http://doi.org/10.35668/2520-6524-2025-4-10
УДК 330.341.1

Г. О. АНДРОЩУК, канд. екон. наук, доц.

ВПЛИВ НЕДОБРОСОВІСНОЇ КОНКУРЕНЦІЇ НА РИНОК ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В ЦИФРОВІЙ ЕКОНОМІЦІ

Резюме. *У статті досліджено вплив недобросовісної конкуренції на ринок інтелектуальної власності в цифровій економіці. Розглянуто головні особливості та тенденції ринку інтелектуальної власності: домінування цифрових активів, глобалізація ринку, нові моделі монетизації, зростання ролі промислової власності, вплив нових технологій, ризики та загрози. Проаналізовано характеристики та нові форми недобросовісної конкуренції в цифровій економіці, вразливості інтелектуальної власності в цифровому ландшафті, економічні та інноваційні наслідки, юридичні та регуляторні виклики та відповіді. Підсумовано, що головна проблема полягає в системній вразливості, яка виникає через швидкий розвиток технологій і постійне відставання регуляторних рамок і міждисциплінарний характер цифрових порушень. Це призводить до значних економічних втрат, пригнічує інновації, концентрує ринкову владу в руках домінуючих гравців та обмежує вибір споживачів. Це вимагає адаптації законодавства, створення нових регуляторних інструментів, посилення міжнародної співпраці для розв'язання транскордонних проблем і проактивних стратегій із боку правовласників.*

Ключові слова: *інтелектуальна власність, недобросовісна конкуренція, правове регулювання, цифрова економіка, економічний вплив.*

ПОСТАНОВКА ПРОБЛЕМИ

Цифрова економіка докорінно змінила динаміку конкуренції, запровадивши нові, часто приховані та технологічно складні форми недобросовісних практик, які безпосередньо підривають права інтелектуальної власності (ІВ). Ці практики, починаючи від алгоритмічної змови та експлуатації даних до діпфейків і патентного тролінгу, не лише спричиняють значні економічні втрати та пригнічують інновації, а й підривають довіру споживачів і спотворюють ринкові структури. Традиційні правові рамки часто виявляються неадекватними для протидії цим загрозам, що вимагає адаптивних законодавчих відповідей, міцної міжнародної співпраці та проактивних технологічних і стратегічних заходів з боку правовласників.

Отже, поширеність недобросовісної конкуренції в цифровому середовищі, у поєднанні зі стрімким розвитком технологій, створює системну вразливість для об'єктів ІВ та підкреслює постійне відставання регулювання. Це не просто питання окремих порушень, а фундаментальний виклик стабільності та справедливості самої екосистеми цифрового ринку. Синтез наявної інформації вказує на глибинну та всеосяжну проблему. За своєю природою цифрові технології сприяють виникненню нових, важко виявлюваних форм недобросовісних практик, які часто є прихованими та міждисциплінарними. До того ж, потужні технологічні платформи активно прагнуть послабити захист ІВ, що посилює цю вразливість. Постійна потреба в оновленні законодавства та труднощі традиційного правозастосування свідчать про те, що правове регулювання постійно наздоганяє технологічний розвиток. Ця сукупність доказів свідчить про те, що проблема полягає не просто в сукупності окремих інцидентів, а в системному виклику цілісності цифрового ринку, що вимагає проактивного та цілісного підходу до управління, а не фрагментарних рішень.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Проблематику конкурентного права, захисту від недобросовісної конкуренції в системі права інтелектуальної власності досліджували такі вітчизняні науковці (юристи та економісти), як Г. О. Андрощук, О. О. Бакалінська, О. В. Безух, З. М. Борисенко, Н. Я. Борсук, Ю. Л. Бошицький, О.Б. Бутнік-Сіверський, С. С. Валітов, О. В. Вознюк, І. І. Дахно, Ю. В. Журик, Ю. М. Капіца, А. О. Кодинець, О. Ю. Кронда, В. Д. Лагутін, В. І. Полюхович, К. В. Смирнова, О. Л. Чернелевська, С. В. Шкляр та ін. Вагомий внесок у розвиток науково-правових досліджень цифрової економіки зробила О. М. Вінник, яка дослідила окремі проблеми антимонопольно-правового регулювання в умовах цифрової економіки [1].

Проте динамічні зміни в економіці, законодавстві у сфері цифрової економіки та ІВ потребують подальших наукових досліджень.

Метою статті є економіко-правовий аналіз впливу недобросовісної конкуренції на ринок інтелектуальної власності в цифровій економіці, виявлення ризиків і загроз та механізмів їх протидії.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

На перетині цифрової економіки, ІВ та конкуренції

Визначення цифрової економіки та її трансформаційний вплив на динаміку ринку. Цифрова економіка характеризується швидким технологічним прогресом, що сприяє безперервному створенню нових форм, моделей і продуктів. Зокрема цифрові товари мають низьку граничну вартість, що робить їхнє копіювання та розповсюдження недорогим. Це середовище значно змінило динаміку конкуренції, не лише створивши абсолютно нові ринки, а й трансформувавши наявні [2]. Хоча цифровізація принесла такі значні переваги споживачам, як нижчі ціни, більша доступність і зручність, розширений вибір та інноваційні продукти, водночас вона породила серйозні проблеми щодо ринкових структур, антиконкурентної поведінки та злиттів, які можуть призвести до стійкої ринкової влади.

Ринок ІВ у цифровій економіці зазнає значних трансформацій і має низку ключових особливостей. Окреслимо головні особливості та тенденції:

- *домінування цифрових об'єктів:* зростає значення таких об'єктів ІВ, як програмне забезпечення, бази даних, цифрові твори (музика, фільми, ігри, електронні книги), торговельні марки та доменні імена;
- *легкість копіювання та розповсюдження:* цифрові технології дають змогу майже миттєво та безкоштовно копіювати та поширювати контент, що створює виклики для захисту авторських та суміжних прав (проблема піратства);
- *глобалізація ринку:* інтернет та цифрові платформи роблять ринок ІВ глобальним, що вимагає гармонізації міжнародного законодавства та ефективних механізмів транскордонного захисту;
- *нові моделі монетизації:* замість традиційного продажу фізичних копій, набувають поширення моделі ліцензування, передплати (стримінгові сервіси), реклами, freemium, а також використання блокчейну та NFT (невзаємозамінних токенів) для унікалізації цифрових активів;
- *розвиток ліцензійного ринку:* згідно з традиційним підходом, ринок ІВ поділяється на *ринок продажу* (*відчуження) майнових прав*, коли права відчужуються назавжди та *ринок передачі майнових прав шляхом ліцензування,* коли надається дозвіл на використання об'єкта ІВ на певний термін, території та умовах. У цифровій економіці ліцензування є провідною формою;
- *зростання ролі промислової власності:* спостерігається активне зростання кількості заявок на винаходи, корисні моделі, промислові зразки та торговельні марки, що свідчить про пожвавлення винахідницької та інноваційної активності;
- *вплив нових технологій:* штучний інтелект (ШІ), блокчейн, великі дані (Big Data) впливають на створення, управління та захист ІВ, ставлячи нові питання щодо авторства та правового регулювання;
- *ризики та загрози:* зростають ризики кіберзлочинності, злому та крадіжки інноваційних ідей, що вимагає посилення цифрової безпеки та правового захисту.

Еволюція ІВ в цифрову еру. Значної еволюції ІВ зазнала в цифрову еру, принципово змінившись від традиційних фізичних об'єктів до нематеріальних форм. Ця розширена концепція власності тепер охоплює широкий спектр цифрових творінь та даних, охоплюючи такі цифрові активи, як музика, тексти та зображення, а також персональні дані, криптовалюти та віртуальні об'єкти в метавсесвіті. Ця трансформація означає, що сама природа "власності" розширилася, що створює нові виклики для її захисту та примусового виконання. Хоча інтернет значно покращив доступ до інформації, саме ця можливість, парадоксально, призвела до суттєвого збільшення випадків піратства та несанкціонованого використання цифрових матеріалів [2].

