



КІБЕРСКВОТИНГ ЯК ПРОЯВ НЕДОБРОСОВІСНОЇ КОНКУРЕНЦІЇ: ЕКОНОМІКО-ПРАВОВІ ОСОБЛИВОСТІ ТА ЗАХОДИ ПРОТИДІЇ

Олександр Бутнік-Сіверський

*доктор економічних наук, професор,
головний науковий співробітник сектору комерціалізації ОІВ
відділу промислової власності та комерціалізації
НДІ інтелектуальної власності НАПрН України
ORCID: 0000-0003-2492-231X*

Комплексно досліджено економіко-правові особливості кіберсквотингу як прояву недобросовісної конкуренції та однієї з форм кіберзлочинності з погляду його економіко-правового змісту, економічних факторів привабливості, критеріїв ідентифікації, запобігання та боротьби з негативними економіко-правовими наслідками для бізнесу та споживачів. Розглянуто заходи протидії кіберсквотингу в українському та європейському законодавстві, механізм запобігання кіберсквотингу та боротьби з ним у країнах Європейського Союзу з використанням позасудової процедури, де домінує Єдина політика вирішення спорів щодо доменних імен.

Ключові слова: кіберсквотинг, доменне ім'я, право інтелектуальної власності, заходи протидії кіберсквотингу

Постановка проблеми. Розвиток інтернет-технологій призвів до появи *кіберзлочинності*, яка здійснюється через комп'ютерні системи або мережі. Така злочинність може містити в собі крадіжку даних, фішинг, шахрайство, хакерство, кіберсквотинг та інші дії, до яких вдаються з метою отримання незаконних переваг або завдання шкоди. Кіберзлочинність з економіко-правової точки зору впливає на сучасні ринкові відносини, що характеризуються переходом від домінування постачальника до домінування споживача. Відповідні технології також дають змогу підвищити в мережі «Інтернет» конкурентоспроможність товарів, розширити ринки збуту, знайти нових постачальників, посередників та споживачів, що відповідає бізнес-процесам залучення клієнта, вивчення його потреб, самого акту вчинення правочину (транзакції) і післяпродажного обслуговування. Зароджувана система, як зазначає А. Манько, «...може охоплювати всі без винятку бізнес-процеси взаємодії компанії з клієнтом. Таку систему функціонування може забезпечити використання інтернет-технологій, що є актуальним для ведення бізнесу і стає невід'ємною частиною функціонування будь-якого підприємства у сучасному світі» [1, с. 2].

Однією з форм кіберзлочинності є *кіберсквотинг* (*cybersquatting*) як «протизаконна діяльність, що полягає у реєстрації, використанні та пропонуванні до продажу доменного імені із несумлінним (недобросовісним) наміром отримати прибуток від паразитування на гудвілі або торговельній марці, яка належить іншій особі» [2]. Особи, які вчиняють

такі дії, називаються *кіберсквотерами* [3, с. 319]. Ці дії належать до недобросовісної конкуренції, оскільки суперечать торговим та іншим чесним звичаям у господарській діяльності. При цьому однією з основних проблем, на якій акцентують увагу науковці, став конфлікт доменних імен і товарних знаків, що в сучасній системі інтелектуальної власності домінує, та залишається низка питань економічного і правового спрямування кіберсквотингу, які потребують подальшого поглибленого дослідження.

Літературний огляд. Дослідженню кіберсквотингу присвячено низку праць таких науковців: Г. Андрощук, Н. Булат, Х. Демченко, Т. Коваленко, А. Ляшенко, Н. Попова, І. Стародуб, М. Петрів та інших. Так, Г. Андрощук досліджує захист від такого виду недобросовісної конкуренції, як недобросовісна реєстрація доменного імені в усіх його проявах (тайпсквотинг, галузевий кіберсквотинг, брендів кіберсквотинг) [4]; Н. Булат вивчає поняття «кіберсквотинг», його види та шляхи боротьби з ним [5]; Н. Попова досліджує кіберсквотинг як основний вид правопорушень у доменних спорах [6]; Т. Коваленко це явище розглядає з позиції ринку купівлі та продажу доменів [7]. Низка науковців деталізує характерні ознаки кіберсквотингу та механізми протидії йому, аналізує судову практику розв'язання доменних спорів. Особливої уваги на сучасному етапі розвитку в умовах цифровізації (кіберфізичного простору) серед інших питань потребує поглиблене дослідження кіберсквотингу з позиції цивільного правопорушення в українському та європейському законодавстві.

Мета дослідження — комплексне економіко-правове вивчення особливостей кіберсквотингу, узагальнення механізмів та способів протидії недобросовісній конкуренції в українському та європейському законодавстві.

Виклад основного матеріалу. Цифровізація є визнаним механізмом економічного зростання завдяки здатності технологій позитивно впливати на ефективність, результативність, вартість та якість економічної діяльності. Для розміщення сайту в інтернеті необхідно придбати *хостинг*, тобто місце, де сайт фізично буде розміщений. *Хост* — комп'ютер, під'єднаний до інтернету. На підрахунок хостів базується найбільш розповсюджений спосіб визначення кількості унікальних користувачів, з якими асоціюється *IP-адреса комп'ютера*, з якого здійснюється доступ. Тут доменне ім'я використовується як адреса ресурсу в мережі, за якою будь-який користувач може знайти і переглянути ресурс [3, с. 320].

