# РОЗДІЛ 3
# ЦИВІЛЬНЕ ПРАВО І ЦИВІЛЬНИЙ ПРОЦЕС; СІМЕЙНЕ ПРАВО; МІЖНАРОДНЕ ПРИВАТНЕ ПРАВО

DOI https://doi.org/10.24144/2307-3322.2021.67.11
УДК: 347

## КІБЕРСКВОТИНГ ЯК ПОРУШЕННЯ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

**Булеца С.Б.,**
*доктор юридичних наук,*
*професор, завідувач кафедри*
*цивільного права та процесу*
*ДВНЗ «Ужгородський національний університет»*
*ORCID ID: https://orcid.org/00000001-9216-0033*

**Тегза А.В.,**
*студентка 3-го курсу*
*юридичного факультету*
*ДВНЗ «Ужгородський національний університет»*

**Булеца С. Б., Тегза А. В. Кіберсквотинг як порушення права інтелектуальної власності.**

В науковій статті було проведено дослідження правових засад кіберсквотингу в Україні, норм чинного законодавства України та ЄС в сфері антикіберсквотигу та юридичної доктрини. Кіберсквотинг став однією з найсерйозніших проблем, з якою стикаються компанії, що працюють із споживачами. Він полягає в недобросовісній реєстрації, продажі або використанні доменного імені чужої торгової марки з наміром отримання прибутку. Шахраї часто використовують найпоширеніші помилки в написанні доменних імен, торгову марку і колірну схему існуючих компаній, щоб ввести споживачів в оману. Міжнародні методи боротьби вибудовують ефективну стратегію, яка дозволяє перешкоджати більшості порушень у майбутньому, однак інновації у системах відстежування та перешкоджання порушень все ж потребують подальшого вдосконалення, оскільки їхню дію важко обмежити виключно рамками конкретного порушення. Провівши аналіз UDRP як процедури можна прийти до висновку, що вона містить не тільки норми, матеріальні і процесуальні, а й є автономним джерелом регулювання, що надає цій процедурі позадержавних характер. На підставі проведеного дослідження для України автори статті пропонують прийняття антикіберквотингового законодавства, яке значною мірою вирішило б проблеми, викликані спробами адаптувати традиційні правові принципи без шкоди та з цілковитим їх збереженням. У законі слід чітко закріпити 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.

**Ключові слова:** кіберсквотинг, доменне ім'я, антикіберквотингове законодавство, інтелектуальна власність, порушення.

**Buletsa S. B., Tegza A. V. Cybersquatting as a violation of intellectual property rights.**

The scientific article conducted a study of the legal basis of cybersquatting in Ukraine, the current legislation of Ukraine and the EU in the field of anti-cybersquatting and legal doctrine. Cybersquatting has become one of the most serious problems faced by companies working with consumers. It consists in the unfair registration, sale or use of a domain name of another's trademark with the intention of making a profit. Scammers often use the most common mistakes in spelling domain names, trademarks and color schemes of existing companies to mislead con-

sumers. International methods of combating build an effective strategy to prevent most violations in the future, but innovations in tracking and prevention systems still need to be further improved, as it is difficult to limit their effects to a specific violation alone. After analyzing the UDRP as a procedure, we can conclude that it contains not only rules, substantive and procedural, but also is an autonomous source of regulation, which gives this procedure a non-state character. Based on the study for Ukraine, the authors of the article propose the adoption of anti-cyber quoting legislation, which would largely solve the problems caused by attempts to adapt traditional legal principles without harm and with their full preservation. The law should clearly enshrine the right of domain name holders to recover damages from anyone who registers and promotes a domain name owned by another company for resale. In addition, it is necessary to improve the existing out-of-court system of protection in the field of protection against cybersquatting, in particular by placing on the official website a column with a protection algorithm for pre-trial investigation, which would significantly reduce the number of lawsuits.