Концептуальні засади недобросовісної конкуренції в цифровому контексті. Недобросовісна конкуренція широко визначається як спосіб ринкових відносин, за якого одна або декілька компаній порушують загальні норми поведінки, чинні закони країни та принципи моралі та справедливості. У цифровій економіці це поняття поширюється на підприємства, які використовують цифрові технології та онлайн-платформи для отримання конкурентних переваг незаконними або неетичними засобами. Така поведінка активно підриває чесну ринкову конкуренцію, завдає шкоди конкурентам і вводить в оману споживачів. На відміну від традиційної конкуренції, яка часто зосереджується на ціні, цифрова недобросовісна конкуренція

часто проявляється як нецінова конкуренція, що досягається за допомогою інших засобів, ніж зниження вартості, наприклад, шляхом маніпулювання якісними характеристиками продукту або умовами його реалізації.

Цифрова економіка за своєю суттю розмиває традиційні межі між захистом ІВ, конкурентним правом і захистом прав споживачів. Практики недобросовісної конкуренції, які націлені на об'єкти ІВ, часто *мають каскадний ефект*, одночасно спотворюючи ширшу ринкову конкуренцію та порушуючи фундаментальні права споживачів, що вимагає цілісного та інтегрованого регуляторного підходу. Визначення недобросовісної конкуренції охоплює порушення "моралі та справедливості", що вказує на ширший обсяг, ніж просто економічна вигода [3]. Практики недобросовісної конкуренції, зокрема алгоритмічні маніпуляції та експлуатація великих даних, безпосередньо пов'язані з прямою шкодою для споживачів, наприклад, з порушенням їхніх прав на інформацію, вибір і добробут, а також з введенням їх в оману. Окрім того, важливість довіри споживачів та їхньої автономії на конкурентному ринку підкреслюється. Коли права ІВ порушуються, то це часто надає неправомірну конкурентну перевагу, що спотворює ринок. Це спотворення зрештою шкодить споживачам, зменшуючи вибір, підвищуючи ціни або підриваючи довіру. Отже, розв'язання проблеми недобросовісної конкуренції в цифровій сфері вимагає розуміння та управління цими взаємопов'язаними впливами у сферах ІВ, конкуренції та захисту прав споживачів, а не розгляду їх як ізольованих правових питань.

Характеристики та нові форми недобросовісної конкуренції в цифровій економіці

Відмінні риси цифрової недобросовісної конкуренції. Цифрове середовище надає недобросовісній конкуренції унікальні характеристики, які відрізняють її від традиційних офлайн-практик, що робить виявлення та правозастосування особливо складними.

Прихованість. Недобросовісні практики в цифровій сфері часто здійснюються за допомогою складних технологічних засобів, що ускладнює їх виявлення традиційними методами. Це вимагає від регуляторних органів володіння провідними технічними знаннями та можливостями для ефективного реагування. Непрозорість алгоритмів та потоків даних значною мірою сприяє цій прихованості.

Міждисциплінарний характер. Цифрова недобросовісна конкуренція часто виходить за межі традиційних галузевих кордонів, водночас залучаючи численні сфери та сектори. Ця властива складність вимагає міцної міжвідомчої координації та співпраці між різними регуляторними та правозастосовними органами для забезпечення ефективного нагляду та втручання.

Специфічні прояви та їхній вплив на ІВ. Цифрова економіка породила нові форми недобросовісної конкуренції, багато з яких безпосередньо впливають на права ІВ та справедливість ринку.

Алгоритмічні маніпуляції та змови. Оператори дедалі частіше використовують алгоритми та інструменти великих даних для тонкого або відкритого впливу на динаміку ринку. Ці інструменти можуть послабити автономію вибору споживачів, перешкоджати їхньому праву на отримання інформації та використовувати правила платформ для отримання неправомірної переваги. Особливо тривожним проявом є використання алгоритмів ціноутворення, які часто охоплюють ШІ та машинне навчання. Ці алгоритми можуть обробляти такі змінні, як попит, пропозиція, і навіть непублічні, конкурентно чутливі дані конкурентів, щоб встановлювати нові ціни майже миттєво. Ця можливість може призвести до антиконкурентної поведінки, зокрема до цифрової змови та фіксації цін, причому дослідження показують, що певні алгоритми ціноутворення призводять до вищих цін для споживачів і можуть навіть "навчитися" мовчазно вступати в змову [4]. Регуляторні органи, наприклад, Федеральна торгова комісія (FTC) та Міністерство юстиції США, однозначно заявляють, що фіксація цін за допомогою алгоритму все ще є фіксацією цін, а угода про використання спільних рекомендацій щодо ціноутворення або алгоритмів є незаконною, незалежно від того, чи є розробник алгоритму прямим конкурентом, або якщо ціни відхиляються від рекомендацій.

Незаконний збір даних, скрапінг (англ. *scraping* — "вишкрібання", вебзбирання або витягнення вебданих) *та неправомірне використання комерційних даних.* Це передбачає несанкціоноване отримання інформації про клієнтів конкурентів або комерційної таємниці. Такі практики можуть призвести до формування монополій на дані, що обмежує вихід конкурентів на ринок та їхній розвиток шляхом використання незаконно зібраних даних користувачів, персональної інформації та споживчих звичок для надання персоналізованих послуг або точної реклами. Неправомірний збір і використання даних від конкурентів або з інших джерел, часто за допомогою автоматизованих інструментів, дає змогу підприємствам копіювати стратегії інших, дізнаватися про операції конкурентів або навіть здійснювати онлайн-атаки. Попри

те, що комерційні дані є критично важливим конкурентним ресурсом, їхній захист ІВ стикається зі значними труднощами через прогалини в спеціалізованому законодавстві та нечіткі шляхи захисту.

Маніпуляції з онлайн-репутацією, неправдива реклама та введення в оману. Цифрові платформи надають величезні рекламні простори, але також сприяють поширенню неправдивої інформації та оманливої поведінки. Це передбачає поширення неправдивої інформації (дифамації) для заподіяння шкоди репутації конкурента. Компанії можуть публікувати перебільшені заяви про ефективність або дієвість продукту, щоб ввести споживачів в оману, тим самим завдаючи шкоди репутації та інтересам інших компаній. Маніпуляції з онлайн-репутацією також можуть передбачати публікацію фальшивих негативних відгуків або використання ботів для штучного спотворення онлайн-рейтингів із метою заподіяння шкоди конкуренту.

Маніпуляції з пошуковою оптимізацією (SEO). Це стосується недобросовісних практик, що спрямовані на штучне підвищення рейтингу вебсайту в результатах пошуку або на шкоду позиції конкурента. Тактика передбачає створення спамних зворотних посилань на сайт конкурента для активації штрафів, перевантаження вебсторінок ключовими словами для обману пошукових алгоритмів або створення мереж низькоякісних вебсайтів для посилання на власний сайт. Хоча пошукові системи можуть виявляти такі маніпуляції, проте вони не завжди можуть застосувати штрафи до маніпуляторів до того, як буде завдано значної шкоди.

Створення штучних бар'єрів для виходу на ринок. На цифрових ринках домінуючі гравці можуть створювати штучні бар'єри для конкуренції. Це передбачає зловживання домінуючим становищем на ринку шляхом відмови в доступі до важливої інфраструктури чи встановлення надмірних цін або несправедливих торговельних умов, тим самим перешкоджаючи конкуренції. Формування монополій на дані шляхом незаконного збору даних також може обмежувати вихід конкурентів на ринок та їхній розвиток. Окрім того, значний обсяг поглинань великими цифровими платформами, часто з використанням сильних мережевих ефектів, високоякісних алгоритмів та економіки масштабу, що ґрунтується на даних, сприяв зростанню та розширенню величезних цифрових екосистем. Ці поглинання часто відбувалися з надзвичайно малою кількістю втручань із боку конкурентних органів, даючи змогу провідним фірмам розширювати свій вплив на ринки, що виходять далеко за межі їхніх основних послуг.