Доменне ім'я (або домен) — це унікальна адреса в інтернеті, яка ідентифікує вебсайт або сервіс і дає змогу користувачам знаходити його в мережі. У Законі України «Про електронні комунікації» в п. 22 ст. 2 зазначено, що *домен* — це «частина ієрархічного адресного простору мережі Інтернет, що має унікальну назву (доменне ім'я), що її ідентифікує, обслуговується групою серверів доменних імен та централізовано адмініструється» [8]. Це можливий спосіб запам'ятати і знайти сайт замість складних IP-адрес.

Доменне ім'я складається з назви *домену та доменної зони* (наприклад, .com, .ua) і використовується для знаходження сервісів та сайтів у мережі. *Доменна зона* — це частина повного доменного імені, розташована праворуч від основної частини. Вона визначає належність домену до певного рівня ієрархії доменних імен. Доменна зона також вказує на геолокацію або тематику сайту, що важливо для SEO (*Search Engine Optimization*) — процесу оптимізації сайту для пошукових систем, щоб покращити його позицію в результатах пошуку.

Зазвичай умовно виділяють три види доменів верхнього рівня:

- *національні доменні зони* — це двосимвольні національні домени країн: .ua, .us, .de, .pl, .укр тощо;
- *регіональні домени, чи географічні домени верхнього рівня* — це можуть бути доменні зони міст: .amsterdam та .barcelona, чи доменні зони великих регіонів: .asia, .africa тощо;

• *тематичні доменні зони* — усі інші доменні імена першого рівня: .com, .photo, .biz, .tickets тощо [9].

З появою різноманітних доменних зон з'явилися нові своєрідні можливості заробітку: *домейнінг* — реєстрація перспективних доменних імен, які пов'язані з уже існуючими торговельними марками, однак у перспективі підходять для продажу різним бізнесам; *кіберсквотинг* — реєстрація доменних імен, пов'язаних з торговельною маркою, що належить іншим особам, з наміром подальшого перепродажу зацікавленим компаніям [10].

Саме *кіберсквотинг*, як один з видів незаконної діяльності в цифровій економіці, спонукає науковців до пошуку економіко-правових механізмів попередження та протидії недобросовісній конкуренції, які також враховують певні види кіберсквотингу (брендовий, іменний, галузевий, географічний, авторський, зворотний, аукціонний, захисний і тайпсквотинг) [3, с. 321–323], що мають свої особливості та негативні економіко-правові наслідки для бізнесу і споживачів.

Так, Т. Коваленко *брендовий кіберсквотинг* визначає як «захоплення доменних імен, ідентичних або схожих із торговельними марками» [7, с. 43], а Н. Булат його розуміє як «порушення прав інтелектуальної власності на засоби індивідуалізації учасників цивільного обороту, товарів і послуг, учинене шляхом недобросовісної реєстрації доменного імені, що містить позначення, яке є тотожним (схожим) із охоронюваним об'єктом (його частиною)» [11, с. 99]. Із цього визначення випливають такі положення. По-перше, брендовий кіберсквотинг характеризується використанням у доменному імені позначень, що є тотожними (схожими) із знаками для товарів і послуг, комерційними (фірмовими) найменуваннями, географічними зазначеннями (їх частинами). Адже, як зазначає Н. Булат, «не доцільно під брендовим кіберсквотингом розуміти лише порушення прав на торговельні марки, а порушення прав на інші засоби індивідуалізації виділяти як окремі види кіберсквотингу, з огляду хоча б на те, що дані об'єкти традиційно об'єднуються в одну групу об'єктів права інтелектуальної власності — засоби індивідуалізації учасників цивільного обороту, товарів і послуг» [11, с. 99]. По-друге, визначальною ознакою брендового кіберсквотингу, як і кіберсквотингу загалом, є недобросовісність реєстрації доменного імені. Адже, як зазначає Н. Булат, «сама по собі реєстрація відповідних позначень у доменному імені ще не створює кіберсквотингу. І, перш за все, необхідно враховувати саме мету такої реєстрації» [11, с. 100].

Кіберсквотингом називають *реєстрацію доменних імен*, що містять у своїй адресі назву компаній, товарів та інших відомих речей, з метою подальшого перепродажу таких доменних імен компаніям, що зацікавилися. Саме *кіберсквотери є зловмисниками*, оскільки реєструють доменні імена, схожі за назвою з реальними сайтами, зокрема, щоб у майбутньому розповсюджувати шкідливе програмне забезпечення із сайтів на таких доменах. Вони використовують сайт з метою отримання конфіденційної інформації опуканих відвідувачів.

З позиції економіко-правових особливостей кіберсквотинг розглядаємо як неетичну та незаконну практику, яка може завдати шкоди бізнесу та ввести в оману споживачів. Розуміння наслідків кіберсквотингу та вжиття проактивних заходів може допомогти захистити присутність і репутацію бренду в мережі «Інтернет». За визначенням Н. Попової, «спонукальними мотивами до діяльності у ролі кіберсквотерів є невелика потреба у початкових капіталовкладеннях та значні прибутки після продажу доменів» [6, с. 135].