**Keywords:** cybersquatting, domain name, anti-cyberquoting legislation, intellectual property, infringement.

**Постановка проблеми.** Сьогодні бізнес покладається на Інтернет та електронну комерцію - або шляхом виключного продажу своєї продукції на просторах Інтернету або використання Інтернету як реклами та інформації , тому запобігання порушенню доменних імен з боку кіберсквотерів стають дедалі важливішими для е-користувачів. Окрім цього проблема полягає в тому, що сьогодні в Україні немає спеціального законодавчого регулювання в даній сфері.

**Стан опрацювання проблематики.** Досліджувана тема знаходить своє відображення у працях багатьох авторів-науковців. Особливої уваги заслуговують праці Попова Н., Ляшенко А., Савчук В., Демченко Х., Раєвська К., Петрів М. та інших, які досить обширно розкривають поняття, характерні ознаки кіберсквотингу та механізми протидії йому. Оскільки розробленість даної теми в літературі знаходиться на високому рівні, ми маємо змогу проаналізувати різні джерела, внести навіть свої корективи і зробити відповідні висновки.

**Метою статті** є комплексне дослідження поняття кіберсквотингу, механізмів та способів захисту у сфері протидії кіберсквотингу та аналіз судової практики ЄС та національних судів.

**Виклад основного матеріалу.** Спалах COVID-19 призвів до серйозних змін у бізнесі, а саме до дуже стрімкого використання Інтернет та електронної комерції , які стали незамінним та доцільним джерело для безлічі інформації та миттєвої комунікації. Проте простота передачі інформації через Інтернет має деякі недоліки, одна з яких полягає в тому, що Інтернет може піддати інтелектуальну власність компанії крадіжці та недобросовісному використанні. Кіберсквотинг став однією з найсерйозніших проблем, з якою стикаються компанії, що працюють із споживачами. Він полягає в недобросовісній реєстрації, продажі або використанні доменного імені чужої торгової марки з наміром отримання прибутку. Кіберсквотинг може приймати різні форми, але його мета завжди одна - крадіжка грошей або цінної особистої інформації у користувачів мережі Інтернет.

Кіберсквотинг (англ. cybersquatting) – протизаконна діяльність, що полягає у реєстрації, використанні та пропонуванні до продажу доменного імені із несумлінним наміром отримати прибуток від паразитування на гудвілі або торговельній марці, яка належить іншій особі. Особи, які вчиняють такі дії, називаються кіберсквотерами. Термін «кіберсквотинг» походить від англійського слова «сквот», що означає акт захоплення занедбаного або порожнього місця або будівлі, якою сквотер не володіє, орендує або має дозвіл на використання. Тобто своєрідне «доменне рейдерство» [1].

Серед основних видів кіберсквотингу слід виділити:

- Брендовий – пов'язаний із реєстрацією доменних тотожних чи схожих до відомих торговельних марок чи комерційних найменувань.
- Галузевий – пов'язаний із реєстрацією доменних імен за назвою видів діяльності, товарів чи послуг.
- Географічний – пов'язаний із реєстрацією доменних імен тотожних назвам міст, сіл, географічних районів.
- Захисний – пов'язаний із реєстрацією подібних доменних імен до свого власного.
- Іменний – пов'язаний із реєстрацією доменних імен однакових чи подібних з власними іменами, прізвищами або псевдонімами відомих людей.
- Тайпсквотинг – пов'язаний із реєстрацією доменних імен, які містять помилку у назві відомих веб-сайтів [2, с.126].

Звісно ж, що саме брендовий кіберсквотинг і тайпсквотинг є найбільш небезпечними видами кіберсквотинга, так як вони направлені на отримання переваг в економічній діяльності, можуть заподіяти серйозні збитки і підірвати ділову репутацію. Другі ж види слід називати саме домейнінгом, так як в загальному випадку вони нешкідливі і можуть вважатися правопорушенням тільки в тому випадку, якщо відповідають умовам, виділеним для визначення незаконного кіберсквотинга.