Таким чином, цифрова недобросовісна конкуренція використовує провідні технології (ШІ, великі дані та алгоритми), щоб діяти з безпрецедентною витонченістю, швидкістю та масштабом, що робить традиційні механізми виявлення та примусового виконання недостатніми. Її "прихованість" та "міждисциплінарний характер" є не просто характеристиками, а фундаментальними викликами для ефективного управління. Ці особливості пояснюють, чому ці практики так важко подолати. Алгоритмічна фіксація цін, наприклад, демонструє, як алгоритми можуть встановлювати ціни "миттєво" і навіть "навчатися" вступати в змову, що свідчить про рівень швидкості та автономії, що значно перевищує людські можливості. Автоматизований скрапінг даних і маніпуляції з SEO, описані в джерелах, вказують на масштаб, що може охоплювати величезні сегменти інтернету. Комбінований ефект цих технологічних можливостей означає, що недобросовісні практики більше не є ізольованими, ручними діями, а системними, технологічно керованими операціями, які можуть швидко поширюватися та залишатися значною мірою невідстежуваними традиційними засобами. Це вимагає фундаментальної переоцінки парадигм регулювання та примусового виконання, вимагаючи від агентств розробки провідних технічних можливостей і сприяння міжвідомчій співпраці, щоб відповідати складності загроз. У **табл. 1** систематизовано головні види недобросовісної конкуренції в цифровій економіці, їхні характеристики та вплив.

Вразливості інтелектуальної власності в цифровому ландшафті.

Огляд цифрових об'єктів ІВ. Цифрова ІВ охоплює будь-яке інтелектуальне творіння, що існує в цифровій формі. Це передбачає охоплення широкого спектра таких активів, як програмне забезпечення, цифрові медіа (наприклад, музика, фільми, книги), онлайн-патенти, торговельні марки, цифрові активи, персональні дані, криптовалюти та віртуальні об'єкти в метавсесвіті. Хоча інтернет значно покращив доступ до інформації, проте саме ця можливість парадоксальним чином призвела до суттєвого збільшення випадків піратства та несанкціонованого використання цифрових матеріалів.

Головні загрози та форми порушень. Цифровий ландшафт представляє численні специфічні загрози та форми порушень, які безпосередньо спрямовані на різні типи ІВ.

Цифрове піратство та порушення авторських прав залишається однією з найзначніших загроз для цифрової ІВ, що охоплює несанкціоноване копіювання та розповсюдження

Таблиця 1

Головні види недобросовісної конкуренції в цифровій економіці та їхні характеристики

Вид недобросовісної конкуренції	Опис / Ключові характеристики	Приклади	Основний вплив на ІВ / ринок
Алгоритмічні маніпуляції та змови	Використання ШІ чи машинного навчання для впливу на ринок, враховуючи фіксацію цін за допомогою непублічних даних конкурентів; послаблення автономії споживачів	Мовчазна алгоритмічна змова, фіксація цін у житловому секторі	Спотворення цін, обмеження вибору споживачів
Незаконний збір даних, скрапінг та неправомірне використання комерційних даних	Несанкціоноване отримання інформації про клієнтів або комерційної таємниці; формування монополій на дані	Монополії на дані, використання автоматизованих інструментів для копіювання конкурентів	Крадіжка комерційної таємниці, обмеження виходу на ринок
Маніпуляції з онлайн-репутацією, неправдива реклама та введення в оману	Поширення неправдивої інформації (дифамація), перебільшені заяви про продукти, фальшиві відгуки, використання ботів	Фальшиві негативні відгуки, перебільшення ефективності продукту	Шкода репутації бренду, введення споживачів в оману
Маніпуляції з пошуковою оптимізацією (SEO)	Недобросовісні практики для штучного підвищення чи зниження рейтингу вебсайту в пошукових системах	Створення спамних зворотних посилань, перевантаження сторінок ключовими словами, дубльований контент	Спотворення ринкових позицій, недобросовісна конкуренція
Створення штучних бар'єрів для виходу на ринок	Зловживання домінуючим становищем, відмова в доступі до важливої інфраструктури, встановлення несправедливих умов, поглинання конкурентів	Відмова в доступі до суттєвої інфраструктури, монополії на дані, злиття без належного контролю	Обмеження конкуренції, пригнічення інновацій

цифрового контенту (музика, фільми, книги та програмне забезпечення). Піратству сприяє легкість цифрового дублювання, поширення платформ для обміну файлами (наприклад, торрент-сайтів, як-от Napster у 1999 р. та The Pirate Bay), а також несанкціоновані потокові вебсайти. Часто чинником, що призводить до піратства, є відсутність обізнаності споживачів або ігнорування законів про авторське право. Реальні приклади включають широке піратство фільмів, електронних книг і музичних альбомів, а також більш серйозні інциденти (наприклад, злам серверів CD Projekt Red у 2021 р., що призвело до витоку вихідного коду Cyberpunk 2077) [5, с. 263].

Контрафактні та імітаційні цифрові продукти також є загрозою для цифрової ІВ. З експоненціальним зростанням е-комерції злочинці знайшли нові шляхи отримання прибутку, створюючи підроблені чи майже ідентичні копії цифрових продуктів. Це передбачає поширення підробленого програмного забезпечення та додатків, які часто несуть ризики безпеки, створення шахрайських вебсайтів, що імітують законні бренди для обману клієнтів, а також виробництво клонованих цифрових продуктів з лише незначними модифікаціями. Прикладом є широка доступність піратських версій програмного забезпечення, наприклад, Microsoft Office, часто зі зловмисним/вірусним програмним забезпеченням.

Порушення ліцензій відкритого вихідного коду. Чимало цифрових продуктів, зокрема програмне забезпечення та моделі ШІ, працюють за ліцензіями відкритого вихідного коду, що розроблені для сприяння співпраці. Однак ці

ліцензії часто порушуються за допомогою таких практик, як відсутність зазначення оригінальних розробників, несанкціоноване комерційне використання програмного забезпечення з відкритим вихідним кодом і конфлікти ліцензій, що виникають внаслідок інтеграції коду з відкритим вихідним кодом у власницьке програмне забезпечення без дотримання умов. Поширеним прикладом є невиконання компаніями Загальної публічної ліцензії GNU (GPL) під час використання ядра Linux, що вимагає публічного доступу до модифікацій.

Кіберзагрози та крадіжка ІВ. Цифрова ІВ є головною мішенню для кіберзлочинців через її невіддільну цінність та цифровий формат. Головні кіберзагрози охоплюють хакерські атаки та витоки даних, спрямовані на крадіжку власницьких алгоритмів, вихідного коду та конфіденційної ділової інформації. Корпоративне шпигунство, коли конкуренти наймають хакерів для доступу до комерційної таємниці, є ще однією значною кіберзагрозою. Хмарні сховища, хоч і зручні, проте також вразливі, якщо не забезпечені належним чином. Такі кібератаки можуть призвести до прямого падіння вартості ІВ компанії та подальшої втрати конкурентоспроможності. Глобальні втрати від кіберзлочинності, які часто передбачають крадіжку ІВ, прогнозуються на рівні приголомшливих 10,5 трлн дол. США щороку до 2025 року [5, с. 263]. Примітним випадком є позов Tesla проти колишнього співробітника за нібито крадіжку комерційної таємниці, пов'язаної з її технологією Autopilot AI.

Кіберсквотинг і порушення прав на торговельні марки. Роль інтернету як основної платформи для бізнесу призвела до таких проблем, як кіберсквотинг, коли особи реєструють доменні імена, схожі на популярні бренди, з наміром продати їх з прибутком [6]. Це також поширюється на імітацію бренду, коли шахрайські вебсайти використовують назви брендів та логотипи для введення споживачів в оману, та маніпуляції з пошуковими системами, коли фальшиві вебсайти використовують тактику SEO, щоб обігнати законні підприємства. Прикладом є реєстрація "apple-support.com" несанкціонованими сторонами для обману клієнтів Apple.

Обхід систем управління цифровими правами (DRM). Управління цифровими правами (DRM) — це технологія, що розроблена для запобігання несанкціонованому доступу, копіюванню та перегляду цифрового контенту. Однак хакери постійно розробляють методи обходу цих обмежень (наприклад, зламане програмне забезпечення), що знімає ліцензійні обмеження, інструменти для запису екрана та захоплення, що використовуються для обходу DRM на потоковому контенті (наприклад, фільмах Netflix), та генератори ключів, що створюють фальшиві ключі продукту для активації програмного забезпечення в режимі "преміум" без покупки. Попри DRM, нелегальні копії популярного програмного забезпечення, такого як Adobe Photoshop та Microsoft Office, залишаються широко доступними.