Сучасний кіберсквотер досліджує економічну спрямованість, передбачувані стратегії розвитку компаній, вивчає кон'юнктуру ринку. Вчасно відстеживши можливість злиття або поділ відомої компанії, просунутий кіберсквотер повинен блискавично розрахувати варіанти майбутніх назв і швидко зареєструвати відповідні доменні імена. У цьому випадку запорука успіху — вміння вибрати перспективне ім'я та зареєструвати домен, який надалі може стати популярним і дасть змогу витягти з цього матеріальну вигоду.

З погляду економіко-правового змісту Н. Булат при визначенні кіберсквотингу пропонує певне коригування: «по-перше, кіберсквотинг варто розуміти як правопорушення. Адже термін «протизаконна бізнес-діяльність» не одержав належного обґрунтування. По-друге, кіберсквотинг полягає у недобросовісній реєстрації доменного імені, при цьому його використання та пропонування до продажу не є обов'язковим. По-третє, метою недобросовісної реєстрації доменного імені може бути не лише отримання прибутку від його перепродажу, а також введення в оману споживачів, обмеження діяльності конкурента тощо. Окреслити повне коло можливих намірів правопорушника у даному випадку не є можливим» [5, с. 73].

До економічних факторів привабливості кіберсквотингу прийнято відносити:

- економічну спрямованість (передбачуваність стратегії розвитку компаній);
- матеріальну вигоду (уміння вибрати перспективне ім'я та зареєструвати домен);
- пасивність бізнесу (покупці завжди самі знаходять продавців);
- простоту ведення бізнесу (для ведення бізнесу не потрібні спеціальні знання, достатньо мати гарну інтуїцію та вміння відстежувати власників доменів);
- мінімальні витрати на старті бізнесу;
- дохід від продажу доменного імені у кілька разів перевищує витрати на його придбання [3, с. 320–321].

Водночас кіберсквотинг може мати кілька негативних економіко-правових наслідків для бізнесу та споживачів:

- втрату перспективи бізнесу: різке зменшення споживачів та покупців товарів;
- маркетингову пасивність: зміна позиції компанії на ринку, спеціалізації в ринковій ніші, ухиляння від прямої конкуренції;
- фінансові втрати: компанії можуть зіткнутися зі значними фінансовими вимогами щодо викупу доменного імені, пов'язаного з їхнім брендом або торговельною маркою, у кіберсквотерів;
- розмивання бренду: наявність несанкціонованого та потенційно шкідливого контенту на захопленому кіберсквотером домені може підірвати репутацію бренду та ввести в оману споживачів;
- обман споживачів: споживачі можуть бути введені в оману, думаючи, що захоплений домен є офіційним сайтом, що може призвести до потенційного шахрайства або дезінформації;
- судові витрати: компанії можуть понести судові витрати, щоб повернути свої доменні імена через суд або арбітраж [12].

До критеріїв ідентифікації кіберсквотингу компанії та приватні особи для запобігання та протидії відносять:

1. Недобросовісні наміри: реєстрант не має законного інтересу або прав на доменне ім'я і має намір продати його з метою отримання прибутку на основі його асоціації з добре відомою торговельною маркою.
2. Оманлива схожість: доменне ім'я ідентичне або схоже до ступеня змішування з відмітною торговельною маркою або назвою бренду.
3. Комерційна вигода: реєстрант має на меті отримати прибуток від продажу доменного імені або його асоціації з відомим брендом [12].

Для запобігання та боротьби з кіберсквотингом існує кілька засобів:

1. Реєстрація відповідних доменів, схожих на бренд або торговельну марку, щоб запобігти їх привласненню кіберсквотерами.
2. Моніторинг реєстрацій доменів та швидке реагування на домен, який порушує права на торговельну марку.
3. Позов до суду з використанням Єдиної політики вирішення спорів щодо доменних імен (СІУС) — (UDRP) (Uniform Domain Name Dispute Resolution Policy), щоб повернути собі домен, захоплений кіберсквотером.

4. Реєстрація торговельної марки, що забезпечить правовий захист і сильніші аргументи проти кіберсквотерів [12].

З позиції протидії кіберсквотингу в українському законодавстві доменні імена, як основа прояву кіберсквотингу, не отримали спеціальної охорони як самостійні об'єкти права інтелектуальної власності. До того ж відсутні будь-які міжнародні акти, що врегульовували б питання охорони доменних імен.

Доменні імена не належать до об'єктів права інтелектуальної власності, однак при цьому виконують не лише технічну функцію зв'язку між сервером та кінцевим користувачем, який бажає отримати будь-яку інформацію, а й вважаються дуже ефективним засобом індивідуалізації особи, товарів та/або послуг. При цьому, як зазначає М. Коваль, «слід враховувати особливість використання доменного ім'я, як словесне вираження (зазвичай латиницею), воно часто може бути ідентичним чи схожим до ступеня сплутування з різними об'єктами права інтелектуальної власності — найчастіше це знаки для товарів і послуг, фірмові (комерційні) найменування, географічні зазначення походження товару, об'єкти авторського права та інші» [13].