На європейському рівні поруч із судовим досить поширеним є вирішення спорів щодо доменних імен у позасудовому порядку, зокрема, способами альтернативного врегулювання спорів. Зокрема, спори вирішуються у порядку процедури UDRP (Uniform Domain Name Dispute Resolution Policy) – Єдиної політики вирішення спорів щодо доменних імен, затвердженої ICANN (Internet Corporation of Assigned Names and Numbers) – організація, що на міжнародному рівні вирішує питання функціонування мережі Інтернет, у тому числі щодо доменів).

Спори за вказаною процедурою можуть розглядатись 5 акредитованими організаціями (Approved Dispute Resolution Service Providers, далі – арбітражні суди), серед яких: Азійський центр з вирішення доменних спорів; Національний Арбітражний Форум; Центр ВОІВ з Арбітражу та Посередництва; Чеський арбітражний суд; арабський центр з вирішення спорів.) [3].

Найбільш поширеними є системи ADR(Alternative dispute resolution) – альтернативне вирішення спорів, на базі UDRP (безпосередньо застосовуючи UDRP або адаптації UDRP), але деякі юрисдикції розробили власні системи ADR, а інші передбачати лише судові розгляди.

Щодо системи на основі UDRP, то у 1999 році ICANN створила єдине вирішення суперечок щодо доменних імен за політикою (UDRP). Це набір правил вирішення суперечок на основі традиційного національного закону про торговельні марки, адаптованого для потреб Інтернету. UDRP не отримує своєї юридичної сили від прийняття законодавчим органом, і в цьому сенсі не є законом. Швидше, це договір підряду включені в угоди про реєстрацію доменних імен відповідно до якого реєстрант приймає "юрисдикцію" одного з п'яти вирішень спорів постачальників даних послуг. Маючи справу UDRP потрібно пам'ятати , що він повністю базується на договорі [4, с.827]. Отже, UDRP передбачає «Вікно» десяти днів для незадоволеної сторони розпочати провадження у справі судом, а якщо таке провадження розпочато, в провадженні UDRP рішення колегії призупиняється. У ЄС деякі країни такі, як Румунія та Кіпр безпосередньо прийняли UDRP без змін як єдину систему вирішення їх суперечок щодо доменних імен ccTLD (Ім'я домену верхнього рівня коду країни).

У деяких країнах існують системи ADR, на які впливає UDRP, тобто жертви кіберсквотингу можуть піти кількома шляхами домагаючись захисту своїх прав. По-перше, як і в країнах, що надають у справах UDRP завжди є можливість подати позов до державного суду. Крім того, багато країн Європи прийняли власні внутрішні ADR політики, в основному засновані на UDRP, затверджені відповідним доменним іменем повноваження [5]. Примітно, що юрисдикцію державного суду не може бути скасовано, що є основним критерієм, що об'єднує правила, розглянуті в цій групі. Представниками його є Бельгія, Нідерланди та Швеція.

Також існують, незалежно розроблені системи ADR, тобто ті, які розробляються самостійно від UDRP. Вони попередньо класифікуються на два підрозділи, а саме ADR та «класичний арбітраж». І все-таки перша група поділяє деякі загальні концепції з UDRP, особливо той факт, що їхня процедура не призводить до остаточних юридично обов'язкових рішень [6]. Ще один своєрідний, але оригінальний набір правил ADR походить з Болгарії. Це суттєво відступає від систем, проаналізованих вище, головним чином завдяки тому факту, що для цього не потрібні недобросовісні наміри реєстранта, який оспорює реєстрацію. Загалом механізм ADR у Register.bg є наступне: По-перше, реєстрант має можливість отримати реєстрацію свого доменного імені як «Захищене» доменне ім'я. Для цього він повинен довести дійсне право на доменне ім'я, яке може виникнути з дуже широкого набору фактів. Відсутність будь-якої з цих підстав автоматично робить домен реєстрація імені "Незахищений". Практична значимість такого поділу доменних імен на захищені та незахищені відбувається пізніше в процедурі арбітражу, при якій скаржник посилається на одного з чотирнадцяти прав, перелічених у Правилі 5.5.1. [7], може вимагати передачі незахищеного доменного імені від реєстранта, не роблячи додаткових показів. Арбітражна процедура проводиться до суперечки комітетом Register.bg і проводиться досить швидко. Процедура є суто приватна та не забороняє позов у національних судах [8].

