

DOI 10.34132/mspc2026.03.13.04

Дмитро Слободянюк

ЕКОНОМІКО-ПРАВОВІ ЗАСАДИ ПРОТИДІЇ КІБЕРСКВОТИНГУ В УМОВАХ ЦИФРОВІЗАЦІЇ: ВІТЧИЗНЯНИЙ ТА ЄВРОПЕЙСЬКИЙ ДОСВІД

У тезах досліджено природу кіберсквотингу як деструктивного явища в умовах розвитку цифрової економіки. Проаналізовано наукові підходи до визначення поняття «кіберсквотинг» та його основних видів. Розглянуто особливості правового регулювання доменних імен в Україні та виявлено прогалини у вітчизняному законодавстві щодо захисту прав інтелектуальної власності в мережі «Інтернет». Особливу увагу приділено досвіду Європейського Союзу, зокрема процедури позасудового врегулювання спорів UDRP та використанню штучного інтелекту для виявлення недобросовісних реєстрацій. Сформульовано пропозиції щодо вдосконалення українського законодавства шляхом імплементації міжнародних стандартів захисту від недобросовісної конкуренції.

Ключові слова: цифровізація, кіберсквотинг, доменне ім'я, інтелектуальна власність, недобросовісна конкуренція, штучний інтелект.

В умовах глобальної турбулентності цифровізація стає не просто трендом, а фундаментальним драйвером економічного поступу, що визначає стратегічну конкурентоспроможність цілих держав. Вона радикально трансформує якісні та кількісні показники господарської діяльності, оптимізуючи операційні витрати та кардинально підвищуючи результативність бізнес-процесів. Завдяки впровадженню хмарних технологій, великих даних та штучного інтелекту, сучасні підприємства отримують можливість масштабуватися поза межами фізичних кордонів, перетворюючи інформацію на ключовий виробничий ресурс.

Вихід підприємства у цифровий простір сьогодні є фактичним актом легітимізації бізнесу в очах споживача; відсутність компанії в мережі автоматично маркує її як нерелевантну сучасним ринковим запитам. Технічним фундаментом такої присутності виступає хостинг – фізичне та логічне місце розміщення активів компанії в мережі, що забезпечує безперервний доступ до її інтелектуального капіталу. Втім, доменне ім'я в цій системі перестає бути просто технічною адресою, набуваючи статусу цінного нематеріального активу, що акумулює в собі гудвіл та ділову репутацію суб'єкта господарювання.

Проте швидкість технологічного розвитку об'єктивно випереджає темпи правової адаптації, що створює сприятливий ґрунт для появи специфічних загроз та нових форм протиправної поведінки. Виникає так званий «правовий лаг» – розрив між виникненням інноваційної моделі зловживання та формуванням ефективної норми стримування. Однією з найбільш деструктивних серед таких загроз є кіберсквотинг. Ця діяльність не лише завдає прямих фінансових збитків правовласникам через втрату трафіку або витрати на викуп доменів, а й системно підриває довіру до цифрових інститутів та електронної комерції загалом.

Кіберсквотинг деформує ринкове середовище, створюючи штучні бар'єри для добросовісних учасників та вводячи в оману кінцевих споживачів, які ризикують стати жертвами фішингу або контрафактної продукції. Така ситуація змушує наукову та юридичну спільноту до активного пошуку дієвих правових інструментів для нівелювання проявів недобросовісної конкуренції. Актуальним стає питання не просто захисту окремої торгової марки, а створення комплексної екосистеми цифрової безпеки, де правові санкції гармонійно поєднуються з технічними протоколами верифікації.

Кіберсквотинг сьогодні – це не монолітне явище, а розгалужена система зловживань. Відповідно до усталеної класифікації [1], виділяють такі види:

- брендовий та іменний: пряма атака на репутаційні активи особи чи компанії;
- галузевий і географічний: монополізація загальних термінів для переходу трафіку;
- авторський, зворотний та аукціонний: складні схеми маніпуляції правом;
- захисний та тайпсквотинг: використання помилок користувачів при введенні адреси.