Рушійним моментом стало прийняття Закону України «Про використання доменних імен у спеціальному публічному домені .gov.ua» [14] як першого спеціального законодавчого акта в Україні, що регулює питання використання доменних імен у публічному секторі. Закон закріплює положення щодо належного розташування та адміністрування програмно-технічних засобів, на яких розміщуються державні електронні інформаційні ресурси, для яких здійснюється реєстрація доменного імені. Відтепер такі домени повинні розташовуватися тільки на території України, а функції з їх адміністрування та технічного супроводу в домені «GOV.UA» виконуються виключно органом державної влади, а саме центральним органом виконавчої влади, що забезпечує формування та реалізацію державної політики у сферах цифровізації, цифрового розвитку, цифрової економіки, цифрових інновацій і технологій, електронного урядування та електронної демократії.

Однак використання доменних імен (адресів сайтів у мережі «Інтернет») не обмежується лише публічним сектором [15, с. 1]. Варто зазначити, що разом з розвитком доменів у зоні .UA зростає необхідність не лише в реєстрації доменного імені, а й у захисті від кіберсквотингу. Адже у сучасних реаліях його обсяги досить великі і можна стверджувати, що більшість доменних імен, які у споживачів асоціюються з відомими світовими брендами, належать зовсім не їм. Правники стосовно цієї проблеми все ще продовжують наукові дискусії.

В Україні, як зазначає Т. Кудрицька, не врегульоване питання правового режиму використання у мережі «Інтернет» більшості з об'єктів — знаків для товарів і послуг, фірмових найменувань, міжнародних непатентованих назв (INN) фармацевтичних препаратів, повних та скорочених назв міжнародних міжурядових організацій, особистих імен, географічних зазначень [16], що сприяє недобросовісній реєстрації доменних імен кіберсквотерами. Найчастіше правовласники звертаються до суду за захистом прав на торговельну марку, посилаючись на норми Закону України «Про охорону прав на знаки для товарів і послуг» [17], згідно з якими порушенням прав власника свідоцтва на торговельну марку вважається використання без його згоди в доменних іменах знаків та позначень, вказаних у законі. У цьому законі відсутнє поняття «домен», а «доменне ім'я» визначається у ст. 1 як ім'я, що використовується для адресації комп'ютерів і ресурсів в інтернеті. У цьому випадку доменне ім'я кваліфікується через його функціональне призначення шляхом об'єднання двох основних його характеристик: *адресація комп'ютерів й адресація ресурсів*. У нормах закону опосередковано встановлюються правові межі використання доменних імен, зареєстрованих як торговельна марка. Зокрема використанням торговельної марки у п. 5 ст. 16 закону певним чином врегульовано способи захисту доменного імені у випадку реєстрації відповідної торговельної марки, а саме: свідоцтво надає його власнику виключне право

забороняти іншим особам використовувати позначення без його згоди, якщо інше не передбачено цим законом, а в абз. 2 ч. 1 ст. 20 запроваджено пріоритет прав на знаки для товарів і послуг над правами на доменні імена: порушенням прав власника свідоцтва вважається також використання без його згоди в доменних іменах торговельних марок та позначень, указаних у п. 5 ст. 16 цього закону.

Для застосування абз. 2 ч. 1 ст. 20 вказаного закону, як вважає Н. Булат, «зовсім не важливо, що зареєстроване раніше — торговельна марка чи доменне ім'я. Так, припустимо, особа зареєструвала певне доменне ім'я, під яким розробила сайт, де пропонує надання певних послуг. Із плином часу даний сайт стає досить популярним. Інша особа реєструє торговельну марку, тотожну доменному імені такого сайту, для аналогічних послуг. Думається, за такої ситуації вводитиме в оману споживачів саме володілець прав на торговельну марку. Однак ... незаконним є використання доменного імені ..., такий пріоритет має бути скасований через те, що, по-перше, норма абз. 2 ч. 1 ст. 20 цього закону не знімає питання кіберсквотингу (зрештою, окрім брендового кіберсквотингу, існують також інші його види, до того ж навіть поняття «брендовий кіберсквотинг» охоплює не лише порушення прав на знаки для товарів і послуг) та, по-друге, дана норма не сприяє справедливому захисту прав і законних інтересів суб'єктів прав на доменні імена» [11, с. 102–103].

Розглядаючи конкуренцію між інтересами володільців доменних імен та володільців комерційних (фірмових) найменувань, варто посилатися на ЦК України, де в ч. 2 ст. 489 зазначено, що право інтелектуальної власності на комерційне найменування є чинним з моменту першого використання цього найменування та охороняється без обов'язкового подання заявки на нього чи його реєстрації та незалежно від того, є чи не є комерційне найменування частиною торговельної марки [18].