Слід заначити, що, наприклад, процедура в Чеській Республіці є типовим арбітражем, а саме компетентним Арбітражним судом є Арбітражний суд при Економічній Палаті Чехії та сільськогосподарській палаті Чеської Республіка. Юрисдикція цього арбітражного суду не обмежена та застосовується виключно до випадків кіберсквотингу. Його джерелом юрисдикції є угода між реєстрантом та реєстратором, що застосовують Правила альтернативного спору. Ця угода, по суті, є арбітражним застереженням, яке зобов'язує реєстранта до вчинення певних дій. Через контрактний характер арбітражної угоди, треті сторони мають як арбітраж, так і засоби загального судового захисту розпорядження щодо претензій щодо реєстрації доменних імен. Арбітражне застереження насправді є публічною пропозицією арбітражу, яке є лише обов'язковим для реєстранта [9].

Таким чином, потенційна третя сторона-скаржник може подати таку угоду до третейського суду та розпочати арбітраж або подати позов до загального суду. У разі арбітражу рішення є обов'язковим і підлягає виконанню однаково як рішення, винесене судом загальної юрисдикції. Як і в більшості арбітражних систем у світі, як тільки арбітр прийняв юрисдикцію, яка становила б lis pendens (письмове повідомлення що сто-

сується або права власності на нерухомість, або заявленого права власності на нього) щодо суду, останній повинен відмовити у юрисдикції або припинити провадження у разі його порушення [10].

Деякі країни взагалі не прийняли жодної системи ADR, отже, загальний суд є єдиним органом, який розглядає суперечки стосовно кіберсквотингу. Це скоріше виняток, ніж правило. В ЄС прикладами країн, що застосовують цю політику, є Німеччина, Австрія та Словаччина. Німеччина є юрисдикцією, що має першочергове значення для перейняття досвіду Україною. Перш за все, це країна з найбільшою кількістю реєстрацій ccTLD в Європі та друга у світі - 15,4 млн. Той факт, що Суди Німеччини мають виключну юрисдикцію у справах доменних імен демонструє, що в цій країні відносна ефективність німецької судової влади та простота виконання торговельної марки та інших прав промислової власності, а також низька кількість випадків кіберсквотингу. Але незважаючи на хороші показники Німеччина у будь-якому випадку планує введення подвійного захист від кіберсквотингу, але навряд це буде реалізовано найближчим часом [11]. Отже, німецький закон про доменні імена є зразковий серед ccTLD. Німеччина також викликає інтерес, оскільки не має спеціальне законодавство про боротьбу з кіберсквотингом, а отже, боротьба з кіберсквотингом провадиться засобами, «витягнутими» із традиційних правових принципів.

Що стосується позасудового захисту, то в Україні був впроваджений Домен верхнього рівня UA, що є складовою частиною всесвітньої системи доменних імен, що її адмініструє «Інтернет корпорація з присвоєння імен і номерів» (ICANN). В ньому існують правила домену UA розроблені адміністратором домену UA з дотриманням чинних правил ICANN, з урахуванням рекомендацій ICANN, а також міжнародного досвіду, і є умовами надання адміністратором домену UA третім особам послуг з адміністрування та технічного супроводу домену UA. Відповідно до рішення експертної групи, впровадження процедури позасудового розгляду спорів буде проходити поетапно. На першому етапі «Хостмайстер» і реєстратори доменних імен внесуть зміни у свої договори, після чого стане можливим використання UDRP під час урегулювання спорів, пов'язаних із доменними іменами другого рівня. Через півроку передбачено ухвалення рішення про використання UDRP у доменних іменах третього рівня [12].