Технологія діпфейків та крадіжка цифрової ідентичності. Швидкий розвиток діпфейків, створених за допомогою ШІ, створив нові виклики для захисту цифрової ідентичності. Ризики, пов'язані з діпфейками, передбачають використання шахраями відео, створених за допомогою ШІ, для просування шахрайських продуктів (фальшиві схвалення знаменитостей), створення злочинцями голосів і відео, згенерованих ШІ, для видавання себе за осіб з шахрайськими цілями (цифрова імітація), а також поширення неправдивої інформації або дифамації за допомогою маніпульованих медіа [7]. Інцидент 2023 р. включав використання кіберзлочинцями діпфейкового клонування голосу ШІ для імітації генерального директора компанії з метою обману співробітників та переказу грошей.

Патентний тролінг — це специфічна форма недобросовісної конкуренції спрямована на ІВ, зокрема патенти, у цифровій економіці. Стартапи особливо вразливі до патентних тролів (суб'єктів, що не займаються виробничою діяльністю, які набувають патенти переважно для судових спорів), які використовують юридичні лазівки, що призводить до тривалих і дорогих судових процесів, які відволікають ресурси та зрештою шкодять та обмежують справжні інновації. Яскравим прикладом є компанія Malikie Innovations Ltd., патентний троль, яка подала позови проти великих фірм із видобутку біткойнів щодо патентів на еліптичну криптографію (ECC), потенційно піддаючи відповідальності будь-кого, хто запускає програмне забезпечення Bitcoin [8]. ***Виклики, що створюються технологіями, які швидко розвиваються.*** Самі технології, що рухають цифрову економіку, також створюють значні складнощі та вразливості для захисту ІВ.

Штучний інтелект (ШІ). Швидкий прогрес ШІ постійно ставить складні питання щодо застосовності законів про ІВ до ШІ та творів, створених ШІ. Це вносить складнощі щодо авторства, оскільки стає спірним, хто володіє твором, створеним ШІ — особа, яка встановила параметри, чи розробник алгоритму. Наприклад, якщо ШІ генерує картину, права на неї можуть бути оскаржені. Окрім того, ШІ може використовуватися для створення діпфейків, які порушують

права на зображення чи голос, що ускладнює захист цифрової ідентичності. З іншого боку, ШІ також пропонує можливості для автоматизації управління правами та аналізу великих наборів даних для виявлення порушень ІВ [9; 10].

Блокчейн. Ця децентралізована технологія зберігання даних пропонує революційні можливості для ІВ, забезпечуючи прозорість прав власності, наприклад, через токенізацію активів, і даючи змогу створювати смарт-контракти для автоматизованого виконання угод, забезпечуючи захист від підробок.

Невзаємозамінні токени (NFT) дають змогу творцям продавати унікальні цифрові об'єкти, підтверджуючи їхню автентичність та право власності. Однак блокчейн має й недоліки. Якщо приватний ключ до криптогаманця втрачено або викрадено, то власник може назавжди втратити доступ до своїх активів без звернення до центрального органу. Окрім того, шахрайство в екосистемі блокчейну (наприклад, підроблені NFT) та вразливості в інфраструктурі (біржі, мости між мережами) становлять загрозу для безпеки цифрової власності. Прикладом є крадіжка понад 600 млн дол. США з мережі блокчейну Ronin у 2022 році [11].

Хмарні сховища. Хмарні сховища дають змогу зберігати дані на віддалених серверах, доступних через інтернет, пропонуючи такі зручності, як доступ до файлів із будь-якого місця, резервне копіювання та обмін контентом. Для творців це спрощує управління такими цифровими активами, як рукописи, фотографії чи відео. Однак дані в хмарних сховищах стають вразливими до кібератак, де злами серверів можуть призвести до втрати чи витоку інформації. Наприклад, у 2014 р. хакери зламали iCloud та оприлюднили приватні фотографії знаменитостей [12]. Власники часто втрачають повний контроль над своїми даними, оскільки постачальники послуг можуть використовувати їх у комерційних цілях або видаляти на власний розсуд, посилаючись на умови надання послуг.

Інтернет речей (IoT). IoT, мережа пристроїв, підключених до інтернету, може покращити управління власністю. Розумні замки можуть захищати фізичні об'єкти, а датчики в логістиці можуть відстежувати рух товарів. Для цифрової власності IoT дає змогу створювати "розумні" об'єкти з унікальними ідентифікаторами. Проте пристрої IoT часто мають слабку безпеку, що робить їх легкою мішенню для хакерів. У 2016 р. ботнет Mirai заразив тисячі пристроїв IoT, використовуючи їх для атак на вебсайти [12]. Дані, зібрані цими пристроями (наприклад, голосові записи з розумних колонок), можуть використовуватися корпораціями без згоди власника, порушуючи приватність та інформаційні права.

Ширші виклики цифрової ери.

- *Юрисдикційна невизначеність:* цифровий світ не має чітких кордонів, що ускладнює визначення "місця вчинення злочину" для правового регулювання. Ця невизначеність впливає на щоденне використання цифрових активів, оскільки їхня доступність може залежати від регіональних законів або угод. Спори щодо NFT, де покупці заявляють лише про цифровий токен без реальних прав на використання, підкреслюють ці правові прогалини. Примусове виконання ІВ через кордони є складним, оскільки кожна країна має власні правила, суди та способи вирішення спорів, що робить права ІВ малозначущими за межами країни походження.
- *Власність та контроль над даними:* користувачі технічно є власниками своїх даних, але часто не мають над ними контролю. Великі технологічні компанії збирають величезні обсяги інформації про користувачів для цільової реклами, генеруючи мільярди прибутку. Скандал з Cambridge Analytica у 2018 р. виявив, як дані користувачів Facebook використовувалися для політичних маніпуляцій без згоди [12]. Умови надання послуг часто дають змогу компаніям розпоряджатися даними на власний розсуд, залишаючи користувачів вразливими.
- *Неадекватність традиційних правових систем:* правові рамки, розроблені протягом століть для фізичної власності, погано пристосовані до швидкості цифрових змін. Багато країн не мають чітких визначень для криптовалют (валюта, товар чи власність), що ускладнює правовий захист. Повільний законодавчий процес, що займає роки для адаптації законів, тоді як технології розвиваються експоненціально, ще більше загострює проблему. Законодавство про боротьбу з недобросовісною конкуренцією, хоча воно і є фундаментом для контролю над даними, не є довгостроковим ефективним інструментом для захисту ІВ комерційних даних через прогалини та відсутність чітких меж. Технологічні платформи активно виступали за зміни в законодавстві, спрямовані на послаблення прав ІВ, зокрема через розширене тлумачення "безпечної гавані" в Законі про авторське право в цифрову епоху (DMCA).

В Україні ситуація є особливо складною через її прагнення до європейської інтеграції та активний розвиток цифрової економіки, що поєднується з активною стадією війни та обмеженими

ресурсами. Країна прагне інтегруватися з такими європейськими стандартами, як GDPR, але стикається з повільними провадженням реформ та транскордонними загрозами. Чинне законодавство, зокрема Закон України "Про захист персональних даних" від 1 червня 2010 р. № 2297-VI, не відповідає реаліям цифрової ери, а законопроєкт 2022 року (№ 8153) ще не було повністю реалізовано.

Економічні та інноваційні наслідки.

Вплив на інновації та інвестиції. Недобросовісна конкуренція послаблює інноваційний стимул підприємств. Коли компанії можуть швидко отримати частку ринку та прибуток за допомогою неправомірних засобів, вони можуть більше не зосереджуватися на перемозі в конкуренції через технологічні інновації та покращення якості послуг. Це призводить до відсутності ефективної конкуренції на ринку, тим самим пригнічуючи інновації та розвиток у цій галузі.

У цьому контексті напрям інновацій спотворюється, оскільки недобросовісна конкуренція може призвести до того, що компанії інвестуватимуть ресурси та енергію в дослідження та застосування недобросовісних методів конкуренції, а не в справжні технологічні інновації. Наприклад, компанії можуть надавати пріоритет видобутку даних та оптимізації алгоритмів для утримання користувачів, замість того, щоб покращувати користувацький досвід за допомогою інновацій продукту. Це спотворення марнує соціальні ресурси та перешкоджає технологічному прогресу та довгостроковому розвитку галузі.