Деталізація представлених видів дозволяє простежити еволюцію таких зловживань. Зокрема, брендовий кіберсквотинг є найбільш агресивною формою, оскільки він прямо експлуатує впізнаваність відомих торговельних марок для переспрямування лояльної аудиторії на сторонні ресурси. У свою чергу, тайпсквотинг базується на

когнітивних особливостях поведінки користувачів: реєстрація доменів на kшталт gogle.com замість google.com дозволяє зловмисникам отримувати колосальний трафік за рахунок звичайної неухважності людей.

Особливої уваги з позиції права заслуговує зворотний кіберсквотинг. Це ситуація, коли велика корпорація намагається через правові механізми відібрати доменне ім'я у добросовісного власника, який зареєстрував його раніше, мотивуючи це своїм правом на однойменну торговельну марку. Це створює небезпечний прецедент маніпуляції нормами інтелектуальної власності, де вже сам правовласник виступає агресором.

Галузевий та географічний кіберсквотинг мають виражений спекулятивний характер. Реєстрація загальних назв (наприклад, lawyer.ua або kyiv.com) створює штучний дефіцит на ринку цифрових адрес. Це змушує реальний бізнес або викупляти ці домени за цінами, що в сотні разів перевищують собівартість реєстрації, або використовувати менш ефективні назви, що безпосередньо впливає на витрати на маркетинг та загальну вартість залучення клієнта.

Таким чином, кожна з наведених форм кіберсквотингу не лише порушує майнові права правовласників, а й викривляє ринкове середовище, створюючи перешкоди для вільної та чесної конкуренції в інтернет-просторі. Розуміння механіки цих зловживань є ключовим для розробки адекватних контрзаходів, що поєднували б юридичну відповідальність із технічними бар'єрами на рівні реєстраторів.

Історія кіберсквотингу як специфічного цифрового феномену бере свій початок у 1990-х роках, у період стихійної комерціалізації мережі Інтернет. На світанку цифрової ери реєстрація доменних імен відбувалася за принципом «першої заявки» без належної перевірки на відповідність торговельним маркам, чим скористалися перші зловмисники. Ключовою передумовою розквіту цього явища стала низька вартість реєстрації домену у порівнянні з потенційною ринковою вартістю бренду, а також недосконалість міжнародного законодавства, яке не встигало за темпами розвитку віртуального простору.

Трансформація кіберсквотингу свідчить про його перехід від випадкової реєстрації за принципом першочерговості до стратегічно спланованої та технологічно оснащеної форми недобросовісної конкуренції. Це технологічна гонка. Сучасні зловмисники використовують ботів для миттєвого перехоплення доменів, що звільняються. Тому боротися з алгоритмами порушників можна лише за допомогою ще досконаліших алгоритмів захисту.

Наукова думка щодо природи цього явища постійно еволюціонує. Зокрема, Т. Коваленко розглядає кіберсквотинг через призму привласнення доменів, що дублюють відомі торговельні марки [2]. Водночас Н. Булат акцентує увагу на глибинному порушенні прав інтелектуальної власності, трактуючи це як недобросовісну реєстрацію ідентифікаторів, тотожних об'єктам правової охорони [3].

Вважаємо за необхідне підкреслити, що за своєю суттю кіберсквотинг є формою інтелектуального рекету. Це спекулятивне резервування імен з метою подальшого фінансового шантажу законних власників. Окрім прямого вимагання коштів, зловмисники часто використовують такі домени як плацдарм для фішингових атак, розповсюдження шкідливого програмного забезпечення або збору конфіденційних даних ошуканих клієнтів. Економіко-правовий аналіз дозволяє кваліфікувати цю практику як таку, що має ознаки паразитування на чужій діловій репутації. Низький поріг входу та потенційно колосальні прибутки, про які зазначає Н. Попова [4], роблять цю діяльність надзвичайно привабливою для кіберзлочинців.

Економічним наслідком кіберсквотингу для бізнесу є не лише прямі фінансові втрати через необхідність викупу домену, а й репутаційні ризики: використання схожих імен для фішингу або розміщення некоректного контенту розмиває цінність бренду в очах споживача. Для цифрової економіки загалом наслідки проявляються у спотворенні добросовісної конкуренції та створенні штучних бар'єрів для виходу законних власників активів на нові ринки, що зрештою зумовило появу таких регуляторних механізмів, як Anticybersquatting Consumer Protection Act (ACPA) у США та міжнародної політики UDRP.

