів та інших наданих переваг при здійсненні цивільних прав, блокування контенту, тощо».

6) Частину 5 викласти у редакції: «На власний розсуд за захистом порушених суб'єктивних цивільних прав та інтересів потерпілий, його представник чи інша пов'язана особа у передбаченому законом порядку можуть звернутися у суд».

7) Відповідно п. 2 ч. 2 та ч. 3 нинішньої редакції ст. 16 ЦК слід вилучити: першу як таку, що перебивається вище запропонованим і положеннями ЦПК України, другу – як процесуальну за змістом і наразі є чисто інформативною: рішення про відмову у задоволенні позову чи заяви повністю чи частково, не відмову у захисті, суд постановляє як акт правозастосування. Тож ч. 3 ст. 16 ЦК є чужою для цивільних правовідносин.

У разі легалізації запропонованих змін володільці суб'єктивних прав отримують можливість швидко блокувати нелегальний контент, якщо протягом встановленого часу отримання повідомлення про розміщення піратського контенту відеовласник ресурсу не видалить його. Це має бути забезпечене санкціями за відмову блокувати нелегальний контент, як і за необґрунтовані вимоги щодо його блокування.

*Постановка проблеми чи точніше проблем.* Проблема перша - це сама природа правовідносин у цій сфері де не завжди доцільні традиційні підходи і формування ІТ-права на не постфактичній, а негайній оцінці правочинів та їх верифікації через призму програмно-правового забезпечення. У сфері авторського права це піратство визначене і перебуває у ідеології дрібнокрадіжкового підходу,

що започаткований ст. 52-1 Кодексу України про адміністративні правопорушення [1] та узагальненого розуміння правопорушень у сфері права інтелектуальної власності, суміші способів захисту цих прав (ст. 432 ЦК України), потреби визнання оперативних способів захисту цивільних прав та запровадження їх в окремих інститутах цивільного права, зокрема у ст. 52 Закону України «Про авторське право та суміжні права».

Є сподівання на оперативні заходи зі сторони державних органів, зокрема Держспецзв'язку, який згідно чинного законодавства: бере участь у формуванні та реалізації державної політики у сфері кібербезпеки; розробляє критерії та порядок оцінки стану кіберзахисту об'єктів критичної інформаційної інфраструктури, забезпечує її організацію та проведення; здійснює державний контроль за станом захисту інформації, яка циркулює на об'єктах критичної інформаційної інфраструктури; створює у межах затвердженої чисельності та забезпечує функціонування підрозділу з питань оперативного реагування на кіберінциденти; забезпечує функціонування системи захищеного доступу державних органів до Інтернету; координує діяльність державних органів, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, підприємств, установ і організацій незалежно від форми власності з питань запобігання, виявлення та усунення наслідків кіберінцидентів; вживає організаційно-технічні заходи із збору та обліку інформації про кіберінциденти і кіберзагрози, узагальнює і надає таку інформацію суб'єктам забезпечення кібербезпеки постійної готовності відповідно до їх повноважень; за результатами аналізу кіберінцидентів координує діяльність операторів, провайдерів телекомунікацій з питань забезпечення збереження ними необхідних даних про відповідні кіберінциденти в інтересах суб'єктів забезпечення кібербезпеки постійної готовності; здійснює міжнародне співробітництво і взаємодіє з компетентними органами інших держав у рамках надання міжнародної технічної допомоги з питань кіберзахисту [3].

В Державному центрі кіберзахисту та протидії кіберзагрозам Держспецзв'язку було сформовано спеціальний структурований підрозділ Computer response team of Ukraine (далі – Cert-UA) – команда реагування на комп'ютерні надзвичайні події України. Основна мета Cert-UA – забезпечити захист інформаційних ресурсів та інформаційних та телекомунікаційних систем від несанкціонованого доступу, неправомірного використання а також порушень їх конфіденційності, цілісності та доступності. Вони вправі приймати заходи, спрямовані на ліквідацію інцидентів у сфері інформаційної без-

пеки, які виникають в кіберпросторі українського сегменту мережі Інтернет. Окрім того, кіберпростір відстежується іншими службами СБУ, МВС, які виявляють порушення та інформують відповідні підрозділи.

Не вдаючись у публічно-правові аспекти протидії зазначеним порушенням, варто зазначити, що розміщення твору на інформаційних загальнодоступних ресурсах є його використанням і вписується в ст. 441 ЦК України, а з другого боку цей інформаційний ресурс може бути використаний не тільки в режимі вільного використання об'єкта авторського права. Проблема стала настільки актуальною, що країнами світу приймаються спеціальні закони про боротьбу з піратством як виклик та протидію. Між тим піратські ресурси легко обходять визначені законодавцем заборони: розміщуються в Інтернет-клубах, на сайтах дітей, через боти, чи давно не використовувані сайти їх володільцями. Відповідно, тут зусиль одних фахівців у сфері цивільного права недостатньо. Більше сподівань на програмне забезпечення та оперативну протидію розміщенню і використанню в Інтернеті незаконних копій кіно- і телефільмів, літературних та наукових творів, насамперед блокування всіма Інтернет-провайдерми таких сайтів. В цьому велике сподівання на системних адміністраторів Інтернет провайдера, який має здійснювати контроль змісту розміщуваних володільцями сайтів ресурсів. Тут проблема в конфлікті свободи розміщення інформації володільцем сайту та контролю щодо її змісту.

