

УДК 330.341.1

АНДРОЩУК Г.О., кандидат економічних наук, доцент, головний науковий співробітник НДІ інтелектуальної власності НАПрН України
ORCID: <https://orcid.org/0000-0003-0781-9740>

НЕДОБРОСОВІСНА КОНКУРЕНЦІЯ В ЦИФРОВИХ РИНКАХ: ЗАГРОЗИ ТА ПРОТИДІЯ

DOI: [https://doi.org/10.37750/2616-6798.2025.4\(55\).346382](https://doi.org/10.37750/2616-6798.2025.4(55).346382)

Анотація. Здійснено економіко-правовий аналіз регулювання захисту від недобросовісної конкуренції в умовах цифрової економіки, впливу на інновації, конкуренцію та споживачів, виявлено загрози та рекомендовано заходи протидії. Показано, що недобросовісна конкуренція в цифрових ринках охоплює широкий спектр агресивних комерційних практик, що мають на меті ввести споживачів в оману та спотворити конкурентні умови, що зрештою підриває довіру споживачів. Такі дії проявляються через оманливу рекламу, маніпуляції даними та порушення прав інтелектуальної власності (ІВ). Ці практики шкодять добросовісним підприємствам, створюють дисбаланс на ринку, що призводить до зниження рівня інновацій та підвищення цін для кінцевих споживачів. Досліджено особливості цифрового ринку і цифрових платформ у сфері ІВ, їх функції і типи, значення для споживачів та інновацій. Проаналізовано маніпуляції з пошуковими системами (SEO-спам, наповнення ключовими словами), використання ботів для маніпуляції відгуками та рейтингами, вплив ШІ на конкурентну поведінку (алгоритмічна змова). Визначено виклики для конкурентного законодавства та регулювання цифрових платформ в Україні. Робиться висновок, що для ефективної боротьби з недобросовісною конкуренцією в цифровій сфері необхідний комплексний підхід, адаптація законодавства, посилення правозастосування, розвиток технологій виявлення зловживань та активна міжнародна співпраця. Забезпечення чесних та відкритих цифрових ринків є критично важливим для стимулювання інновацій, захисту споживачів та підтримки здорового економічного середовища.

Ключові слова: інтелектуальна власність, недобросовісна конкуренція, цифрова економіка, цифрові ринки, довіра споживачів, захист прав.

Summary. An economic and legal analysis of the regulation of protection against unfair competition in the digital economy, its impact on innovation, competition and consumers was conducted, threats were identified and measures to counter them were recommended. It was shown that unfair competition in digital markets covers a wide range of aggressive commercial practices aimed at misleading consumers and distorting competitive conditions, which ultimately undermines consumer trust. Such actions are manifested through misleading advertising, data manipulation and violation of intellectual property rights (IP). These practices harm bona fide enterprises, create an imbalance in the market, which leads to a decrease in the level of innovation and an increase in prices for end consumers. The features of the digital market and digital platforms in the field of IP, their functions and types, and their significance for consumers and innovation are studied. The analysis includes search engine manipulation (SEO spam, keyword stuffing), the use of bots to manipulate reviews and ratings, and the impact of AI on competitive behavior (algorithmic collusion). Challenges for competition law and regulation of digital platforms in Ukraine are identified. It is concluded that an integrated approach, adaptation of legislation, strengthening of law enforcement, development of technologies for detecting abuse, and active international cooperation are necessary to effectively

combat unfair competition in the digital sphere. Ensuring fair and open digital markets is critical to stimulating innovation, protecting consumers, and supporting a healthy economic environment.

Keywords: *intellectual property, unfair competition, digital economy, digital markets, consumer trust, protection of rights.*

Постановка проблеми. Загальне розуміння недобросовісної конкуренції в цифрових ринках. Паризька конвенція з охорони промислової власності (Паризька конвенція) у ст.10-bis (2) визначає, що *актом недобросовісної конкуренції є будь-який акт конкуренції, що суперечить чесним практикам у промислових і торговельних справах.* [1,с.156] У Типових положеннях ВОІВ про захист від недобросовісної конкуренції (Model Provisions on Protection Against Unfair Competition) здійснено уточнення дефініції “недобросовісної конкуренції”, що міститься в Паризькій конвенції, в якому відсутнє посилання на конкурентні відносини, як на один з основних критеріїв цього поняття. [2, с.189] Багато країн вже адаптувало ці рекомендації в своє національне законодавство.

Недобросовісна конкуренція в цифрових ринках охоплює широкий спектр практик, що мають на меті ввести споживачів в оману та спотворити конкурентні умови, що зрештою підриває довіру споживачів та цілісність бренду. Такі дії можуть проявлятися через оманливу рекламу, маніпуляції даними та порушення прав інтелектуальної власності. Ці практики не лише шкодять добросовісним підприємствам, але й створюють дисбаланс на ринку, що може призвести до зниження рівня інновацій та підвищення цін для кінцевих споживачів. Цифрові платформи, завдяки своїй здатності забезпечувати миттєву та масштабну взаємодію між мільйонами користувачів, створюють унікальні вигоди, такі як зниження транзакційних витрат, зменшення витрат на пошук інформації та ефективна організація великих обсягів даних. Вони надають величезну кількість можливих контрагентів для транзакцій або обміну інформацією в єдиному середовищі, часто за невелику або нульову вартість для кінцевого користувача. Однак, ця ж ефективність та здатність до масового збору даних створюють нові виклики для конкуренції.

Збір та використання даних користувачів дозволяють платформам зміцнювати свою владу над багатьма аспектами відносин між бізнесом та споживачами. Це зміцнення влади створює умови для недобросовісної конкуренції, оскільки домінуючі гравці можуть використовувати своє становище для отримання несправедливих переваг, що, у свою чергу, призводить до зменшення стимулів для інновацій та потенційного підвищення цін для споживачів. Отож, притаманна платформам ефективність, що сприяє їх швидкому зростанню та набуттю ринкової влади, через накопичення та використання даних, може перетворитися на джерело недобросовісної конкуренції та антиконкурентних практик.

Аналіз останніх досліджень та публікацій. Проблематику конкурентного права, захисту від недобросовісної конкуренції досліджували такі вітчизняні науковці (юристи і економісти) як Андрощук Г.О., Бакалінська О.О., Безух О.В., Борисенко З.М., Бутнік-Сіверський О.Б., Валітов С.С., Вознюк О.В., Дахно І.І., Журик Ю.В., Капіца Ю.М., Кодинець А.О. Лагутін В.Д., Полухович В.І., Смирнова К.В., Чернелевська О.Л., Шкляр С.В. та інші. Вагомий внесок у розвиток науково-правових досліджень цифрової економіки внесла О.М. Вінник, яка дослідила окремі проблеми антимонопольно-правового регулювання в умовах цифрової економіки.[3] Проте динамічність змін в економіці, законодавстві у сфері цифрової економіки, потребують подальших наукових досліджень.

Метою статті є економіко-правовий аналіз регулювання захисту від недобросовісної конкуренції в умовах цифрової економіки, впливу на інновації, конкуренцію та споживачів, виявлення загроз та їх протидії.