Послаблення прав ІВ є вигідним для технологічних платформ, оскільки вони прагнуть зменшити витрати на придбання вхідних даних. Якщо постачальник технологій або контенту більше не може реально погрожувати зверненням за судовою забороною або навіть грошовою компенсацією проти користувача-порушника, то ціна, яку він може вимагати в ліцензійних переговорах, відповідно падає. Зі зниженням цін, що сплачуються постачальникам технологій і контенту, прибуток користувачів ІВ зростає. Фактично, технологічні платформи переглянули ціну на необхідні вхідні дані для контенту та технологій, послабивши інфраструктуру ІВ цифрової економіки. У короткостроковій перспективі користувачі, імовірно, вітають це переоцінювання, оскільки їм подобається дивитися захищені авторським правом відео безоплатно чи платити менше за запатентовані ліки. Привабливість "безкоштовних (або дешевших) речей" частково пояснює успіх кампанії за послаблення прав ІВ. Однак деградація прав ІВ, імовірно, призведе до політики "програшу-програшу", яка зробить ринки технологій та контенту менш конкурентоспроможними та менш інноваційними в довгостроковій перспективі. Інновації можуть зберігатися за режиму слабкої ІВ, але, імовірно, відбуватимуться переважно в рамках екосистем продуктів і послуг, що підтримуються вертикально інтегрованими чи системно інтегрованими фірмами. Навпаки, надійні права ІВ сприяють як інноваціям, так і конкуренції, що показано на прикладі моделі "безфабричного" виробництва в напівпровідниковій промисловості, де ІВ полегшила вхід нових фірм. Ерозія прав ІВ у контентних і технологічних ринках призводить до створення перекошеної екосистеми, що віддає перевагу платформовим моделям монетизації контенту та технологічних активів, водночас нехтуючи незалежними інноваторами та творцями, які підтримують найбільш міцні знаннєві екосистеми.

Концентрація ринку та спотворення. Недобросовісна конкуренція, зокрема видобуток даних і монополії на дані, обмежує вихід конкурентів на ринок та їхній розвиток. Метою конкурентного права є захист споживачів, підприємств та економіки від спотворень на ринку, спричинених створенням монополії чи олігополії, картелів або зловживанням ринковою владою.

Отже, серед заборонених видів поведінки виділяють такі: фіксація цін, коли компанії встановлюють однакові ціни на товари чи послуги, що зменшує конкуренцію за ціною та шкодить споживачам; обмеження виробництва та розвитку шляхом прямого чи опосередкованого обмеження виробництва, інвестицій або технологічного прогресу, що перешкоджає конкуренції та інноваціям, які створювали б нові пропозиції товарів і послуг; поділ ринку чи клієнтів, коли фірми домовляються про поділ географічних зон або сегментів клієнтів, що призводить до відсутності прямої конкуренції між ними та зменшення вибору споживачів [13].

Зловживання домінантним становищем також передбачає відмову в доступі до важливої інфраструктури, коли підприємство, що володіє ресурсом або інфраструктурою, важливою для здійснення діяльності, відмовляє конкурентам у доступі до неї без достатнього обґрунтування, тим самим перешкоджаючи конкуренції. Окрім того, компанія, що займає провідне становище, зловживає, якщо встановлює надмірні ціни чи несправедливі торговельні умови, коли ціни або умови непропорційні економічній цінності товару чи послуги та мають на меті отримання несправедливого прибутку. Прикладом є справа Microsoft, де компанія, домінуючи на ринку операційних систем, зловживала своїм становищем, попередньо встановлюючи свій Windows Media Player (WMP) у своїх операційних

системах, тим самим розширюючи свій вплив на ринок медіаплеєрів [13].

Цифрові злиття відрізняються видатною роллю екосистем платформ, що покладаються на сильні мережеві ефекти, високоякісні алгоритми, економію масштабу та економію обсягу, що ґрунтується на даних. Це ставить під сумнів здатність традиційних теорій шкоди відображати реальну конкурентну шкоду, яка може виникнути. Останні декілька десятиліть спостерігався значний обсяг поглинань найбільшими цифровими платформами, причому надзвичайно мало з них призвели до будь-якого втручання з боку конкурентних органів. Ці поглинання сприяли зростанню та розширенню великих цифрових екосистем, за допомогою яких платформи розширили свій вплив на ринки, що виходять далеко за межі їхніх головних послуг. Алгоритмічна конкуренція потребує ретельного моніторингу, оскільки, хоча алгоритми можуть призвести до багатьох ефектів, що підвищують ефективність і сприяють конкуренції, вони також можуть використовуватися фірмами для обмеження конкуренції.

Фінансові втрати через порушення прав ІВ. Фінансовий вплив порушення авторських прав є значним. Згідно зі звітом Міжнародної торгової палати (ICC), світова економіка щорічно втрачає від 29,2 до 71 млрд дол. США через підробку та піратство. Згідно з оцінками Торгової палати США, порушення авторських прав коштує економіці США 29,2 млрд дол. США щорічно у вигляді втраченого економічного виробництва та призводить до втрати понад 373 000 робочих місць [14].

Креативні індустрії, які охоплюють музику, кіно, літературу та розроблення програмного забезпечення, особливо вразливі до наслідків порушення авторських прав. Коли матеріал, захищений авторським правом, піратується, творці та виробники цього матеріалу втрачають дохід. Ця втрата може мати значний вплив, що поширюється не лише на творців, а й на галузі, які їх підтримують, зокрема маркетинг і дистрибуція. Ринок праці також страждає, оскільки компанії можуть скорочувати робочу силу чи скасовувати проєкти через фінансові обмеження, спричинені піратством. Лише індустрія відеоігор підтримує понад 220 000 робочих місць у США. Глобальні втрати від кіберзлочинності, які часто включають крадіжку ІВ, прогнозуються на рівні 10,5 трлн дол. США щорічно до 2025 року [14].

Ерозія довіри та вибору споживачів. Недобросовісна конкуренція, зокрема алгоритмічні маніпуляції та експлуатація великих даних, серйозно шкодить правам споживачів на інформацію, вибір і добробут. Споживачі легко піддаються впливу та маніпуляціям із боку алгоритмів, а надмірний вибір, спричинений масовою інформацією, може призвести до того, що споживачі уникатимуть або навіть нудьгуватимуть. Це також обмежує свободу вибору споживачів. У цьому процесі негативний вплив недобросовісної конкуренції на споживачів проявлятиме експоненційну тенденцію до розширення, що також призводить до опосередкованого та безпосереднього впливу недобросовісної конкуренції на споживачів.

Оператори, застосовуючи алгоритми та інструменти великих даних, послаблюють автономію споживачів у виборі, втручаються в їхнє право на отримання інформації та використовують правила платформ. Компанії застосовують дедалі більш складні методи для впливу на вибір і вподобання споживачів у цифровому середовищі. Однак наразі незрозуміло чи і як Закон про захист прав споживачів має реагувати на такі практики. Можливо, є підстави розширити сферу застосування законів про недобросовісну торговельну практику, щоб включити перевірку стратегій онлайн-маркетингу, спрямованих на рішення споживачів, які потенційно можуть призвести до порушень приватності. Окрім того, медіапіратство може призвести до девальвації творчої роботи, перешкоджати творчості та інноваціям, а також призводити до розповсюдження низькоякісного або зміненого контенту, потенційно шкодячи репутації творців та культурному значенню їхньої роботи.

Юридичні та регуляторні виклики та відповіді.

Неадекватність чинних правових рамок. Традиційні правові системи, що розвивалися протягом століть для фізичної власності, погано пристосовані до швидкості цифрових змін. Існують прогалини в спеціалізованому законодавстві, нечіткі шляхи захисту та обмежена застосовність чинних законів щодо захисту ІВ комерційних даних. Закон про боротьбу з недобросовісною конкуренцією, хоча його мета — підтримувати нормальний конкурентний порядок підприємств, не є довгостроковим, ефективним інструментом для конкретного захисту прав ІВ комерційних даних. Він забезпечує лише реактивне регулювання, не відповідаючи економічним інтересам підприємств, і не встановлює чітких меж між комерційними, публічними та персональними даними.