ACPA – це перша у світі масштабна спроба криміналізувати кіберсквотинг на державному рівні. Його поява була відповіддю на неспроможність класичного законодавства про торговельні марки захистити власників брендів у віртуальному просторі. Законодавством дозволено власникам торговельних марок подавати позови проти осіб, які з «недобросовісним наміром отримати прибуток» реєструють, використовують або продають доменні імена, що є ідентичними або схожими до ступеня змішування з охоронюваними торговельними марками. Головною особливістю ACPA є можливість застосування процедури in rem. Це означає, що якщо власника домену неможливо знайти або він перебуває під іншою юрисдикцією, позивач може подати позов безпосередньо проти самого доменного імені за місцем знаходження реєстратора.

UDRP – це міжнародний стандарт, розроблений корпорацією ICANN спільно з ВОІВ (WIPO) у тому ж 1999 році. На відміну від ACPA, це не закон конкретної країни, а система адміністративного (позасудового) врегулювання. Це обов'язкова умова договору при реєстрації будь-якого домену в загальних зонах (gTLD, як-от .com, .net, .org). Реєструючи домен, особа автоматично погоджується на участь в арбітражі, якщо виникне спір. Спір розглядається незалежними експертами (арбітрами) без участі державних судів. Це значно швидше та дешевше, ніж класичний судовий розгляд. Рішення арбітражу є обов'язковим для реєстратора: якщо арбітр вирішить, що домен вкрадено, реєстратор просто переоформлює його на позивача.

На нашу думку, ці механізми ідеально доповнюють один одного: ACPA забезпечує потужний судовий захист із

можливістю відшкодування збитків, тоді як UDRP пропонує бізнесу глобальний, швидкий та недорогий інструмент для повернення своїх цифрових активів у будь-якій точці світу. Для українського законодавства саме модель UDRP виглядає найбільш перспективною для адаптації, оскільки вона дозволяє розвантажити судову систему та забезпечити оперативність, критично важливу для IT-сфери, оскільки ситуація в Україні в цій сфері залишається складною.

На сучасному етапі доменні імена фактично виведені за межі об'єктів права інтелектуальної власності як самостійні одиниці. Ми спостерігаємо правовий вакуум: відсутність консолідованої міжнародної та національної бази створює умови, за яких домен сприймається лише як технічний елемент маршрутизації.

Прийняття Закону щодо доменів у зоні .gov.ua [5] стало важливим прецедентом, проте воно вирішило проблему лише в державному секторі. Приватний сегмент (зона .UA) залишається «сірою зоною». На мій погляд, парадоксальною є ситуація, коли за наявності норм ЦК України щодо охорони комерційних найменувань (ст. 489) [6], реальний захист у доменних спорах є надто дорогим та тривалим процесом. Ю. Науменко слушно зазначає, що популярність ресурсу автоматично робить його мішенню для «паразитів» [7], а превентивна реєстрація всіх можливих варіацій домену є економічно виснажливою для бізнесу.

Досвід ЄС демонструє ефективність комплексного підходу. Регламент (ЄС) 2019/517 та система ADR пропонують механізм, де реєстратор може оперативно реагувати на порушення без залучення громіздкої судової машини. Центральне місце тут посідає Єдина політика вирішення спорів (UDRP). На мою думку, саме впровадження критеріїв «триелементного тесту» (схожість, відсутність прав, недобросовісність) є тим стандартом, якого потребує українська судова практика [8].

Перспективними виглядають ініціативи Г. Андрощука щодо модернізації UDRP, зокрема впровадження правила «програв – платить» та створення апеляційних інстанцій [9]. Це дозволить відсіяти завідомо безпідставні скарги та підвищити відповідальність сторін. Окремої уваги заслуговує технологічний аспект: успіх організації EURid у використанні ШІ доводить, що боротьба з кіберсквотингом у майбутньому буде автоматизованою та превентивною.