Виклад основного матеріалу дослідження. Еволюція конкурентного законодавства у відповідь на цифрові виклики. Правозастосування конкурентного законодавства постійно розвивається, адаптуючись до нових реалій цифрової економіки. Антимонопольні органи в усьому світі вдосконалюють інструменти та методології для боротьби з антиконкурентними практиками в різних секторах економіки. Особлива увага приділяється ролі даних у наданні послуг цифровими платформами, що привертає пильну увагу споживачів, бізнесу та регуляторів.

Європейський Союз (ЄС) став одним із лідерів у розробці нового регулювання, запровадивши Закон про цифрові ринки (Digital Markets Act, DMA), який набув чинності 7 березня 2024 року.[4] DMA є центральним елементом європейської цифрової стратегії, покликаним регулювати великі онлайн-платформи, так званих “гейткіперів”. Цей закон представляє собою фундаментальну зміну в підході до регулювання. Традиційне антимонопольне законодавство часто реагує на порушення вже *після* того, як вони відбулися (*ex post*). Однак, швидкий розвиток та унікальні характеристики цифрових ринків, такі як мережеві ефекти, накопичення даних та динаміка “переможець отримує все”, роблять такі втручання менш ефективними або занадто повільними. Підхід DMA, що ґрунтується на *ex ante* регулюванні, спрямований на запобігання зловживанням шляхом встановлення чітких “що дозволено” та “що заборонено” для гейткіперів *до* того, як шкода повністю матеріалізується. Це свідчить про визнання того, що швидкість та масштаб еволюції цифрового ринку вимагають більш проактивної регуляторної позиції для збереження конкурентоспроможності та стимулювання інновацій.

У своєму дослідженні В.І. Полухович зазначає: “Цифрові ринки — це електронні платформи, які функціонують на основі цифрових технологій в мережі “Інтернет”, є джерелами інформації та дозволяють на її основі здійснювати електронні трансакції, що служать підставою для переміщення, обміну, купівлі-продажу товарів, робіт, послуг. Вони поєднують продавців і покупців у віртуальному середовищі та включають широке коло економічних взаємодій — від електронної комерції і фінансових операцій до різноманітних онлайн-сервісів. Цифрові ринки мають такі характерні риси, як глобальний доступ, висока швидкість обміну інформацією, низькі транзакційні витрати, а також наявність великих обсягів даних, які впливають на ринкову конкуренцію, вибір споживачів та формують пропозицію”..[5, с.21]

Цифровий ринок і цифрові платформи у сфері інтелектуальної власності (ІВ)

— це надзвичайно важлива і динамічна сфера, яка суттєво трансформує підходи до створення, розповсюдження, захисту та монетизації об'єктів ІВ.

Цифровий ринок у сфері ІВ: Сутність: Це глобальне віртуальне середовище, де відбувається обіг цифрових товарів і послуг, які є об'єктами ІВ (наприклад, музика, фільми, програмне забезпечення, електронні книги, патенти, торгові марки). **Особливості:** **Глобалізація:** Дозволяє необмежений і швидкий доступ до об'єктів ІВ незалежно від географічного розташування. **Швидкість і масштабованість:** Миттєве копіювання, розповсюдження та використання цифрового контенту. **Виклики для ІВ:** Створює складнощі із захистом прав через легкість несанкціонованого копіювання (піратство), онлайн-шахрайства та фішинг. **Приклади ініціатив:** Ініціативи на кшталт **Єдиного цифрового ринку (ЄС)** спрямовані на створення рівних умов для доступу та захисту прав споживачів і бізнесу в цифровому просторі.

Цифрові платформи для ІВ: Це технологічні рішення та онлайн-сервіси, які полегшують управління, ліцензування, захист та комерціалізацію ІВ. **Основні функції та типи платформ:** **Платформи для розповсюдження контенту та ліцензування:** Стрімінгові сервіси (музика, відео) Онлайн-магазини програмного забезпечення, електронних книг. Маркетплейси, де автори можуть продавати свої твори (наприклад, фотостоки, платформи для 3D-моделей). **Платформи для управління та захисту ІВ:** Блокчейн-платформи (наприклад, Story (IP)): Використовуються для надійного та незмінного запису інформації про авторство, час створення, транзакції та ліцензування об'єктів ІВ. Це допомагає автоматизувати процес управління правами та захищати від фальсифікації. Системи Digital Rights Management (DRM): Технології для контролю використання цифрового контенту. **Платформи для патентування та торгових марок:** Онлайн-сервіси національних та міжнародних відомств, які спрощують подання заявок та управління портфелем ІВ. **Платформи для спільної роботи та інновацій:** Інструменти для командної розробки та управління проектами, де фіксується внесок кожного учасника (наприклад, *Notion*, *ClickUp* можуть опосередковано використовуватися для фіксації процесу створення). **Вплив на сферу ІВ:** Цифровий ринок і платформи створюють нові можливості, але й виклики: **Монетизація:** Нові моделі, як-от підписка, мікроплатежі та токенизація активів (NFT). **Доступність:** Спрощення доступу до ІВ для споживачів та спрощення процедур для правовласників. **Захист:** Посилення потреби в цифрових механізмах захисту (DRM, блокчейн) та оновлення законодавства для боротьби з піратством у мережі.

Значення для споживачів та інновацій. На цифрових ринках також мають місце прояви недобросовісної конкуренції, яка може здійснюватися у вигляді поширенні недостовірної інформації про товари, послуги або ділову репутацію конкурентів, незаконного використання торгових марок, промислових зразків (дизайнів) або інших об'єктів промислової власності конкурентів, а також у розголошенні або використанні комерційної таємниці конкурента без його згоди.[5, с.26-27] Недобросовісна конкуренція в цифрових ринках має негативні наслідки для споживачів та інновацій. Вона спотворює динаміку ринку, що може призвести до зменшення інновацій, оскільки фірми втрачають стимули до розробки нових продуктів, якщо конкуренти можуть займатися недобросовісними практиками. Крім того, це може призвести до підвищення цін для споживачів через відсутність конкуренції, що зменшує їхню купівельну спроможність. Важливим наслідком також є підриг довіри споживачів, оскільки користувачі стають обережними щодо маніпулятивних практик.

Закон про цифрові ринки (DMA) покликаний забезпечити чесну діяльність, запобігти зловживанню владою та становищем на ринку, а також захистити конфіденційність споживачів в інтернеті. Він має на меті надати споживачам більше вибору, кращі послуги та справедливіші ціни, а також забезпечити прямий доступ до послуг.

Ерозія довіри споживачів, спричинена недобросовісними практиками, є не просто наслідком, а й механізмом, що посилює спотворення ринку. Коли споживачі втрачають довіру до онлайн-інформації через оманливу рекламу або фальшиві відгуки, вони стають більш схильними до ризику. Це може призвести до того, що вони залишатимуться з усталеними, домінуючими платформами або брендами, які вони *сприймають* як надійні, навіть якщо ці платформи можуть займатися самопреференціями. Це небажання досліджувати альтернативи, підживлювана недовірою, ще більше зміцнює ринкову владу домінуючих гравців, ускладнюючи новим, інноваційним учасникам ринку отримання позицій. У результаті це пригнічує загальну

інноваційну активність на ринку. Таким чином, недобросовісні практики призводять до зниження довіри споживачів, що, у свою чергу, зменшує їхню готовність до зміни постачальника, закріплює домінуючих гравців і, як наслідок, гальмує інновації.