Отже, міжнародні методи боротьби вибудовують ефективну стратегію, яка дозволяє перешкоджати більшості порушень у майбутньому, однак інновації у системах відстежування та перешкоджання порушень все ж потребують подальшого вдосконалення, оскільки їхню дію важко обмежити виключно рамками конкретного порушення. Провівши аналіз UDRP як процедури можна прийти до висновку, що вона містить не тільки норми, матеріальні і процесуальні, а й є автономним джерелом регулювання, що надає цій процедурі позадержавних характер.

Звертаючись до аналізу судової практики європейських країн, то багато з них побудували суцільну судову практику, що стосується доменних імен, котрі порушують торгові марки. Так Французька судова влада наблизила широко відомі знаки захисту в оригінальний спосіб у контексті доменних імен. У відомій справі Christiane L. / Sa L'Oréal [13] позивач «L'Oréal parce que je le vaux bien » подав позов проти відповідача за створення веб-сайтів під доменним іменем «parce que je le vaux bien» різними доменами верхнього рівня. Веб-сайти були присвячені збору монет, що зовсім відрізнялось від операцій позивача. Було встановлено, що підсудний навмисно використовували славу торгової марки, хоча вона була в іншому класі та заборонено пані Л. відтворювати чи використовувати будь-яким способом, повністю або частково, торгову марку L'Oréal під штраф 150 євро на день затримки через п'ятнадцять днів з моменту постановлення рішення.

Справа приводить нас до оригінального аргументу щодо кіберсквотингу, що включає блокування реєстрації. За такого сценарію як обговорено вище, важко підтримувати будь-яке використання в торгівлі з розумною аргументацією або ймовірністю плутанини. Отже, власник торгової марки залишається без належної причини позову проти кіберсквотера.

Також, вагомою проблемою є недобросовісна конкуренція кіберсквотингу приклади такої практики можна знайдені в Чехії. Зокрема, у справі ibico.cz/mobile.cz [14],відповідач, який керував бізнесом, щодо продажу офісних машин для оформлення та обробки документів зареєструвала доменне ім'я ibico.cz. Він керував кількома іншими магазинами під різними доменними іменами, такими як mobile.cz, де він займався продажем офісної техніки, але не товарів позивача. Важливим було те що відповідач зазначив, що він пропонував продати доменне ім'я, про яке йдеться, позивачу за сума € 20000. Позивач займався виробництвом офісу техніка під торговою маркою Ibico, на яку він мав реєстрацію. позов щодо торговельної марки не вдався, оскільки відповідач не продавав жодної продукції котра охоплюється товарним знаком позивача на веб-сайті ibico.cz. Суд правильно заперечив, що «сама реєстрація маркування ідентичний тому, що захищений товарним знаком, являє собою порушення прав від товарних знаків без будь-яких інших умов". Тоді суд посилався на недобросовісну конкуренцію відповідно до §44 Цивільного кодексу Чеської Республіки. Було виявлено, що існував конкурентні відносини між позивачем та відповідачем, оскільки обидва продано офісну техніку для обробки документів.

Судова практика зарубіжних країн не визнає доменне імена товарними знаками, але вважає, що захоплення доменного імені, схожого з товарними знаком, є порушенням прав власника даного товарного знака. В більшості країн в даний час не існує спеціальних законів, що охороняють права на доменний імена. Це дає можливість кіберсквотером реєструвати величезна кількість доменних імен з метою їх подальшого перепродажу. Практика українських судів у вирішенні доменних спорів, на жаль, неоднозначна та нестабільна. Судам варто звертати увагу на міжнародні правила регулювання спорів у сфері доменних імен, але слід зазначити, що застосування іноземного досвіду для модифікації національної системи правової охорони прав в мережі Інтернет вимагає особливої уваги до специфіки підходів, які використовуються порушниками.