Відсутність чітких положень щодо власності, застосування та захисту комерційних даних створює виклики для судових органів. Міжнародні угоди, зокрема Угода ТРІПС, Бернська конвенція та Договір ВОІВ про авторське

право (WCT), хоча й підтримують інновації в галузі даних, мають обмежений захист комерційних даних, якщо вони не є творчими компіляціями. Повільний законодавчий процес, що охоплює роки для адаптації законів, тоді як технології розвиваються експоненціально, ще більше загострює проблему [15]. Технологічні платформи послідовно виступали за зміни в законодавстві, спрямовані на послаблення прав ІВ, що проявляється в сотнях поданих ними amicus curiae (від лат. — друг суду), мільйонах доларів, витрачених на лобіювання, а також фінансуванні адвокатських організацій. Це послаблення інфраструктури ІВ дає змогу платформам переглядати ціни на необхідні вхідні дані, збільшуючи їхні прибутки.

Труднощі транскордонного правозастосування. Транскордонне правозастосування ІВ є складним, оскільки кожна країна має власні правила, суди та способи вирішення спорів. Права ІВ можуть мало що означати, якщо виходити за межі рідної країни. Адже не існує "глобального патенту" або "глобальної торговельної марки"; захист є специфічним для кожної країни, і реєстрація необхідна в кожній юрисдикції, де планується ведення бізнесу, щоб уникнути ризику втрати прав.

Бар'єри для примусового виконання передбачають невідповідності в механізмах примусового виконання та правових культурах між країнами. Отримання сприятливого судового рішення може бути важко виконати на різних територіях. Юрисдикційна невизначеність у цифрових спорах виникає через те, що акти порушення можуть починатися в одній країні, відбуватися в іншій і бути доступними з будь-якого місця. Ця взаємопов'язаність робить глобальну співпрацю та синхронізацію законів про права ІВ імперативними для ефективного вирішення динамічних транскордонних спорів щодо ІВ.

Для України ситуація особливо складна через її прагнення до європейської інтеграції та активний розвиток цифрової економіки, що поєднується з війною та обмеженими ресурсами. Країна прагне інтегруватися з такими європейськими стандартами, як GDPR, але стикається з повільними реформами та транскордонними загрозами.

Регуляторні відповіді та адаптація. Законодавство певною мірою відреагувало на виклики цифрової економіки. Наприклад, Цивільний кодекс України формує систему управління цифровою економікою, включаючи положення про захист даних і віртуальної мережевої власності, а також спеціальний розділ про захист приватності та персональної інформації. В Україні тіньова економіка є сектором, який важко оцінити та контролювати. Вона перетворилася на повноцінного конкурента держави в управлінні фінансовими потоками. Згідно з підрахунками Міністерства економіки, нині близько 40 % ВВП перебуває поза офіційним обігом, а за даними World Economics (2024), що базуються на середніх оцінках провідних економістів, цей показник сягає 44,2 % ВВП. Відповіддю держави на масштаб тінізації є Національна антикорупційна стратегія 2021–2025 років, що визначає чітку мету: мінімізувати вплив людського чинника та створити цифрові механізми контролю, які роблять корупційні ризики невигідними. Стратегією передбачено понад 60 ІТ-рішень, спрямованих на автоматизацію публічних процесів, прозорість фінансів і громадський контроль. Однак темпи реалізації залишаються повільними. Згідно з даними OECD Integrity and Anti-Corruption Review of Ukraine 2025, лише 28 % заходів виконано повністю, ще 9 % — частково, а понад 30 % — навіть не розпочато [16]. Ця статистика сигналізує: без пришвидшення впровадження антикорупційних ініціатив детінізація залишиться на папері.

*Захист прав споживачів від недобросовісних комерційних практик***.** Підписавши Угоду про асоціацію між Україною, з одного боку, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншого, Україна взяла на себе зобов'язання щодо приведення вітчизняного законодавства до *acquis communautaire*, зокрема щодо захисту прав споживачів від недобросовісних комерційних практик. На теренах ЄС знаковим документом, що покликаний визначити загальні правила правового регулювання відносин недобросовісної комерційної діяльності є Директива Європейського Парламенту і Ради № 2005/29/ЄС (далі — Директива 2005/29) від 11 травня 2005 р. стосовно недобросовісних комерційних практик бізнесу щодо споживачів на внутрішньому ринку та внесення змін до Директиви Ради 84/450/ЄЕС, директив Європейського Парламенту і Ради 97/7/ЄС, 98/27/ЄС та 2002/65/ ЄС та Регламенту Європейського Парламенту і Ради (ЄС) № 2006/2004 ("Директива про недобросовісні комерційні практики") [17]. Кабінет Міністрів України прийняв постанову, що затверджує порядок оцінки нечесних комерційних практик. Документ надає Державній службі України з питань безпечності харчових продуктів та захисту споживачів (Держпродспоживслужбі) право перевіряти бізнес і фіксувати порушення, що вводять споживачів в оману чи мають агресивний характер. Кабінет Міністрів України прийняв постанову "Про затвердження Порядку оцінки

застосування суб'єктами господарювання нечесних комерційних практик" від 26 серпня 2025 р. № 1030. Цей документ набере чинності одночасно із Законом України "Про захист прав споживачів" від 10 червня 2023 р. № 3153-IX. Відповідно до постанови Держпродспоживслужба здійснює оцінку застосування суб'єктами господарювання нечесних комерційних практик під час здійснення заходів державного нагляду (контролю) у сфері захисту прав споживачів на підставі: ст. 32 Закону України "Про захист прав споживачів"; Закону України "Про основні засади державного нагляду (контролю) у сфері господарської діяльності" від 05 квітня 2007 р. № 877-V. У рамках заходів державного нагляду серед інших порушень вимог законодавства фіксуються порушення стосовно застосування суб'єктами господарювання нечесних комерційних практик шляхом застосування уніфікованої форми акта. Комерційна практика оцінюється як нечесна, якщо з переліку питань щодо здійснення держнагляду посадовими особами встановлено хоча б одну ознаку нечесної комерційної практики згідно із ст. 26–29 Закону України "Про захист прав споживачів". Держпродспоживслужба встановлює належність комерційної практики: до комерційної практики, що **вводить в оману** відповідно до ст. 26 та 27 Закону; до **агресивної** комерційної практики відповідно до ст. 28 та 29 Закону. Під час оцінки наявності ознак нечесної комерційної практики Держпродспоживслужба встановлює: належність споживачів, щодо яких здійснюється комерційна практика, до **вразливих** категорій; наявність завданої (можливо завданої) комерційною практикою шкоди економічним інтересам споживача або спотворення такою комерційною практикою економічної поведінки споживача щодо певної продукції. У разі встановлення, що споживачі належать до вразливих категорій, Держпродспоживслужба відповідно до законодавства, оцінює врахування суб'єктом господарювання особливих характеристик такої групи споживачів, імовірність здійснення ними несвідомого вибору або допущення помилки під час вчинення правочину щодо обставин, які мають істотне значення. З метою встановлення факту застосування суб'єктом господарювання нечесних комерційних практик посадові особи Держпродспоживслужби мають право: отримувати безоплатно від суб'єктів господарювання, що перевіряються, копії документів, матеріалів, довідок тощо, які мають значення для розгляду питання застосування суб'єктом господарювання нечесних комерційних практик.

Розслідування органами Антимонопольного комітету України (АМКУ) справ щодо захисту від недобросовісної конкуренції триває від чотирьох місяців до 6,5 року, в середньому — 2,5 року, залежно від складності справи та поведінки її фігурантів. Справи (у межах компетенції) розглядають такі органи: АМКУ як колегіальний орган, адміністративна колегія територіального відділення АМКУ; державний уповноважений АМКУ; адміністративна колегія АМКУ [18, с. 88]. Однак загалом кількість справ, розглянутих органами АМКУ, не відображає масштабів проблеми. Випадки недобросовісної конкуренції трапляються майже щодня, але справи відкриваються не за кожним фактом. Серед причин — перевантаженість відомства та недостатньо активна позиція виробників і споживачів, що постраждали від порушень. Можливо, така пасивність зумовлена незнанням інструментів протидії. У більшості випадків недобросовісна поведінка щодо конкурента є порушенням конкурентного законодавства та законодавства про інтелектуальну власність [18, с. 89].