Маніпуляції з пошуковими системами (SEO-спам, наповнення ключовими словами).

Визначення та види SEO-спау.[6] SEO-спам, також відомий як спамдексинг, є сукупністю неетичних методів, що використовуються для маніпулювання рейтингом веб-сторінок у результатах пошукових систем. Ці тактики, часто класифіковані як “чорні” методи SEO, можуть принести короткострокові вигоди, але в довгостроковій перспективі серйозно шкодять довірі до веб-сайту, призводять до штрафів від пошукових систем і навіть до повного видалення з результатів пошуку (SERP).

Однією з найпоширеніших форм SEO-спау є **наповнення ключовими словами (Keyword Stuffing)**. Це неетична практика, яка полягає у надмірному заповненні веб-сторінки цільовими ключовими словами з метою маніпулювання рейтингом. Пошукові системи легко виявляють такі дії та застосовують санкції, оскільки контент, перенасичений ключовими словами, часто є нечитабельним та некорисним для користувачів.

Наповнення ключовими словами може бути реалізовано двома основними способами:

- **Видиме наповнення:** Це відбувається, коли ключові слова надмірно та неприродно повторюються в тексті, будучи видимими для читача, часто поза контекстом. Прикладом може бути: “Шукаєте найкращий пілосос? Ви прийшли в потрібне місце за найкращим пілососом. Наш бренд пропонує найкращий пілосос, який ви тільки можете побажати. Легкий, але потужний, це найкращий пілосос для всіх ваших потреб у прибиранні. Найкращий пілосос.”. Таке використання термінів є надмірним та нерелевантним. Також це може включати неприродне додавання довгого списку ключових слів в абзаці.

- **Невидиме наповнення:** Цей метод передбачає приховування спам-тексту від читачів, але залишення його доступним для пошукових роботів. Це може бути досягнуто шляхом використання тексту того ж кольору, що й фон сторінки, або розміщення ключових слів у невидимих частинах веб-сторінки, таких як alt-текст зображень, мета-теги або коментарі в HTML-коді.

Окрім наповнення ключовими словами, існують інші поширені форми SEO-спау[7]:

- **Придбання зворотних посилань (Buying Backlinks):** Це створення штучних посилань на сайт з інших ресурсів, часто з нерелевантних або спамних джерел, з метою маніпулювання авторитетом сторінки (“link juice”).

- **Дубльований контент (Duplicate Content):** Розміщення ідентичного або майже ідентичного контенту на кількох сторінках, що збиває з пантелику пошукові системи, оскільки їм важко визначити найбільш релевантну версію, і може негативно впливати на рейтинг.

- **Низькоякісний контент (Low-Quality Content):** Створення контенту, який не надає цінності користувачам, а лише призначений для маніпулювання рейтингом.

- **Прихований текст та посилання (Hidden Text and Links):** Розміщення тексту або посилань, які не видно користувачам, але доступні пошуковим системам.

- **Клікабельні заголовки та мета-описи (Clickbait Titles and Meta Descriptions):** Використання оманливих заголовків та описів для залучення кліків.

• **Спам у коментарях (Comment Spam):** Розміщення нерелевантних коментарів з посиланнями на інших сайтах, блогах або форумах.

• **Сторінки-двері (Doorway Pages):** Створення сторінок, які автоматично перенаправляють користувачів на інший ресурс без надання релевантного контенту.

• **Клоакінг (Cloaking):** Практика, при якій інформація, що представляється пошуковій системі, відрізняється від тієї, що відображається користувачам. Наприклад, сторінка може бути про бронювання готелів, але пошуковій системі представляється контент про фармацевтичні продукти.

• **Японський хак ключових слів (Japanese Keyword Hack):** Незвичайний, але поширений метод SEO-спаму, що полягає у впровадженні японських символів та контенту на сайт, зазвичай за допомогою грубої сили, для генерації зворотних посилань на шахрайські ресурси.

Вплив на результати пошуку, користувацький досвід та цілісність ринку. Маніпуляції з пошуковими системами здійснюють негативний вплив на результати пошуку, користувацький досвід та цілісність ринку.

Негативний вплив на SEO: Пошукові системи, такі як Google та Bing, чітко заявляють, що наповнення ключовими словами порушує їхні рекомендації. Вони активно знижують рейтинг або видаляють сайти, що займаються такими практиками. Сучасні пошукові системи є дуже складними: оновлення, такі як Hummingbird, BERT та MUM, дозволили Google значно краще розуміти контекст, синоніми та намір користувача, а не просто кількість входжень ключових слів. Це означає, що маніпулятивні тактики є неефективними, і Google застосовує ручні дії або автоматичні системи для виявлення та покарання такого контенту.

Погіршення користувацького досвіду: Контент, перенасичений ключовими словами, часто є нечитабельним та некорисним для користувачів. Це призводить до високого показника відмов (bounce rate), що, у свою чергу, сигналізує пошуковим системам про низьку якість сторінки, призводячи до її зниження в рейтингу. Пошукові системи надають перевагу сторінкам, які забезпечують чудовий користувацький досвід.

Спотворення результатів пошуку: Маніпуляції з пошуковими системами спотворюють результати, ускладнюючи для користувачів пошук релевантної та якісної інформації. Це має далекосяжні наслідки, впливаючи на рішення споживачів. Наприклад, в експерименті було показано, що маніпуляція результатами пошуку може змінити думку виборців, ймовірність впливу на голосування може сягати 25% для найбільш сприйнятливих груп населення. Кінцевим користувачам важко виявити такі маніпуляції, оскільки вони взаємодіють з пошуковою системою обмежену кількість разів і не мають необхідної експертизи для виявлення упередженості.

Еволюція SEO-спаму є постійним змаганням між маніпуляторами та пошуковими системами, де складні алгоритми, керовані штучним інтелектом (ШІ), адаптуються для виявлення та покарання “чорних” тактик. Спочатку просте наповнення ключовими словами могло бути ефективним, але пошукові системи швидко навчилися його виявляти. Це спонукало спамерів до більш прихованих методів, таких як клоакінг або прихований текст. У відповідь пошукові системи розробили більш складні алгоритми, які розуміють контекст та намір користувача, а не лише щільність ключових слів. Ця безперервна адаптація свідчить, що те, що колись було ефективним, стає згубним, оскільки штрафи є суворими. Це змінює конкурентний ландшафт від технічної маніпуляції до створення справжньої цінності, вимагаючи від ефективного SEO зосередженості на користувацькому досвіді та високоякісному, природному контенті. Слід зазначити, що захист пошукових систем, таких як Google, від звинувачень у

недобросовісній конкуренції, зокрема у пріоритезації власних сервісів, часто ґрунтується на аргументі, що їхні результати пошуку є формою “мови”, захищеної Першою поправкою (до Конституції США, яка проголошує загальні свободи громадян). Якщо результати пошуку справді класифікуються як мова, то регулювання їхнього ранжування для запобігання самопреференціям або іншим формам маніпуляції стає конституційно проблематичним. Це створює напругу між принципами свободи слова та антимонопольними цілями, потенційно дозволяючи домінуючим платформам виправдовувати практики, що спотворюють конкуренцію, під виглядом редакційної свободи. Це підкреслює значний юридичний виклик у застосуванні традиційних антимонопольних рамок до нових структур цифрового ринку. Види SEO-спаму та їхній вплив показано у Таблиці 1.