На думку М. Петрів, «кіберсквотинг підпадає під поняття недобросовісної конкуренції ..., використання в домені чужого комерційного позначення є недобросовісною конкуренцією, оскільки таке використання є неправомірним» [19, с. 128]. Так, відповідно до ч. 1 ст. 1 Закону України «Про захист від недобросовісної конкуренції» [20] недобросовісною конкуренцією є будь-які дії у конкуренції, що суперечать торговим та іншим чесним звичаям у господарській діяльності. Відповідно до ч. 1 ст. 4 закону неправомірним є використання імені, комерційного (фірмового) найменування, торговельної марки (знака для товарів і послуг), рекламних матеріалів, оформлення упаковки товарів і періодичних видань, інших позначень без дозволу (згоди) суб'єкта господарювання, який раніше почав використовувати їх або схожі на них позначення у господарській діяльності, що призвело чи може призвести до змішування з діяльністю цього суб'єкта господарювання. Як вважає М. Петрів, «...одним із способів кіберсквотингу є реєстрація домену, схожого на домен правовласника з метою ввести споживачів в оману і заманити на свій вебсайт, видавши його за сайт правовласника», і далі — «кіберсквотинг є фактично єдиним правопорушенням, яке зумовлює виникнення доменних спорів». На думку науковця, «потребує спеціального правового регулювання характеристика порушення, яке вважається кіберсквотингом» [19, с. 129].

У дослідженні С. Булеца та А. Тегза запропоновано доповнити Закон України «Про електронну комерцію» «розділом, який би чітко закріпив право власників доменних імен на стягнення збитків з будь-якого, хто реєструє і просуває доменне ім'я, що належить іншій компанії, з метою його подальшого перепродажу. Крім цього, необхідно вдосконалити наявну позасудову систему захисту в сфері захисту від кіберсквотингу, зокрема розмістивши на офіційному сайті графу з алгоритмом захисту при здійсненні досудового розслідування, яка б значно зменшила кількість відповідних позовів» [21, с. 63].

Кіберсквотинг в Україні характерний для всіх доменних зон, що ускладнює вирішення проблеми захисту доменного імені від можливих посягань. З погляду Ю. Науменко, «не існує повноцінного захисту від кіберсквотингу. Чим популярнішим стає сайт — тим

більше у нього з'являється недоброзичливців, які бажають заробити на вашій назві. Щоб захиститися від кіберсквотингу, потрібні чималі кошти, щоб зареєструвати безліч схожих доменів у різних доменних зонах» [22, с. 88–90].

З позиції протидії кіберсквотингу в європейському законодавстві, а саме на загальному рівні — законодавства в Європейському Союзі, то воно спрямоване на: забезпечення ефективного функціонування доменних імен та їх реєстрації; захист прав власників торговельних марок, що мають відповідні доменні імена; вирішення спорів, пов'язаних з доменними іменами, і забезпечення справедливості для всіх сторін; забезпечення безпеки та стабільності інтернету, зокрема у сфері доменних імен. Протидія та захист від кіберсквотингу в ЄС підпадає під поняття недобросовісної конкуренції стосовно прав власників торговельних марок, які мають відповідні доменні імена та розглядають позови в судах за певною процедурою.

У ЄС доменні імена регулюються різними нормативно-правовими актами, серед яких ключовим є Регламент (ЄС) 2019/517 про запровадження та функціонування доменного імені верхнього рівня [23]. Крім того, законодавство ЄС (Закон про торговельні марки (Регламент Європейського Парламенту і Ради (ЄС) № 2017/1001 [24]), забезпечує захист доменних імен, які також є зареєстрованими торговельними марками.

Зазначимо, *домен верхнього (першого) рівня* (top-level domain — TLD) — в ієрархії доменної системи імен (DNS) найвищий. Доменні імена у ЄС є різноманітними і можуть бути як національними (наприклад, .de для Німеччини, .fr для Франції), так і загальними для Євросоюзу (наприклад, .eu). Домени .eu доступні для фізичних та юридичних осіб, які мають зв'язок з ЄС, і можуть бути використані для просування бізнесу або приватних проєктів.

Механізм регулювання доменного імені в ЄС відповідає ст. 4 Регламенту 2019/517, згідно з якою доменне ім'я призначається правомочній стороні, чий запит був отриманий реєстром першим, у технічно правильний спосіб, відповідно до принципу «firstcome-firstget», тобто першості надходження заявки на реєстрацію доменного імені. Зареєстроване доменне ім'я є недоступним для повторної реєстрації до завершення строку першої реєстрації без поновлення або відкликання доменного імені. Реєстратор може відкликати доменне ім'я за власною ініціативою, не передаючи спір на досудове вирішення (ADR) — це метод вирішення конфліктів без звернення до суду. Ідеться про залучення посередника, арбітраж або просто переговори між сторонами для досягнення взаємовигідного рішення, або судову процедуру у випадках заборгованості перед реєстром; невідповідності власника доменного імені критеріям прийнятності; порушення вимог до запитів на реєстрацію, передбачених вказаним регламентом. Доменне ім'я також може бути відкликане і передане іншій стороні після відповідного досудового розгляду або судової процедури, якщо буде виявлено ознаки його недобросовісної реєстрації. Крім того, скасування підлягають доменні імена, визнані рішенням суду держави-члена ЄС такими, що є наклепницькими, расистськими або такими, що суперечать державній політиці чи громадській безпеці відповідно до законодавства Євросоюзу чи національного законодавства, яке відповідає законодавству ЄС.