У всьому світі було запропоновано чи прийнято нові регуляторні реформи для розв'язання проблем цифрової конкуренції за допомогою нових регуляцій *ex ante*, що доповнюють зусилля *ex post* щодо примусового виконання на цифрових ринках. Органи з питань конкуренції повинні адаптувати свої аналітичні інструменти до унікальності цифрових ринків, що може вимагати законодавчих змін та адаптованих процесів, щоб відповідати швидкості еволюції на цифрових ринках. Окрім того, моніторинг алгоритмічної конкуренції є критично важливим, оскільки компанії дедалі частіше використовують алгоритми для встановлення цін та створення або вдосконалення нових продуктів і послуг. Хоча алгоритми можуть призвести до багатьох ефектів, що підвищують ефективність та сприяють конкуренції, вони також можуть використовуватися фірмами для обмеження конкуренції. Органи з питань конкуренції мають усвідомлювати ці ризики, знати, як їх розслідувати, а також усувати будь-яку можливу шкоду для споживачів.

Міжнародна співпраця також є ключовою. Так, у США Федеральна торгова комісія (FTC) співпрацює з міжнародними агентствами з питань конкуренції, захисту прав споживачів і приватності по всьому світу для припинення оманливих, недобросовісних та антиконкурентних ділових практик, що впливають на споживачів. Діяльність комісії передбачає співпрацю у справах про злиття та антиконкурентну поведінку, обмін досвідом та методами правозастосування через двосторонні взаємодії, технічну допомогу та участь у багатосторонніх форумах. Закон SAFE WEB, повторно дозволений у 2020 р.,

підтверджує повноваження FTC щодо притягнення до відповідальності іноземних правопорушників за дії, що мають зв'язок зі США, а також підтримує обмін інформацією та допомогу в розслідуваннях з іноземними колегами [19].

З огляду на зазначене, для України пропонуються такі рішення: модульне законодавство для швидкої адаптації, створення незалежних регуляторів, інтеграція інновацій (ШІ для моніторингу, блокчейн для смарт-контрактів) і підвищення цифрової грамотності. Підприємства також мають вживати проактивних заходів для захисту від сучасних, але все ще недобросовісних практик. Це охоплює адаптацію засобів захисту, консультації з бізнес-юристами, чітке визначення прав власності на ІВ в угодах і використання систем скарг на платформах.

ВИСНОВКИ

Вплив недобросовісної конкуренції на ринок ІВ у цифровій економіці є багатогранним та глибоким. Аналіз показує, що цифрова економіка, хоча й приносить значні переваги, також створює нові, складні та часто приховані форми недобросовісних практик. Ці практики, зокрема алгоритмічні маніпуляції, незаконний збір даних, маніпуляції з онлайн-репутацією та патентний тролінг, безпосередньо загрожують ІВ, спотворюючи певні ринкові механізми та підриваючи довіру споживачів.

Головна проблема полягає в системній вразливості, що виникає через швидкий розвиток технологій і постійне відставання регуляторних засад. Традиційні правові системи, розроблені для фізичної власності, часто виявляються неадекватними для боротьби зі швидкістю, масштабом та міждисциплінарним характером цифрових порушень. Це призводить до значних економічних втрат, пригнічує інновації, концентрує ринкову владу в руках домінантних гравців та обмежує вибір споживачів.

Успіх захисту прав власників у цифровому світі залежить від комплексного поєднання правових, технологічних і соціальних заходів. Це вимагає адаптації законодавства, створення нових регуляторних інструментів, посилення міжнародної співпраці для розв'язання транскордонних проблем та проактивних стратегій з боку правовласників. Особливо для таких країн, як Україна, яка прагне до європейської інтеграції, але стикається з обмеженими ресурсами та повільними реформами, необхідність радикального переосмислення підходів до регулювання власності є нагальною. Лише за умови цілісного та динамічного підходу можна забезпечити справедливе та інноваційне цифрове середовище.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Вінник О.* Право цифрової економіки [Електронний ресурс] : монографія / О. Вінник. — Київ : НДІ приватного праваі підприємництва імені академіка Ф. Г. Бурчака НАПрН України, 2021. — 350 с. — Режим доступу: https://surl.li/rhwobf.
2. Інтелектуальна власність в цифровій економіці: проблеми теорії і практики [Електронний ресурс] : монографія / за наук. ред. Г. О. Андрощука. — Київ : Інтерсервіс, 2025. — 452 с. — Режим доступу: https://drive.google.com/file/d/16xDa1LRj52vOFVJv6oYVaIptpNtyvDoF/view.
3. *Андрощук Г. О.* Конкурентне право: захист від недобросовісної конкуренції : наук.-практ. вид. / Г. О. Андрощук, С .В. Шкляр. — Київ : Юстініан, 2012. — 472 с.
4. *Полюхович В.* Захист економічної конкуренції на цифрових ринках в Україні / В. Полюхович // Університетські наукові записки — 2024. — № 5 (101). — С. 17–30. DOI: https://doi.org/10.37491/UNZ.101.2.
5. *Погорілець М.* Інтелектуальна власністьу цифрову еру в контексті розвитку технологій / М. Погорілець, С. Сорока // Наукові записки Львівського університету бізнесу та права. — 2025. — Серія економічна. Серія юридична. — Вип. 44. — С. 260–266. DOI: https://doi.org/10.5281/zenodo.15340521.
6. *Андрощук Г.* Протидія недобросовісним реєстраціям і використанню засобів індивідуалізації в умовах цифрової трансформації / Г. Андрощук // Теорія і практика інтелектуальної власності. 2021. — № 1. — С. 48–67. DOI: https://doi.org/10.33731/12021.234192.
7. *Іванченко А.* Діпфейки: розбираємося з технологією та її наслідками [Електронний ресурс] / А. Іванченко // Сайт "Бренди Acer". — Режим доступу: https://blog.acer.com/ua/discussion/2686/dipfeyki-rozbirayemosya-z-tehnologiyeyu-ta-yiyi-naslidkami.
8. *Crossman C.* The Trolls Are Coming: Defending Bitcoin Mining from Patent Trolls [Electronic resource] / C. Crossman // BITCOIN MAGAZYNE. — 2025. — Access mode: https://surl.li/tycyjr.
9. *Андрощук Г. О.* Штучний інтелект і інтелектуальна власність: проблеми регулювання [Електронний ресурс]: : наук.-практ. вид. / НДІ ІВ НАПрН України. — Київ : Інтерсервіс, 2023. — 204 с. — Режим доступу: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/0a3ae7df-6993-490d-9eae-d5a6d1cab8d1/content.
10. *Баранов О.* Штучний інтелект і система права: монографія / О. Баранов; ДНУ "Інститут інформації, безпеки і права Національної академії правових наук України". — Київ; Одеса : Фенікс, 2025. — 296 с. — Режим доступу: https://ippi.org.ua/sites/default/files/shtuchniix__x_ntelekt_x__sistema_prava_monografiya-2_1.pdf.
11. *Tidy J.* Ronin Network: What a $600m hack says about the state of crypto [Electronic resource] / J. Tidy // BBC. — 30 March 2022. — Access mode: https://www.bbc.com/news/technology-60933174.
12. Digital Intellectual Property: Challenges, Best Practices & Future Trends [Electronic resource] // The Legal School. — Access mode: Digital Intellectual Property: Challenges, Best Practices & Future Trends.
13. Algorithms and Collusion: Competition Policy in the Digital Age [Electronic resource] / OECD. — 2017. — 72 p. — Access mode: https://surl.lt/nbwtnt.

14. U.S. Chamber Report Examines Copyright Value and Piracy Harms [Electronic resource] / Claims Journal. — July 10, 2025. — Access mode: https://www.claimsjournal.com/news/national/2025/07/10/331597.htm.
15. *Tewari K.* Cross border intellectual property disputes: challenges and legal strategies for global businesses [Electronic resource] / K. Tewari // Indian Journal of Integrated Research in Law. — 2025. — Vol. 5. — Issue 1. — P. 603–612. — Access mode: https://surl.li/bonvvd.
16. *Балим М.* Цифрові рішення проти тіньових потоків [Електронний ресурс] / М. Балим // Юридична газета. — 05 листопада 2025. — Режим доступу: https://yur-gazeta.com/dumka-eksperta/cifrovi-rishennya-proti-tinovih-potokiv.html\.
17. *Пожоджук Р. В.* Характеристика недобросовісних комерційних практик у контексті захисту прав споживачів / Р. В. Пожоджук // Держава та регіони. Серія Право. — 2023. — № 2 (80). — С. 31–37. DOI: https://doi.org/10.32840/1813-338X-2023.2.5.
18. *Борсук Н. Я.* Захист інтелектуальної власності від недобросовісної конкуренції органами Антимонопольного комітету України / Н. Я. Борсук // Науковий вісник Ужгородського Національного Університету. — 2021. — Серія Право. — Вип. 68. — С. 86–90. — Режим доступу: http://visnyk-pravo.uzhnu.edu.ua/article/view/253928/251190.
19. International Law Enforcement [Electronic resource] // International Cooperation. — 2020. — Access mode: International Cooperation | Federal Trade Commission.