Таблиця 1.

Види SEO-спаму та їхній вплив

Вид SEO-спаму	Опис/Механізм	Приклад	Вплив на SEO/Користувача
Наповнення ключовими словами (Keyword Stuffing)	Надмірне, неприродне використання цільових ключових слів у контенті (видиме) або приховане в HTML-коді (невидиме).	Видиме: “Найкращий пилосос, найкращий пилосос, купити високий показник пилосос.” Невидиме: білий текст на білому фоні.	Зниження рейтингу, видалення з пошуку, поганий досвід.
Придбання зворотних посилань (Buying Backlinks)	Штучне створення посилань на сайт з нерелевантних або спамних джерел.	Посилання зі спамних сайтів, каталогів або нерелевантних блогів.	Шкода довірі до сайту, штрафи пошукових систем, зниження авторитету сторінки.
Дубльований контент (Duplicate Content)	Розміщення ідентичного або майже ідентичного контенту на кількох сторінках одного або різних сайтів.	Ідентичні описи продуктів на різних електронних сторінках комерції.	Зниження рейтингу, розбавлення пошукових позицій, негативний вплив на видимість.
Прихований текст та посилання (Hidden Text and Links)	Розміщення тексту або посилань, які не видно користувачам (наприклад, через колір, розмір шрифту), але невидимих елементів доступні пошуковим системам.	Текст, прихований за зображеннями, або посилання в системі.	Штрафи пошукових систем, зниження рейтингу.
Клоакінг (Cloaking)	Представлення пошуковим системам іншої інформації, ніж та, що відображається користувачам.	Для робота сторінка про ліки, для користувача – про готелі.	Google-штрафи, введення користувачів в оману.

Вид SEO-спаму	Опис/Механізм	Приклад	Вплив на SEO/Користувача
Впровадження			
Японський хак ключових слів (Japanese Keyword Hack)	японських символів та контенту на сайт для ранжування генерації зворотних японськими посилань на шахрайські пошуковими запитами. ресурси.	Сайт починає за японськими пошуковими запитами.	Шкода репутації, складність усунення, можливі штрафи.
Розміщення			
Спам коментарях (Comment Spam)	у нерелевантних коментарів посиланнями на інших сайтах, блогах або форумах.	Коментарі з посиланнями на комерційні сайти, пов'язані з темою обговорення.	Шкода репутації, не видалення коментарів, можливі штрафи.
Створення сторінок, які автоматично перенаправляють користувачів на інший ресурс без надання релевантного контенту.			
Сторінки-двері (Doorway Pages)	Сторінка, створена лише для перенаправлення на цільовий сайт, без корисної інформації.	Штрафи пошукових систем, негативний користувацький досвід.	

Використання ботів для маніпуляції відгуками та рейтингами. Визначення та методи маніпуляції за допомогою ботів.

Фальшиві відгуки — це навмисно оманливі оцінки або відгуки, що спотворюють правду про бізнес або продукт. Вони можуть походити від різних джерел, включаючи продавців, сторонні агентства, автоматизовані боти або конкурентів, що робить їх виявлення дедалі складнішим.

Методи маніпуляції за допомогою ботів та фальшивих відгуків включають:

- **Штучне завищення популярності:** Фальшиві 5-зіркові відгуки використовуються для штучного завищення сприйняття якості продукту або послуги. Наприклад, на Amazon надзвичайно рідко можна знайти продукт лише з 5-зірковими відгуками, і така закономірність може вказувати на шахрайську діяльність.

- **Пошкодження репутації конкурентів:** Фальшиві негативні відгуки завдають шкоди репутації бренду та вводять споживачів в оману. Це може бути скоординована атака з боку конкурента.

- **Маніпуляція поведінкою споживачів:** Контент, згенерований ботами, не є справжнім людським досвідом, що спотворює показники залученості та впливає на рішення про покупку. Фальшиві відгуки можуть стимулювати бажання покупки, змінюючи сприйняття попиту, або впливати на оцінку альтернативних планів.

- **“Мережева водна армія”:** Це групи, що діють з високим рівнем приховування та груповими операціями, створюючи фальшивий та зловмисний маркетинг.

- **“Набивання” (brushing):** Практика маніпулювання відгуками, що вводять в оману громадськість щодо реальної діяльності магазину, впливаючи на поведінку споживачів.

- **Оманливі стимули:** Деякі споживачі пишуть фальшиві відгуки в обмін на безкоштовні товари, знижки або інші бонуси, пропоновані брендами. Прикладом може

бути справа бренду догляду за шкірою Sunday Riley, який інструктував своїх співробітників писати фальшиві позитивні відгуки на сайті Sephora.

Вплив на довіру споживачів, рішення про покупку та чесну конкуренцію. Вплив фальшивих відгуків та ботів на довіру споживачів, їхні рішення про покупку та чесну конкуренцію є значним та руйнівним.

Ерозія довіри споживачів: Фальшиві відгуки та боти становлять серйозну загрозу довірі споживачів та репутації бренду. Згідно зі звітом BrightLocal за 2023 рік, 98% споживачів читають онлайн-відгуки, і, на жаль, 42% з них стикалися з тим, що вони вважають фальшивими відгуками. [8] Використання ботів для штучного створення контенту у великих масштабах ще більше підриває довіру споживачів до брендів, які можуть сприйматися як оманливі або маніпулятивні. Навіть справжні та достовірні відгуки можуть зустрічатися зі зростаючим скептицизмом через поширеність фальшивих.

Спотворення рішень про покупку: Фальшиві відгуки створюють значні перешкоди для споживачів у прийнятті правильних рішень про покупку. Вони можуть стимулювати бажання покупки, змінюючи сприйняття попиту, або впливати на оцінку альтернативних планів. В епоху великих даних та інформаційних технологій, зіткнувшись з численними продавцями та обмеженим часом, споживачі зазвичай зосереджуються на рівні довіри продавця та оцінках інших споживачів при виборі продуктів. Практика “набивання” (brushing) може ввести громадськість в оману щодо реальної діяльності магазину, що зрештою впливає на купівельну поведінку споживачів.

Недобросовісна конкуренція: Фальшиві відгуки створюють недобросовісну конкуренцію на ринку. Менш конкурентоспроможні компанії часто використовують їх як швидкий спосіб штучно покращити свій імідж, тоді як якісніші конкуренти можуть страждати від цілеспрямованих негативних відгуків. Ця маніпуляція підриває справедливість екосистеми е-комерції, яка має винагороджувати бізнес на основі автентичної репутації.