Регулювання питання використання доменних імен також здійснюється на підставі Виконавчого регламенту Європейської Комісії (ЄС) 2020/857 від 17 червня 2020 року [25], що встановлює принципи, які необхідно включити до договору між Європейською Комісією та Реєстром домену верхнього рівня .eu відповідно до Регламенту (ЄС) 2019/517 Європейського Парламенту і Ради, а також Виконавчого регламенту Європейської Комісії (ЄС) 2022/1862 про створення списків зарезервованих і заблокованих доменних імен у домені верхнього рівня .eu відповідно до Регламенту (ЄС) 2019/517 Європейського Парламенту і Ради [15, с. 7].

Запобігання кіберсквотингу та боротьби з ним у країнах ЄС розглядають шляхом вирішення спорів за певною позасудовою процедурою. Саме в Євросоюзі домінує позасу-

дова процедура на підставі Єдиної політики вирішення спорів стосовно доменних імен (ЄПУС) — UDRP. Вона є стандартизованою позасудовою процедурою вирішення спорів стосовно доменних імен, що розроблена Всесвітньою організацією інтелектуальної власності (ВОІВ) у 1999 році та використовується для швидкого вирішення відповідних спорів у загальних доменах верхнього рівня (gTLD). Це дає змогу власникам торговельних марок швидко і недорого захистити свої права від неправомірного використання їхніх імен у доменних назвах. Спори за процедурою UDRP розглядаються, якщо позивач довів наявність кожного з таких трьох елементів: 1) доменне ім'я ідентичне або оманливо подібне до знака для товарів та послуг, на який позивач має права; 2) відповідач не має законних прав або законних інтересів стосовно доменного імені; 3) доменне ім'я зареєстроване або використовується недобросовісно [26].

На думку Г. Андрощука, «відповідно до ЄПУС подавач скарги зобов'язаний підтвердити для її обґрунтування наявність трьох умов, а саме: 1) доменне ім'я ідентичне торговельній марці, що належить подавачеві скарги, або схоже з ним до ступеня змішання; 2) особа, яка зареєструвала доменне ім'я, не має ніяких прав чи законних інтересів щодо цього доменного імені; 3) доменне ім'я було зареєстровано і використовується «недобросовісно». У разі задоволення скарги за процедурою ЄПУС її подавач може або перейняти контроль над спірним доменним іменем, або зажадати анулювання його реєстрації». «Процедура UDRP є швидшою, ніж розгляд справи в суді: два місяці замість одного року». «...Щоб скарга була успішною, необхідно довести, що торговельна марка заявника ідентична або подібна до ступеня змішання з доменним іменем, реєстрант доменного імені не має прав або законних інтересів з приводу цього доменного імені; а також те, що доменне ім'я зареєстроване або використовується недобросовісно» [27, с. 54].

Експертам пропонується внести низку змін щодо перспективи охорони торговельних марок у рамках ЄПУС: «1) замінити формулювання «недобросовісна реєстрація та використання» формулюванням «недобросовісна реєстрація або використання» з урахуванням ситуацій, коли за допомогою раніше зареєстрованого доменного імені відкрито порушуються права бренда, який виник пізніше; 2) впровадити правило «той, хто програв, платить» (аналогічно практиці, що застосовується в рамках розглядів, пов'язаних із запереченнями проти реєстрації торговельних марок і вимогами про їх анулювання, в ЄС); 3) розробити процедуру подання апеляцій на рішення, прийняті за процедурою ЄПУС, з їх розглядом у рамках ВОІВ. Згідно з чинною системою апеляції повинні подаватися до суду відповідної юрисдикції, що потребує значних витрат часу і ресурсів; 4) передбачити можливість заборони на майбутню реєстрацію нових доменів повторним порушникам прав на доменні імена. До числа інших пропонованих пропозицій входять додавання до тексту правила про позовну давність, зокрема етап посередництва до початку арбітражної фази (наприклад, щоб передбачити можливість видалення гіперпосилання, що випадково порушує правила, без необхідності вилучення у власника самого домену), а також продовження строків відповіді на скарги, пов'язані з передбачуваними порушеннями» [27, с. 54–55].

Щодо перспективи підвищення ефективності експертизи Г. Андрощук акцентує увагу на застосуванні штучного інтелекту (ШІ), який «використовується для аналізу та оцінки об'єктивних ознак «недобросовісності». Так, організація «EURid» (реєстратор доменів у зоні .eu) успішно застосовує ШІ для превентивного аналізу даних про реєстрацію доменів з метою виявлення доменних імен, що реєструються з метою ведення неправомірної діяльності. Відповідно до звітів про роботу програми ШІ в рамках EURid випадки недобросовісної реєстрації доменів вдається виявляти з точністю 92 %» [27, с. 56].

Отже, у ЄС протидія та захист від кіберсквотингу зводиться до розгляду спорів у судах за певною позасудовою процедурою, де домінує ЄПУС — UDRP в ході вирішення спорів стосовно доменних імен, що свідчить про подальше удосконалення цього правового механізму.

Висновки.