У сучасній архітектурі глобального ринку доменне ім'я трансформувалося з технічної адреси у фундаментальний нематеріальний актив. Кіберсквотинг – це не просто поодинокі юридичні інциденти, а системна деструктивна практика, що підриває цифровий суверенітет бренду – здатність суб'єкта господарювання повноцінно контролювати свою репутацію, ідентичність та канали комунікації в мережі. Посягання на доменне ім'я фактично означає відчуження частини клієнтського капіталу компанії, що в умовах цифрової трансформації може призвести до повної втрати ринкових позицій.

Для ефективної протидії цьому явищу в Україні першочерговим завданням є подолання правової невизначеності. Законодавче закріплення дефініції «кіберсквотинг» на рівні профільного законодавства дозволить вивести цю діяльність із «сірої зони». Це дасть змогу правоохоронним та судовим органам чітко кваліфікувати захоплення доменів як акт недобросовісної конкуренції. Така визначеність усуне потребу в складних лінгвістичних експертизах та спростить процес доказування наміру недобросовісного використання чужої репутації.

Нинішня судова система України в питаннях доменних спорів часто є надто інертною, дорогою та технічно складною для малого та середнього бізнесу. Доцільним вбачається створення Спеціалізованого центру вирішення доменних спорів, який би функціонував на засадах адміністративного арбітражу за міжнародною моделлю Uniform Domain-Name Dispute-Resolution Policy. Така процедура вирішення конфлікту скорочується з років до місяців. Крім того, значно знижує фінансовий поріг входу в судовий процес, що дозволить невеликим компаніям захищати свої права без надмірних витрат на адвокатське супроводження в судах загальної юрисдикції.

На шляху до європейської інтеграції та побудови безпечної цифрової економіки Україна має запроваджувати проактивні методи захисту. Інтеграція інструментів штучного інтелекту та машинного навчання в алгоритми реєстратора доменів зони .UA дозволить реалізувати концепцію «безпечної реєстрації». ШІ здатен в режимі реального часу аналізувати нові заявки на предмет:

- 1) фонетичної та візуальної схожості з уже зареєстрованими торговельними марками;
- 2) виявлення ознак тайпсквотингу та автоматичного маркування підозрілих транзакцій.

Такий підхід не лише мінімізує кількість майбутніх спорів, а й підвищує інвестиційну привабливість українського сегмента інтернету, роблячи його прогнозованим та захищеним за найвищими міжнародними стандартами. Тільки через синергію правових інновацій та технологічного контролю в Україні буде забезпечено сталий розвиток вітчизняного сегменту інтернету та захищено інтереси як бізнесу, так і споживачів.

References

1. Khodakivskyi, Ye.I., Yakobchuk, V.P., & Litvinchuk, I.L. (2014). *Intelektualna vlasnist: ekonomiko-pravovi aspekty [Intellectual property: economic and legal aspects]*. Kyiv: Tsentr navchalnoi literatury. Retrieved from: http://ir.polissiauniver.edu.ua/bitstream/123456789/2861/3/Intelektualna_vlasnist_ekonomiko_pravovi_aspekty.pdf [in Ukrainian].