Соціальні та політичні ризики: Окрім впливу на репутацію бренду, боти можуть мати значний соціальний та політичний вплив. Дослідження 2019 року виявило, що соціальні боти відіграли "непропорційну роль у поширенні дезінформації в інтернеті" під час президентських виборів у США 2016 року, причому 6% облікових записів Twitter, ідентифікованих як боти, поширювали 31% інформації з низьким рівнем довіри.

Поява генеративного штучного інтелекту (ШІ) значно ускладнює проблему фальшивих відгуків, перетворюючи їх виявлення з простого розпізнавання патернів на складний лінгвістичний та поведінковий аналіз. Хоча фальшиві відгуки завжди були проблемою, поява генеративного ШІ означає, що вони стають “більш досконалішими та складнішими для виявлення”. Це свідчить про перехід від простих, легко ідентифікованих патернів (наприклад, загальна мова, раптові сплески) до більш складного, людиноподібного контенту. Отже, методи виявлення повинні еволюціонувати від базового аналізу патернів до передового лінгвістичного аналізу на основі ШІ. Ця ескалація змагальності між шахрайством, що генерується ШІ, та виявленням, керованим ШІ, покладає більший тягар на платформи та регулятори, вимагаючи інвестування в передові технології та постійної адаптації стратегій. [9]

Важливим аспектом є те, що тягар доведення для видалення фальшивих відгуків часто лягає на самі підприємства. Хоча платформи повільно реагують на скарги щодо фальшивих відгуків, саме постраждалий бізнес часто несе відповідальність за доведення шахрайства. Це створює значний оперативний та фінансовий тягар для підприємств, які

дотримуються правил. Така асиметрія означає, що ті, хто займається недобросовісними практиками, стикаються з меншим безпосереднім ризиком та витратами, тоді як їхні жертви несуть значні витрати та репутаційну шкоду. Це може призвести до “тонки на дно”, де підприємства можуть бути спокушені використовувати подібні тактики для виживання, що ще більше забруднює ринок та підриває саму мету зворотного зв'язку від споживачів.

• **Методи виявлення фальшивих відгуків та ботів.** Для боротьби з маніпуляціями відгуками та рейтингами застосовують різноманітні методи виявлення:

• **Аналіз патернів відгуків:** Виявлення великих обсягів відгуків за короткі періоди, надмірної кількості 5-зіркових (або 1-зіркових) оцінок, сплесків, що збігаються з діями конкурентів, а також дубльованих або надто загальних відгуків.

• **Аналіз патернів рецензентів:** Перевірка облікових записів з мінімальними деталями або активністю, віку облікового запису, кількості відгуків, повноти профілю.

• **Лінгвістичний аналіз:** Використання ШІ для виявлення семантичних патернів, що вказують на текст, згенерований ботами, таких як незвичайна синтаксис, повторення та граматичні помилки.

• **Перевірка метаданих:** Аналіз IP-адрес, геолокації та часових міток для виявлення ферм відгуків.

• **Стратегія “медової пастки” (Honeypot strategy):** Створення фіктивних пропозицій для приваблення фальшивих рецензентів та подальший аналіз їхніх патернів.

• **Перевірка рецензентів:** Ручний контакт та верифікація підозрілих рецензентів з великою кількістю відгуків для підтвердження їхньої справжності.

• **Стимування:** Активний моніторинг, повідомлення та вжиття правових заходів проти підтверджених фальшивих рецензентів. Запропоновані правила FTC роблять фальшиві відгуки незаконними, передбачаючи значні штрафи.

• **Проактивні політики платформ:** Заохочення платформ до постійного вдосконалення механізмів виявлення фальшивих відгуків за допомогою технологій та людського нагляду.

• **Платформи управління відгуками:** Використання спеціалізованих платформ, які допомагають брендам моніторити, керувати та відповідати на відгуки, а деякі використовують NLP для виявлення тенденцій та настроїв.

• **Інструменти для споживачів:** Доступні інструменти на основі ШІ, такі як розширення для браузера FakeSpot, які допомагають споживачам самостійно виявляти фальшиві відгуки.

• **Моніторинг аномальних сплесків:** Відстеження незвичайних сплесків обговорень або раптових змін настроїв, пов'язаних з галуззю, на форумах та в соціальних мережах.

• **Трасування метаданих облікових записів:** Дослідження метаданих облікових записів, таких як дати створення профілю, обсяг опублікованого контенту та геолокація, для ідентифікації мереж ботів.

• **Зворотний пошук зображень:** Використання Google зворотного пошуку зображень для визначення походження зображень, які використовуються підозрілими обліковими записами ботів.

• **Цифрове маркування:** Розгляд можливості цифрового маркування власного контенту, щоб копії, змінені ботами, залишалися прив'язаними до оригінального джерела.

- **Зловживання домінуючим становищем на ринку цифрових послуг (самопреференції, обмеження доступу).**

- **Визначення домінуючого становища та його особливості в цифрових ринках.** Домінуюче становище на ринку цифрових послуг часто пов'язане з поняттям “гейткіперів”, визначених Законом про цифрові ринки (DMA) Європейського Союзу. Гейткіпери — це великі цифрові платформи, які пропонують певні “основні послуги платформи”, такі як онлайн-пошукові системи, магазини додатків та месенджери. Щоб бути визначеною як гейткіпер, компанія повинна відповідати кільком критеріям: мати сильну економічну позицію та значний вплив на внутрішній ринок, діяти в багатьох країнах ЄС; займати сильну посередницьку позицію, тобто пов'язувати велику базу користувачів з великою кількістю підприємств; та мати усталене та стійке становище на ринку, що означає, що їхня позиція залишалася стабільною протягом тривалого часу. Станом на 6 вересня 2023 року Європейська Комісія визначила шість компаній як гейткіперів: Alphabet, Amazon, Apple, ByteDance, Meta та Microsoft.[10] Особливості домінуючого становища в цифрових ринках полягають у тому, що доступ та управління даними користувачів можуть ще більше зміцнювати владу цих платформ над різними аспектами відносин між бізнесом та споживачами. Платформи часто отримують вигоду від мережевих ефектів, коли цінність платформи збільшується зі зростанням кількості користувачів, що створює ефект “переможець отримує все”. Крім того, вони користуються економією масштабу, досягаючи ефективності шляхом одночасного надання кількох послуг.

- **Самопреференції (Self-Preferencing).** Самопреференції — це практика, коли цифрова платформа надає перевагу власним продуктам або послугам над послугами конкурентів. Це може проявлятися різними способами:

- **Пріоритезація у пошукових результатах:** Google може упереджено ставитися до відеоконтенту, розміщеного на YouTube (актив Alphabet), або надавати вищий рейтинг фірмам, які заплатили за це.

- **Вибірковість у маркетплейсах:** Пошук продукту на Amazon, наприклад, тостера, може надавати перевагу власній марці Amazon Basics, розміщуючи її першою у списку.

- **За замовчуванням встановлені сервіси:** Виробник мобільних телефонів з операційною системою Android (продукт Google) може зробити Google Search пошуковою системою “за замовчуванням” на новому пристрої. Хоча користувачі можуть завантажувати інші пошукові системи, статус “за замовчуванням” є надзвичайно цінним, як показує щорічна плата Alphabet компанії Apple у розмірі 12 млрд доларів за статус пошукової системи за замовчуванням на iPhone.