1. Економіко-правові особливості кіберсквотингу в умовах цифровізації (кіберфізичного простору) обумовлюють трактування кіберсквотингу як однієї з форм кіберзлочинності, як протизаконну бізнес-діяльність, за якої порушується право на доменні імена, що призводить до негативних економіко-правових наслідків для бізнесу та споживачів.
2. Потребує посилення протидія кіберсквотингу в українському законодавстві шляхом введення в правове поле поняття «кіберсквотинг», застосування економіко-правових механізмів попередження та протидії недобросовісній конкуренції щодо порушення прав інтелектуальної власності на знаки для товарів і послуг, комерційні (фірмові) найменування, авторських прав на доменні імена.
3. Врахувати досвід ЄС стосовно запобігання та боротьби з кіберсквотингом в Україні. Розвивати позасудову процедуру на підставі впровадження Єдиної політики вирішення спорів стосовно доменних імен (ЄПУС) — UDRP. Врахувати перспективи підвищення ефективності експертизи «недобросовісності» із застосуванням штучного інтелекту.

Перелік використаних джерел

1. Манько А. В. Сучасні тенденції застосування інтернет-технологій у бізнесі: Розвиток європейського простору очима молоді: економічні, соціальні та правові аспекти: матеріали Всеукраїнської наук.-практ. конф. докторантів, молодих учених та студентів, м. Харків, 17 травня 2019 року. Харків: ХНЕУ ім. С. Кузнеця, 2019. URL: <https://cdn.hneu.edu.ua/rozvitok19/thesis02-39.html#thesis02-39> (дата звернення: 07.07.2025).
2. Стародуб І. Кіберсквотинг: як захистити «візитівку» бізнесу. Юридична газета. 2022. № 1 (755). URL: <https://jur-gazeta.com/dumka-eksperta/kiberskvoting-yak-zahistiti-vizitivku-biznesu.html> (дата звернення: 07.07.2025).
3. Ходаківський Є. І., Якобчук В. П., Літвінчук І. Л. Інтелектуальна власність: економіко-правові аспекти: навч. посіб. Київ: Центр навчальної літератури, 2014. 276 с.
4. Андрощук Г. О., Шкляр С. В. Конкурентне право: захист від недобросовісної конкуренції: науково-практичне видання. Київ: Юстініан, 2012. 472 с.
5. Булат Н. М. Поняття кіберсквотингу та його види. Правова держава. 2018. № 31. С. 72–80. <https://doi.org/10.18524/2411-2054.2018.31.143453>.
6. Попова Н. О. (2015) Кіберсквотинг як основний вид правопорушень в доменних спорах: Вітчизняний та світовий досвід правового регулювання відносин у сфері інтелектуальної власності: зб. наук. праць за матеріалами Всеукраїнської наук.-практ. Інтернет-конф. / за заг. ред. О. В. Черевка, О. П. Орлюк. Навчально-науковий інститут економіки і права ХНЕУ ім. С. Кузнеця (8 травня 2020 р.). С. 134–137.
7. Коваленко Т. Кіберсквотинг, ринок купівлі та продажу доменів. Теорія і практика інтелектуальної власності. 2013. № 6. С. 40–45.
8. Про електронні комунікації : Закон України від 16.12.2024 р. № 1089-IX. URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text> (дата звернення: 07.07.2025).
9. Яку доменну зону вибрати: найкращі доменні зони для бізнесу і не тільки. HOSTiQ. URL: <https://hostiq.ua/blog/ukr/how-to-choose-domain-zone/> (дата звернення: 07.07.2025).
10. Кіберсквотинг: чесний бізнес чи спекуляція? Natalia.t (20 жовтня 2021). URL: <https://info.nic.ua/uk/blog-uk/kiberskvotyng/> (дата звернення: 07.07.2025).