2. Kovalenko, T. (2013). Kiberskvotynh, rynek kupivli ta prodazhu domeniv [Cybersquatting, the domain purchase and sale market]. *Teoriia i praktyka intelektualnoi vlasnosti – Theory and practice of intellectual property*, 6, (pp. 40-45). Retrieved from: http://www.ndiiv.org.ua/Files2/2013_6/2013_06.pdf [in Ukrainian].
3. Bulat, N.M. (2018). Poniattia brendovoho kiberskvotynhu ta shliakhy borotby z nym [The concept of brand cybersquatting and ways to combat it]. *Visnyk ONU imeni I.I. Mechnykova. Pravoznavstvo – Herald of ONU named after I.I. Mechnikov. Law*, 23 (1(32)), (pp. 98-110). Retrieved from: <https://heraldlaw.onu.edu.ua/article/view/133826>. DOI: [https://doi.org/10.18524/2304-1587.2018.1\(32\).133826](https://doi.org/10.18524/2304-1587.2018.1(32).133826) [in Ukrainian].
4. Popova, N.O. (2015). Kiberskvotynh yak osnovnyi vyd pravoporushen v domennykh sporakh [Cybersquatting as the main type of offense in domain disputes]. *Vitchyzniani ta svitovyi dosvid pravovoho rehulivannia vidnosyn u sferi intelektualnoi vlasnosti – Domestic and world experience of legal regulation of relations in the field of intellectual property*, (pp. 134-137). Kharkiv: KhNEU im. S. Kuznetsia. Retrieved from: <https://eprints.cdu.edu.ua/2766/> [in Ukrainian].
5. Zakon Ukrainy Pro vykorystannia domennykh imen u spetsialnomu publicnomu domenii .gov.ua No. 3284-IX [Law of Ukraine On the use of domain names in the special public domain .gov.ua No. 3284-IX]. *zakon.rada.gov.ua*. Retrieved from: <https://zakon.rada.gov.ua/laws/show/3284-%D0%86%D0%A5#Text> [in Ukrainian].
6. Zakon Ukrainy Tsyvilnyi kodeks Ukrainy No. 435-IV [Law of Ukraine Civil Code of Ukraine No. 435-IV]. *zakon.rada.gov.ua*. Retrieved from: <https://zakon.rada.gov.ua/laws/show/435-15#Text> [in Ukrainian].
7. Naumenko, Yu.M. (2016). Kiberskvotynh yak zahroza systemi pravovoi okhorony domennykh imen v Ukraini [Cybersquatting as a threat to the system of legal protection of domain names in Ukraine]. *Pravo ta innovatsiine suspilstvo – Law and innovative society*, 2 (7), (pp. 86-90) [in Ukrainian].
8. Regulation (EU) 2019/517 on the implementation and functioning of the .eu top-level domain name. *eur-lex.europa.eu*. Retrieved from: <https://eurlex.europa.eu/eli/reg/2019/517/oj/eng> [in English].
9. Androshechuk, H. (2021). Protydiia nedobrosovisnym reiestratsiiam i vykorystanniu zasobiv indyvidualizatsii v umovakh tsyfrovoi transformatsii [Countering unfair registrations and the use of means of individualization in the context of digital transformation]. *Teoriia i praktyka intelektualnoi vlasnosti – Theory and practice of intellectual property*, 1, (pp. 48-67). Retrieved from: <https://drive.google.com/file/d/16X1P0KypnD949q-ypcL5QutWgjfDA8Q3/view>. DOI: <https://doi.org/10.33731/12021.234192> [in Ukrainian].

DOI 10.34132/mspc2026.03.13.04

Dmytro Slobodianiuk

ECONOMIC AND LEGAL PRINCIPLES OF COUNTERING CYBERSQUATTING IN THE CONTEXT OF DIGITALIZATION

The abstract explores the nature of cybersquatting as a destructive phenomenon within the development of the digital economy. Scientific approaches to defining the concept of "cybersquatting" and its primary types are analyzed. The features of legal regulation of domain names in Ukraine are examined, highlighting gaps in national legislation regarding the protection of intellectual property rights on the Internet. Particular attention is paid to the experience of the European Union, specifically the UDRP dispute resolution procedure and the use of artificial intelligence to detect bad-faith registrations. Proposals are formulated to improve Ukrainian legislation by implementing international standards for protection against unfair competition.

Keywords: digitalization, cybersquatting, domain name, intellectual property, unfair competition, artificial intelligence.

Відомості про автора / Information about the author

Дмитро Слободянюк, доктор філософії в галузі публічного управління та адміністрування, викладач кафедри публічного управління та адміністрування, Юридичного факультету, Чорноморського національного університету імені Петра Могили, м. Миколаїв, Україна. E-mail: slobodyanyuk.dmitry@gmail.com, orcid: <https://orcid.org/0000-0001-6281-1907>.

Dmytro Slobodianiuk, Doctor of Philosophy in Public Management and Administration, Lecturer of the Department of Public Administration and Management, Faculty of Law, Petro Mohyla Black Sea National University, Mykolaiv, Ukraine. E-mail: slobodyanyuk.dmitry@gmail.com, orcid: <https://orcid.org/0000-0001-6281-1907>.