REFERENCES

1. Vinnyk, O. (2021). Pravo tsyfrovoi ekonomiky [Law of the digital economy]. Kyiv, 350 p. Retrieved from: https://surl.li/rhwobf. [in Ukr.].
2. Androshchuk, H. O. (Ed.). (2025). Intelektualna vlasnist v tsyfrovii ekonomitsi: problemy teorii i praktyky [Intellectual property in the digital economy: problems of theory and practice]. Kyiv, 452 p. Retrieved from: https://drive.google.com/file/d/16xDa1LRj52vOFVJv6oYValptpNtyvDoF/view. [in Ukr.]
3. Androshchuk, H. O., & Shkliar, S. V. (2012). Konkurentne pravo: zakhyst vid nedobrosovisnoi konkurentsii [Competition law: protection against unfair competition]. Kyiv, 472 p. [in Ukr.].
4. Poliukhovych, V. (2024). Zakhyst ekonomichnoi konkurentsii na cyfrovykh rynkakh v Ukraini [Protection of economic competition in digital markets in Ukraine]. *Universytetski naukovi zapysky* [University Scientific Notes], *5(101),* 17-30. DOI: https://doi.org/10.37491/UNZ.101.2. [in Ukr.].
5. Pohorilets, M., & Soroka, S. (2025). Intelektualna vlasnist u tsyfrovu eru v konteksti rozvytku tekhnolohii [Intellectual property in the digital era in the context of technological development]. *Naukovi zapysky Lvivskoho universytetu biznesu ta prava* [Scientific Notes of Lviv University of Business and Law], *44*, 260-266. DOI: https://doi.org/10.5281/zenodo.15340521. [in Ukr.].
6. Androshchuk, H. (2021). Protydiia nedobrosovisnym reiestratsiiam i vykorystanniu zasobiv indyvidualizatsii v umovakh tsyfrovoi transformatsii [Counteraction to unfair registrations and uses of means of individualization under digital transformation]. *Teoriia i praktyka intelektualnoi vlasnosti* [Theory and Practice of Intellectual Property]. *1*, 48-67. DOI: https://doi.org/10.33731/12021.234192. [in Ukr.].
7. Ivanchenko, A. (n.d.). Dipfeiky: rozbiraemosia z tekhnolohiieiu ta yii naslidkamy [Deepfakes: understanding the technology and its consequences]. Retrieved from: https://blog.acer.com/ua/discussion/2686/dipfeyki-rozbirayemosya-z-tehnologiy-eyu-ta-yiyi-naslidkami. [in Ukr.].
8. Crossman, C. (2025). The trolls are coming: Defending Bitcoin mining from patent trolls. *Bitcoin Magazine*. Retrieved from: https://surl.li/tycyjr.
9. Androshchuk, H. O. (2023). Shtuchnyi intelekt i intelektualna vlasnist: problemy rehuliuvannia [Artificial intelligence and intellectual property: regulatory issues]. Kyiv, 204 p. Retrieved from: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/0a3ae7df-6993-490d-9eae-d5a6d-1cab8d1/content. [in Ukr.]
10. Baranov, O. (2025). Shtuchnyi intelekt i systema prava [Artificial intelligence and the legal system]. Kyiv–Odesa, 296 p. Retrieved from: https://ippi.org.ua/sites/default/files/shtuchniix__x_ntelekt_x__sistema_prava_monografiya-2_1.pdf. [in Ukr.].
11. Tidy, J. (2022). Ronin Network: What a $600m hack says about the state of crypto. *BBC News*. Retrieved from: https://www.bbc.com/news/technology-60933174.
12. The Legal School. (n.d.). Digital intellectual property: Challenges, best practices & future trends. Retrieved from: https://thelegalschool.com/.
13. OECD. (2017). Algorithms and collusion: Competition policy in the digital age. 72 p. Retrieved from: https://surl.lt/nbwtnt.
14. Claims Journal. (2025). U.S. Chamber Report examines copyright value and piracy harms. Retrieved from: https://www.claimsjournal.com/news/national/2025/07/10/331597.htm.
15. Tewari, K. (2025). Cross border intellectual property disputes: Challenges and legal strategies for global businesses. *Indian Journal of Integrated Research in Law*. *5*(1), 603-612. Retrieved from: https://surl.li/bonvvd.
16. Balym, M. (2025). Tsyfrovi rishennia proty tinovykh potokiv [Digital solutions against shadow flows]. *Iurydychna hazeta* [Lawyer's Newspaper]. Retrieved from: https://yur-gazeta.com/dumka-eksperta/cifrovi-rishennya-proti-tinovih-potokiv.html. [in Ukr.].
17. Pozhodzhuk, R. V. (2023). Kharakterystyka nedobrosovisnykh komertsiinykh praktyk u konteksti zakhystu prav spozhyvachiv [Characteristics of unfair commercial practices in the context of consumer rights protection]. *Derzhava ta rehiony. Seriia Pravo* [State and Regions. Law Series]. *2(80)*, 31-37. DOI: https://doi.org/10.32840/1813-338X-2023.2.5. [in Ukr.].
18. Borsuk, N. Ya. (2021). Zakhyst intelektualnoi vlasnosti vid nedobrosovisnoi konkurentsii orhanamy Antymonopolnoho komitetu Ukrainy [Protection of intellectual property from unfair competition by the Antimonopoly Committee of Ukraine]. *Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia Pravo* [Scientific Bulletin of Uzhhorod National University. Law Series]. *68*, 86-90. Retrieved from: http://visnyk-pravo.uzhnu.edu.ua/article/view/253928/251190. [in Ukr.].
19. Federal Trade Commission. (2020). International cooperation: International law enforcement. Retrieved from: https://www.ftc.gov/international.

H. O. ANDROSHCHUK, PhD in Economics, Associate Professor

THE IMPACT OF UNFAIR COMPETITION ON THE INTELLECTUAL PROPERTY MARKET IN THE DIGITAL ECONOMY

Abstract. *The paper examines the impact of unfair competition on the intellectual property (IP) market in the digital economy. The main features and trends of the IP market are considered: the dominance of digital assets, market globalization, new monetization models, the growing role of industrial property, the impact of new technologies, risks and threats. The characteristics and new forms of unfair competition in the digital economy, IP vulnerabilities in the digital landscape, economic and innovation consequences, legal and regulatory challenges and responses are analyzed. It is concluded that the main problem lies in the systemic vulnerability that arises due to the rapid development of technologies and the constant lag of the regulatory framework. interdisciplinary nature of digital violations. This leads to significant economic losses, stifles innovation, concentrates market power in the hands of dominant players and limits consumer choice. This requires adaptation of legislation, creation of new regulatory instruments, strengthening international cooperation to address cross-border problems, and proactive strategies on the part of rights holders.*

Keywords: *intellectual property, unfair competition, legal regulation, digital economy, economic consequences.*

ІНФОРМАЦІЯ ПРО АВТОРА

Андрощук Геннадій Олександрович — канд. екон. наук, доц., голов. н. с., Науково-дослідний інститут інтелектуальної власності Національної академії правових наук України, вул. Казимира Малевича, 11, корп. 4, м. Київ, Україна, 03680; +38 (044) 200-08-76; genandro1@gmail.com; ORCID: 0000-0003-0781-9740

INFORMATION ABOUT THE AUTHOR

Androshchuk H. O. — PhD in Economics, Associate Professor, Chief Researcher, Scientific Research Institute of Intellectual Property of the National Academy of Legal Sciences of Ukraine; 11, Kazymira Malevycha Str., building 4, Kyiv, 03680; +38 (044) 200-08-76; genandro1@gmail.com; ORCID: 0000-0003-0781-9740

Надійшла до редакції 10.11.2025