- **Обмеження в магазинах додатків:** Apple, наприклад, обмежує продаж додатків для iPhone власним App Store, де стягує значну комісію.

Закон про цифрові ринки (DMA) прямо забороняє гейткіперам віддавати перевагу власним продуктам або послугам у рейтингу над аналогічними послугами або продуктами, пропонованими третіми сторонами на їхній платформі. Вони також повинні дозволяти своїм бізнес-користувачам просувати свої пропозиції та укладати контракти зі своїми клієнтами за межами платформи гейткіпера. Ці положення спрямовані на забезпечення чесного бізнес-середовища для бізнес-користувачів, які залежать від гейткіперів.

Антимонопольні органи вже давно розслідують такі практики. Європейська Комісія, наприклад, оштрафувала Google на 4,34 млрд євро за зловживання домінуючим становищем через самопреференції у практиках Android.[11] Amazon також стикався з антимонопольним контролем щодо поводження з сторонніми продавцями на своїй

платформі. DMA, запроваджуючи *ex ante* регулювання, є прямою відповіддю на обмеження *ex post* правозастосування в динамічних цифрових ринках. Це підкреслює, що регулятори визнають необхідність попереджувальних заходів для забезпечення конкурентоспроможності.

Обмеження доступу (Restriction of Access). Обмеження доступу — це практика, коли домінуюча платформа використовує свій контроль для обмеження або перешкоджання доступу конкурентів до ринку або до своїх послуг. Це може проявлятися у вигляді:

- **Заборони зв'язуватися з бізнесом за межами платформи:** Гейткіпери не можуть перешкоджати споживачам зв'язуватися з бізнесом за межами їхніх платформ.

- **Обмеження на видалення програмного забезпечення:** Гейткіпери не повинні перешкоджати користувачам видаляти будь-яке попередньо встановлене програмне забезпечення або додатки, якщо вони бажають це зробити.

- **Примусове використання платіжних систем:** Гейткіпери не можуть змушувати розробників додатків використовувати власні платіжні системи для покупок у додатках, а повинні дозволяти використання сторонніх платіжних систем.

- **Несправедливі умови для розробників додатків:** Гейткіпери не можуть нав'язувати несправедливі умови розробникам додатків для доступу до своїх магазинів додатків.

DMA встановлює чіткі зобов'язання для гейткіперів щодо забезпечення справедливого доступу та інтероперабельності. Вони повинні дозволяти третім сторонам взаємодіяти зі своїми послугами в певних визначених ситуаціях. Також гейткіпери зобов'язані надавати своїм бізнес-користувачам доступ до даних, згенерованих через використання платформи гейткіпера, на справедливих, розумних та недискримінаційних умовах. Для месенджерів це означає, що гейткіпери повинні забезпечити інтероперабельність своїх служб обміну повідомленнями зі сторонніми службами.

Цифрові ринки часто характеризуються мережевими ефектами, коли цінність платформи зростає зі збільшенням кількості користувачів, що може створити середовище “переможець отримує все”. Це створює виклики для нових учасників ринку, оскільки їм важко подолати існуючі бар'єри входу, що зміцнює позиції вже усталених гравців.

Вплив на конкуренцію, інновації та споживачів. Зловживання домінуючим становищем, включаючи самопреференції та обмеження доступу, має значний негативний вплив на конкуренцію, інновації та споживачів. Це призводить до зниження інновацій, оскільки менші фірми та стартапи стикаються з перешкодами для конкуренції та розвитку. Споживачі можуть зіткнутися з вищими цінами через відсутність конкуренції та мати менший вибір послуг. Також це може призвести до закріплення ринку, де новим учасникам важко конкурувати, що веде до монополістичної поведінки.

Закон про цифрові ринки (DMA) покликаний протидіяти цим негативним наслідкам. Він створює більш справедливе бізнес-середовище для бізнес-користувачів, які залежать від гейткіперів. Інноватори та технологічні стартапи отримують нові можливості для конкуренції та інновацій без несправедливих умов, що обмежують їхній розвиток. Споживачі отримують більше та кращих послуг на вибір, більше можливостей змінити постачальника та справедливіші ціни.

Недотримання зобов'язань DMA може призвести до значних наслідків для гейткіперів, включаючи штрафи до 10% від загального річного світового обороту компанії (до 20% у разі повторних порушень) та періодичні штрафні санкції до 5% від

середньоденного обороту. [4] У разі систематичних порушень можуть бути накладені додаткові заходи, включаючи нефінансові заходи, такі як відчуження частин бізнесу. DMA також спрямований на усунення проблеми регуляторної фрагментації, спричиненої національними законодавчими ініціативами в країнах-членах ЄС, що раніше призводило до збільшення витрат на дотримання вимог для транскордонних платформ. Нові правила забезпечують чітко визначені зобов'язання для гейткіперів, тоді як менші гравці та стартапи не підпадають під ці правила, але отримують вигоду від справедливішої поведінки при взаємодії з гейткіперами.

Вплив ШІ на конкурентну поведінку (алгоритмічна змова). Визначення та форми алгоритмічної змови. [12,13]

Алгоритмічна змова — це явище, коли алгоритми використовуються для координації цін, обсягів виробництва або інших конкурентних змінних між фірмами, тим самим обмежуючи конкуренцію. Це є однією з найбільш актуальних проблем у контексті зростаючої залежності ринків від ШІ для встановлення цін, особливо на цифрових ринках.

Алгоритмічна змова може приймати різні форми:

- **Фіксація цін (Price-fixing):** Алгоритми можуть бути використані для встановлення цін на певному рівні, усуваючи цінову конкуренцію між фірмами.
- **Розподіл ринку (Market allocation):** Алгоритми можуть бути використані для розподілу ринків або клієнтів між фірмами, зменшуючи конкуренцію.
- **Обмеження виробництва (Output restriction):** Алгоритми можуть бути використані для обмеження виробництва, тим самим зменшуючи пропозицію та підвищуючи ціни.

Алгоритми відіграють вирішальну роль у ціноутворенні, обсягах виробництва та інших бізнес-рішеннях у цифровій економіці. Вони можуть сприяти змові шляхом моніторингу та забезпечення виконання змовницьких угод, координації цін та обсягів виробництва, а також адаптації до змін ринкових умов.

Механізми та приклади. Механізми алгоритмічної змови ґрунтуються на використанні складних алгоритмів, які обробляють великі обсяги даних для прийняття рішень.

- **Алгоритми ціноутворення:** Ці алгоритми використовують дані про ціни, попит та інші ринкові змінні для встановлення цін.
- **Алгоритми машинного навчання:** Ці алгоритми використовують дані для вивчення патернів та здійснення прогнозів, які можуть бути використані для сприяння змові.