Блокування піратського контенту як оперативний захід можна кваліфікувати: з одного боку як самозахист від можливих санкцій та дії із захисту суб'єктивних прав і охоронюваних законом інтересів володільців майнових прав інтелектуальної власності як третіх осіб, а з другого – обов'язок провайдера щодо дотримання вимог чинного законодавства як ліцензійна умова його діяльності. Відповідно невиконання останнього може слугу-

вати підставою призупинення ліцензії. Проте цього недостатньо.

Сам правоволоділець при виявленні порушення його прав вправі звертатися за захистом порушених авторських прав, в тому числі, надавати підтвердження підстав звернення за ним : а) авторства на об'єкт чи правового титулу володіння майновими правами на нього; б) скріншот протиправного розміщення копії такого об'єкта і мережі. З огляду на презумпцію прав позивача і його право на негайне застосування забезпечувальних заходів (зволікання може призвести до втрати доказової бази з файлообмінними ресурсами) вбачається, що при зверненні в суд це є різновид «позову Морєва», що передбачає негайне блокування неліцензійного контенту в цілому. Провайдер має негайно реагувати на протиправне розміщення контенту його клієнтом, що потребує перевірки правомірності змісту розміщеного контенту. Вважаємо, що суд вправі прийняти рішення про блокування, якщо на вимогу автора чи володільця прав у блокуванні контенту системний адміністратор їм відмовить.

**Висновок.** Найбільш ефективними в даному разі є програмні та правові засоби. Хоча вони наразі обходяться або через розміщення контенту на альтернативних доменах, чи наданням можливості користувачам заходити на цей сайт через спеціальний VPN-сервіс, який змінює їх IP-адреси на зарубіжні та тим виводить їх із національної юрисдикції. Попри заборону в Україні російських доменів значна частина їх користувачів успішно ними користується хоча б тому, що значна частина їх адресатів також є їх користувачами чи вони є більш «розкрученими» і програмно забезпеченими, надають їх користувачам більше можливостей. Тим більше, що більшість російських сайтів, в тому числі й піратські, доступні в Україні.

Таким чином, проблема протидії піратству досить складна і потребує свого комплексного вирішення.

#### ЛІТЕРАТУРА:

1. Кодекс України про адміністративні правопорушення : Закон, Кодексвід 07.12.1984 № 8073-X (Редакція станом на 27.09.2017). – Режим доступу: zakon.rada.gov.ua/laws/show/80731-10
2. Про авторське право та суміжні права : Закон України від 23.12.1993 № 3792-XII (Редакція станом на 26.04.2017). – Режим доступу: zakon.rada.gov.ua/laws/show/3792-12
3. Про основні засади забезпечення кібербезпеки України: Проект закону України №2 126а от 13.05.2017. – Режим доступу: search.ligazakon.ua/1\_doc2.nsf/link1/JH1N268V.html
4. Цивільний кодекс України: Закон від 16.01.2003 № 435-IV (Редакція станом на 19.07.2017). – Режим доступу: zakon.rada.gov.ua/laws/show/435-15

**Шишка Роман Богданович**

**ПРАВОВІ ОСНОВИ ПРОТИДІЇ ПІРАТСТВУ В ІТ СФЕРІ**

У статті досліджено засоби та способи протидії піратству в ІТ сфері. Звернуто увагу на необхідність дослідження витоків, проявів небезпеки та наслідків піратства, вироблення стратегії і тактики протидії піратству і на їх основі формулювання форм, засобів та способів такої протидії. Запропоновано внесення змін до ст. 16 Цивільного кодексу України щодо нового способу захисту порушених прав.

**Ключові слова:** піратство, кібербезпека, способи, засоби захисту, порушення прав, провайдер, Інтернет ресурс, контент.

**Шишка Роман Богданович**

**ПРАВОВЫЕ ОСНОВЫ ПРОТИВОДЕЙСТВИЯ ПИРАТСТВУ В ИТ СФЕРЕ**

В статье исследованы средства и способы противодействия пиратству в ИТ сфере. Обращается внимание на необходимость исследования истоков, проявлений небезопасности и последствий пиратства, разработку стратегии и тактики противодействия пиратству. На этой основе предлагается формулировать формы, средства и способы противодействия пиратству. Предложено внести изменения в ст. 16 Гражданского кодекса Украины относительно нового способа защиты нарушенных прав.

**Ключевые слова:** пиратство, кибербезопасность, способы, средства защиты, нарушение прав, провайдер, Интернет ресурс, контент.

**Shyshka Roman Bohdanovych**

**LEGAL BASICS OF COUNTERACTION TO PIRACY IN IT SPHERE**

In the article means and ways of counteraction to the piracy in IT sphere are investigated. It is paid attention to necessity of research of sources, indications of nonsafety and the consequences of the piracy, development of the strategy and counteraction tactics to the piracy. On this base it is offered to formulate forms, ways and means of counteraction to the piracy. It is offered to make changes to the article 16 of Civil code of Ukraine regarding a new way of protection of violated rights.

**Keywords:** piracy, cybersecurity, ways and means of counteraction, violated rights, provider, Internet resource, content.