-
11. Булат Н. М. Поняття брендового кіберсквотингу та шляхи боротьби з ним. *Вісник ОНУ імені І. І. Мечникова. Правознавство*. 2018. Т. 23. Вип. 1(32). С. 98–110. [https://doi.org/10.18524/2304-1587.2018.1\(32\).133826](https://doi.org/10.18524/2304-1587.2018.1(32).133826).
 12. SEO Glossary: Кіберсквотинг. URL: <https://www.ranktracker.com/uk/seo/glossary/cybersquatting/> (дата звернення: 07.07.2025).
 13. Коваль М. Протидія кіберсквотингу: як повернути вкрадене доменне ім'я. *Юридична газета*. 2019. № 47 (701). URL: <https://jur-gazeta.com/publications/practice/informaciune-pravo-telekomunikaciyi/protidiya-kiberskvotingu-yak-povernuti-vkradene-domenne-imya.html> (дата звернення: 07.07.2025).
 14. Про використання доменних імен у спеціальному публічному домені .gov.ua : Закон України від 28.07.2023 р. № 3284-IX. URL: <https://zakon.rada.gov.ua/laws/show/3284-%D0%86%D0%A5#Text> (дата звернення: 07.07.2025).
 15. Парламентське дослідження щодо правової охорони та регулювання використання доменних імен в Україні, Європейському Союзі, державах-членах Європейського Союзу та США (у контексті Закону України «Про використання доменних імен у спеціальному публічному домені .gov.ua» від 28.07.2023 року). URL: <https://research.rada.gov.ua/uploads/documents/33344.pdf> (дата звернення: 07.07.2025).
 16. Кудрицька Т. Доменні спори в Україні: останні тенденції та перспективи застосування альтернативних способів вирішення. *Інтелектуальна власність України*. 2012. № 10. URL: https://vkr.ua/publication/domain_disputes_in_ukraine_latest_trends_and_perspectives_of_alternative_dispute_resolution (дата звернення: 07.07.2025).
 17. Про охорону прав на знаки для товарів і послуг : Закон України № 3689-XII від 15 грудня 1993 року. URL: <https://zakon.rada.gov.ua/laws/show/3689-12#Text> (дата звернення: 07.07.2025).
 18. Цивільний кодекс України : Закон України № 435-IV від 16.01.2003 р. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text> (дата звернення: 07.07.2025).
 19. Петрів М. В. Поняття та ознаки кіберсквотингу. *Науковий вісник Ужгородського національного університету. Серія Право*. 2018. Вип. 52. Том 1. С. 127–130.
 20. Про захист від недобросовісної конкуренції : Закон України № 236/96-ВР 7 червня 1996 року. URL: <https://zakon.rada.gov.ua/laws/show/236/96-%D0%B2%D1%80#Text> (дата звернення: 07.07.2025).
 21. Булеца С. Б., Тегза А. В. Кіберсквотинг як порушення права інтелектуальної власності. *Науковий вісник Ужгородського національного університету. Серія Право*. 2021. Вип. 67. С. 59–63. <https://doi.org/10.24144/2307-3322.2021.67.11>.
 22. Науменко Ю. М. Кіберсквотинг як загроза системі правової охорони доменних імен в Україні. *Право та інноваційне суспільство*. 2016. № 2 (7). С. 86–90.
 23. Regulation (EU) 2019/517 of the European Parliament and of the Council of 19 March 2019 on the implementation and functioning of the .eu top-level domain name and amending and repealing Regulation (EC) No 733/2002 and repealing Commission Regulation (EC) No 874/2004. URL: <https://eur-lex.europa.eu/eli/reg/2019/517/oj/eng> (дата звернення: 07.07.2025).
 24. Регламент Європейського Парламенту і Ради (ЄС) № 2017/1001 від 14 червня 2017 року про торговельну марку Європейського Союзу. URL: https://zakon.rada.gov.ua/laws/show/984_003-17#Text (дата звернення: 07.07.2025).
 25. Commission Implementing Regulation (EU) 2020/857 of 17 June 2020 laying down the principles to be included in the contract between the European Commis-

-
- sion and the .eu top-level domain Registry in accordance with Regulation (EU) 2019/517 of the European Parliament and of the Council. URL: https://eur-lex.europa.eu/eli/reg_impl/2020/857/oj/eng (дата звернення: 07.07.2025).
26. UA-DRP. URL: <https://wiki.drs.ua/UA-DRP> (дата звернення: 12.05.2025).
27. Андрощук Г. Протидія недобросовісним реєстраціям і використанню засобів індивідуалізації в умовах цифрової трансформації. Теорія і практика інтелектуальної власності. 2021. № 1. С. 48–67. <https://doi.org/10.33731/12021.234192>.

Oleksandr Butnik-Siverskyi

Doctor of Economics, Professor, chief researcher of the Sector of IP commercialization of the Department of industrial property and commercialization of the Intellectual Property Scientific Research Institute of the National Academy of Legal Sciences of Ukraine

The cybersquatting as a form of unfair competition: economic and legal features and countermeasures

The author comprehensively researched the economic and legal features of cybersquatting as a computer crime from the position of its economic and legal meaning; economic factors of attractiveness (passivity of business, simplicity of doing business, minimal costs at the start of a business, income from the sale of a domain name, that several times exceeds the costs of its acquisition); identification criteria (unfair intentions, confusing similarity, commercial benefit); prevention and fight against cybersquatting (register relevant domains in advance, monitoring domain registrations, lawsuit, trademark registration); negative economic and legal consequences of cybersquatting for business and consumers (financial losses, brand dilution, consumer fraud, legal costs).

The economic and legal features of cybersquatting are considered from the perspective of the cybersquatting consequences and measures against it. An advanced cybersquatter investigates the economic direction, the intended development strategies of companies, and studies the market situation. The key to a cybersquatter's success is considered to be the ability to choose a prospective name and register a domain that can later become popular and allow to derive material benefits from it.

Cybersquatting is considered as unfair competition, in which domain names are registered that do not belong to intellectual property objects, but at the same time they perform not only the technical function of communication between the server and the end user, but are also a very effective means of individualization of a person, goods and/or services.

The position of counteraction to cybersquatting in Ukrainian legislation has been researched, revealing it to be a poorly regulated phenomenon in terms of scientific and theoretical substantiation, legislative regulation, and judicial practice.

The author considers the countermeasures against cybersquatting in European legislation at a general level, where counteracting and protecting against cybersquatting in the EU falls under unfair competition in relation to the rights of trademark owners, who have the corresponding domain names, using an out-of-court procedure, where the Uniform Domain Name Dispute Resolution Policy — UDRP in generic top-level domains (gTLDs) dominates.

Keywords: cybersquatting, domain name, intellectual property, countermeasures against cybersquatting

*Рекомендовано засіданням відділу промислової власності і комерціалізації
об'єктів інтелектуальної НДІ інтелектуальної власності
(протокол № 11 від 29.10.2025 р.)*

Подано / Submitted: 28.07.2025

Доопрацьовано / Revised: 24.09.2025

Прийнято до публікації / Accepted: 29.10.2025