Приклади алгоритмічної змови включають:

- **Справа Топкінса (Topkins case):** У 2016 році Міністерство юстиції США оштрафувало Девіда Топкінса, генерального директора компанії з виробництва плакатів, за використання алгоритмів для фіксації цін.
- **Справа Трода (Trode case):** У 2018 році Управління з питань конкуренції та ринків Великої Британії оштрафувало Trode, онлайн-компанію з продажу плакатів, за використання алгоритмів для фіксації цін.
- **Справа RealPage Inc.:** Міністерство юстиції США висловило занепокоєння щодо використання сторонніх алгоритмів ціноутворення, зокрема у справі проти RealPage Inc., чий інструмент ціноутворення на основі ШІ для оренди житла нібито сприяли змові між орендодавцями. Подібні судові позови були подані проти інструментів ціноутворення в готельній та орендній галузях, що свідчить про зміну акценту антимонопольного законодавства на алгоритмічне ціноутворення в різних галузях.

Важливою проблемою є так звана “мовчазна співпраця” або “паралельна поведінка”, коли алгоритми можуть узгоджувати ринкову поведінку конкурентів без явних людських угод. Це відбувається, коли кожне підприємство використовує власний алгоритм встановлення цін, і хоча між компаніями немає початкового чи постійного зв'язку, алгоритми можуть автономно досягати цілей, що призводять до антиконкурентних результатів.

Виклики для антимонопольного законодавства та регулювання. [12] Зростаюча залежність від ШІ в ціноутворенні створює значні виклики для існуючих антимонопольних рамок, які традиційно ґрунтуються на припущенні, що змова є процесом, керованим людиною.

Основні виклики включають:

- **Відсутність прозорості:** Алгоритми можуть бути складними та непрозорими, що ускладнює виявлення змови.

- **Відсутність наміру:** Алгоритми можуть сприяти змові без людського наміру, що ускладнює встановлення відповідальності. Це є фундаментальним викликом для юридичної концепції “змови” та “відповідальності”, оскільки традиційне право вимагає доведення наміру. Коли алгоритм діє автономно, досягаючи антиконкурентного результату, виникає питання, чи можна приписати цей намір компанії, яка його розробила або використовує. Це вимагає переоцінки існуючих правових рамок.

- **Відсутність юрисдикції:** Алгоритмічна змова може залучати фірми з кількох юрисдикцій, що ускладнює координацію правозастосування.

Існує дискусія серед науковців щодо того, чи має антимонопольне законодавство бути більш суворим чи, навпаки, більш м'яким у відповідь на технології ШІ. Також виникають занепокоєння щодо хижацького ціноутворення, яке може бути полегшене ШІ, дозволяючи фірмам мінімізувати втрати та ефективніше відшкодовувати витрати. Регуляторам необхідно переглянути контрфактичні оцінки, які використовуються для визначення цінових умов за відсутності змовницької поведінки, щоб вони відображали можливості алгоритмічного ціноутворення на основі ШІ.

Для бізнесу, що використовує алгоритмічне ціноутворення, для зниження ризиків рекомендується вживати таких заходів:

- **Перегляд та аудит алгоритмічних моделей ціноутворення:** Документувати, що використання ШІ та алгоритмічного ціноутворення є лише одним з факторів визначення справедливої ціни, та регулярно перевіряти алгоритми на наявність ризиків координації.

- **Впровадження суворого моніторингу та контролю:** Забезпечити автоматизовані системи відстеження та людський нагляд для функціонування алгоритмів, моніторинг коригувань цін у реальному часі та ведення журналів аудиту для рішень щодо ціноутворення.

- **Підтримка ретельної документації:** Зберігати записи, які пояснюють, як функціонують моделі ціноутворення та чому приймаються конкретні рішення, включаючи журнали рішень щодо розробки алгоритмів та їх оновлень.

- **Уникнення недовіри клієнтів:** Розглядати питання прозорості використання алгоритмічних інструментів ціноутворення, оскільки розкриття такої інформації може відштовхнути потенційних клієнтів, які сприймають цю технологію як маніпулятивну або несправедливу.

Концепція ШІ як “продовженої руки” підприємства набуває дедалі більшого значення для забезпечення підзвітності. Якщо алгоритм виконує свої функції для підприємства та під його керівництвом, він інтегрований в економічну одиницю

підприємства, і компанія несе відповідальність за його дії, подібно до дій працівника. [14]

Український контекст: Законодавство та регулювання.

Загальні положення українського законодавства про конкуренцію. В Україні питання захисту від недобросовісної конкуренції та антимонopolного регулювання регулюються ст.42 Конституції, Законами України “«Про захист від недобросовісної конкуренції”, “Про захист економічної конкуренції” та “Про захист прав споживачів”. Ці закони, хоча і не містять безпосереднього визначення “цифрових ринків”, забороняють низку антиконкурентних практик. До них належать зловживання монополічним становищем на ринку, що може призвести до обмеження конкуренції або заподіяння шкоди споживачам, а також антиконкурентні узгоджені дії. В Законі України “Про захист прав споживачів” закріплено нові підходи до тлумачення нечесної комерційної практики та визначено критерії, за якими визначається чи є комерційна практика нечесною, прописано визначення, види та регулювання оманливої комерційної практики. Новий Закон значно посилює регулювання в цій частині захисту прав споживачів та встановлює для суб’єктів господарювання підвищені вимоги та обмеження. Позитивним є також визначення вичерпного переліку видів агресивної комерційної практики. Окремо закон забороняє недобросовісну конкуренцію, яка включає неправомірне використання ділової репутації, поширення неправдивої інформації та створення перешкод для діяльності конкурентів. Ці правила спрямовані на сприяння прозорості та запобігання діям, що можуть обмежувати конкуренцію, таким як маніпуляції з цінами або створення монополічних умов на ринку.

Регулювання цифрових послуг та контенту. З 7 березня 2024 року в Україні набув чинності Закон України «Про цифровий контент та цифрові послуги». [15] Цей закон визначає ключові поняття у сфері цифрових продуктів:

- **Цифровий контент:** Дані, що створюються та надаються в цифровій формі, включаючи комп’ютерні програми, застосунки, відео- та аудіофайли, музичні файли, цифрові ігри та електронні книги.

- **Цифрові послуги:** Послуги, що надають споживачам можливість створювати, обробляти, зберігати та поширювати дані в цифровій формі або отримувати доступ до таких даних. До них належать хмарні сервіси, соціальні мережі, сервіси потокового відео (наприклад, Netflix або Spotify).

Закон поширюється на відносини, в яких цифровий контент та/або цифрові послуги розробляються відповідно до специфікації споживача, а також на відносини, в яких виконавець надає цифровий контент на матеріальному носії, що використовується виключно для зберігання такого контенту. Компанії, що працюють у цій сфері, зобов’язані переглянути умови договорів, впровадити політики, що гарантують якість продуктів, та забезпечити підтримку клієнтів у разі проблем. Важливою вимогою є також надання оновлень для продуктів з метою забезпечення їхньої безпеки та функціональності.

Виклики антимонopolного регулювання цифрових платформ в Україні. Цифрові платформи, алгоритми та Великі Дані є новою реальністю глобальної цифрової економіки. Основні гравці ринку цифрових платформ використовують інноваційне середовище для забезпечення домінуючого становища на ринку. Використання компаніями передових технологій дозволяє їм нав’язувати споживачам неправомірні умови, розширювати ринкову владу, підвищувати ціни та закривати ринки для потенційних конкурентів.