В цілому можна зробити висновок, що система, розроблена ВОІВ, явно має певні переваги: суперечка розглядають кваліфіковані фахівці причому в дуже стислі терміни. Іноземні юрисдикції у здійсненні своєї політики щодо захисту від кіберсквотингу покладаються на новітні методи боротьби із порушеннями. І хоча вільний обмін інформацією є одним із фундаментальних принципів відносин в мережі Інтернет, іноземна практика демонструє здатність відповідати сучасним викликам та успішно розмежовувати добросовісну реалізацію прав користувачів та зловживання такими правами.

Таким чином, враховуючи вищевикладене та на основі проаналізованого матеріалу, ми пропонуємо 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.

## Список використаних джерел:


1. Киберсквоттинг (англ. cybersquatting – захват доменов) – проблемы защиты доменного имени. URL:https://pravorub.ru/articles/13827.html (Дата звернення 10.04.2021).
2. Петрів М.В. Кіберсквотинг як вид недобросовісної конкуренції. Матеріали науково-практична конференція «Актуальні проблеми інтелектуального, інформаційного та ІТ права» м. Львів, 17-18 травня 2019 р. С.125-127.
3. Савчук В. Демченко Х. Європейський захист від кіберсквотера. Де пасе задніх Україна. «Європейська Правда». URL:https://www.legalalliance.com.ua/publikacii/evropejskij-zahist-vid-kiberskvotera-de-pase-zadnih-ukrain (Дата звернення 10.04.2021).
4. Sharrock, Lisa M., The Future of Domain Name Dispute Resolution: Crafting Practical International Legal Solutions from Within the UDRP Framework (Майбутнє вирішення суперечок щодо доменних імен: розробка практичних міжнародно-правових рішень у рамках UDRP).Юридичний журнал герцога Вип. 51, No 2 (листопад, 2001) , С. 817-849.
5. Про близькість між бельгійським ADR та UDRP URL:http://dns.be/en/legal/domain_name_disputes/adr_procedure (Дата звернення 10.04.2021).
6. Torsten Bettinger ed., al domain name law and practice (Torsten Bettinger ed., 2005). URL:http://www.iana.org/domains/root/db (Дата звернення 10.04.2021).
7. The domain name registry for UK. URL:http://www.nominet.org.uk/disputes/when-use-drs/policy-and-procedure/drs-policy (Дата звернення 10.04.2021).
8. Dispute Resolution Policy Dispute Resolution Regulations for .nl Domain Names.URL:https://www.sidn.nl/fileadmin/downloads_en/Procedures/Dispute%20Resolution (Дата звернення 10.04.2021).
9. CEPANI, Belgian Centre for Arbitration and Mediation, Rules for Domain Name Dispute Resolution URL:http://www.cepina.be/EN/Default.aspx?PId=900 (Дата звернення 10.04.2021).
10. Czech Arbitration Court's Supplemental Rules to ICANN's Uniform Domain Name URL:https://www.icann.org/en/dndr/udrp/uniform-rules.htm (Дата звернення 10.04.2021).
11. Meissner Bolte. Germany: Fight for your (domain name) rights. March №1 2017. (Мейснер Болте. Німеччина: Боріться за свої права на (доменне ім'я).URL:https://www.lexology.com/library/detail.aspx?g=1e7fa208-c738-4ef1-98ab-fffd2e3fa4ce (Дата звернення 10.04.2021).
12. Світові практики розв'язання доменних спорів для домену .UA. URL:https://hostmaster.ua/news/?pr20181221 (Дата звернення 10.04.2021).
13. Case of Christiane L. / Sa L'Oréal Versailles, 14e ch., Jan. 8, 2003, URL:https://www.legalis.net/jurisprudences/cour-dappel-de-versailles-14eme-chambre-arret-du-8-janvier-2003/ (Дата звернення 10.04.2021).
14. Case of ibico.cz/mobile.cz Prague, 4 June 2007 URL:http://www.nic.cz/page/314/rules-andpolicies under № 82b (Дата звернення 10.04.2021).