Нова модель ринкової конкуренції в умовах цифрової економіки вимагає використання якісно нових інструментів регулювання та вдосконалення існуючих способів захисту конкуренції [16]. Нещодавно Мінцифри запустило Digital State UA-платформу цифрової України. Платформа представляє досягнення України в GovTech, IT і Tech. На жаль, український законодавець ще не приділяє достатньої уваги проблемам функціонування цифрових платформ. Домінування глобальних цифрових платформ та брак в Україні “національних” платформ ставить українських підприємців у заздалегідь програшне становище, створюючи ризик втрати українськими торговими мережами контакту з українськими ж споживачами. Існує загроза монополізації ринків з боку глобальних цифрових монополій, що використовують потужні цифрові платформи, та витіснення ними менших гравців.

Як зазначає Бутнік-Сіверський О.Б. “Розвиток цифровізації економіки інтелектуальної власності в умовах цифрових платформ, як ознака людино-цифрової системи, вимагає докорінних змін у загальних підходах правової регламентації нового типу економічних відносин, оскільки діяльність цифрових платформ зачіпає предмети як публічного (фінансове, податкове), так і приватного права (цивільне, господарське, трудове)”. [17, с.32]

Антимонопольний комітет України (АМКУ) визнає необхідність адаптації конкурентного законодавства. У жовтні 2023 року АМКУ визначив вектор для аналізу товарних меж ринку за наявності ринкової влади покупця (монопсонії), що відображає міжнародний досвід та розвиток конкурентного законодавства. Це свідчить про розуміння того, що антимонопольні органи в усьому світі вдосконалюють інструменти та методології для боротьби з антиконкурентними практиками, і Україна також долучається до цього процесу, розширюючи своє розуміння ринкової влади за межі традиційних монополій.

Висновки. Недобросовісна конкуренція в сфері нових технологій та цифрових платформ є складною та динамічною проблемою, що постійно еволюціонує разом з технологічним прогресом. Вона охоплює широкий спектр практик, від маніпуляцій пошуковими системами та відгуками до зловживання домінуючим становищем та алгоритмічної змови. Ці практики не лише спотворюють ринкові умови, але й підривають довіру споживачів, гальмують інновації та можуть мати значні соціальні та політичні наслідки.

Ключові висновки з проведеного аналізу:

1. **Двоїста природа цифрових платформ:** Хоча цифрові платформи є надзвичайно ефективними та сприяють зниженню транзакційних витрат, їхня здатність до масового збору даних та мережеві ефекти можуть призводити до зміцнення ринкової влади та створення умов для недобросовісної конкуренції.

2. **Еволюція регулювання:** У відповідь на ці виклики конкурентне законодавство у світі, зокрема в Європейському Союзі із Законом про цифрові ринки (DMA), переходить від реактивного (ex post) до превентивного (ex ante) підходу. Це свідчить про визнання необхідності проактивних заходів для збереження конкурентоспроможності ринків, що швидко змінюються.

3. **Постійна “гонка озброєнь”:** У сферах SEO-спаму та маніпуляцій відгуками спостерігається безперервна адаптація між маніпуляторами та системами виявлення, керованими ШІ. Це вимагає від бізнесу та регуляторів постійних інвестицій у передові технології та стратегії для захисту цілісності ринку та довіри споживачів.

4. **Виклики для традиційного права:** Алгоритмічна змова, де ШІ може координувати ринкову поведінку без явного людського наміру, створює фундаментальні

виклики для існуючих антимонопольних рамок, які традиційно вимагають доведення людської змови. Це вимагає переосмислення понять відповідальності та наміру в цифрову епоху.

5. Втрата довіри споживачів: Ерозія довіри споживачів через фальшиві відгуки та оманливі практики не є лише наслідком, а й механізмом, що посилює домінування великих гравців, оскільки споживачі стають менш схильними досліджувати альтернативи.

6. Український контекст: Українське законодавство поступово адаптується до реалій цифрової економіки, зокрема із Законом “Про цифровий контент та цифрові послуги”. Однак існує нагальна потреба у подальшому вдосконаленні регулювання конкуренції для ефективної протидії зловживанням домінуючим становищем та недобросовісним конкурентним практикам глобальних цифрових платформ та захисту національних підприємств.

Для ефективної боротьби з недобросовісною конкуренцією в цифровій сфері необхідний комплексний підхід, що включає постійну адаптацію законодавства, посилення правозастосування, розвиток технологій виявлення зловживань та активну міжнародну співпрацю. Забезпечення чесних та відкритих цифрових ринків є критично важливим для стимулювання інновацій, захисту споживачів та підтримки здорового економічного середовища.

Використана література

1. Боденгаузен Г. Паризька конвенція з охорони промислової власності: коментар / пер. з англ., передм. та наук. ред. Г.О.Андрощука. Київ: Парламентське вид-во, 2018. 264 с.
2. Андрощук Г.О. Конкурентне право: захист від недобросовісної конкуренції.. / Г.О. Андрощук, С.В. Шкляр - Науково-практичне видання. К.: Юстініан, 2012. 472 с.
3. Вінник О.М. Право цифрової економіки. Київ : НДІ приватного права і підприємництва імені академіка Ф.Г. Бурчака НАПрН України, 2021. 350 с. Repository of Academic Texts of Academician F. H. Burchak Scientific Research Institute of Private Law and Entrepreneurship of National Academy of Law Sciences of Ukraine. URL: <https://t.ly/osxVj>.
4. The Digital Markets Act URL: https://digital-markets-act.ec.europa.eu/index_en
5. Валерій Полухович Захист економічної конкуренції на цифрових ринках в Україні // Університетські наукові записки, – Хмельницький. 2024. № 5 (101), С. 17-30. DOI 10.37491/UNZ.101.2
6. Sanja Trajcheva What is SEO Spam and How Does It Impact Your Site? URL: What is SEO Spam and How Does It Impact Your Site?
7. Aaron R. Winston 10 SEO Spam Types & How to Avoid: Personal Injury Lawyers URL 6 10 SEO Spam Types & How to Avoid: Personal Injury Lawyers
8. Local Consumer Review Survey 2023 URL: <https://www.brightlocal.com/research/local-consumer-review-survey-2023/>
9. Fake Reviews: A Growing Threat to Trust in the Digital Marketplace URL: Fake Reviews: A Growing Threat to Trust in the Digital Marketplace - Center for Digital Society
10. Commission designates six gatekeepers under the Digital Markets Act URL: https://digital-markets-act.ec.europa.eu/commission-designates-six-gatekeepers-under-digital-markets-act-2023-09-06_en
11. Commission fines Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine URL: <https://ec.europa.eu/newsroom/comp/items/631884/>
12. Sarah Lee Algorithmic Collusion in Antitrust URL: Algorithmic Collusion in Antitrust

13. Maria Giacalone Algorithmic Collusion: Corporate Accountability and the Application of Art. 101 TFEU. URL: Algorithmic Collusion: Corporate Accountability and the Application of Art. 101 TFEU | European Papers

14. Андрощук Г.О. Штучний інтелект і інтелектуальна власність: проблеми регулювання: науково-практичне видання. НДІ ІВ НАПрН України. К.: Інтерсервіс, 2023.- 204 с. URL: <https://ekmair.ukma.edu.ua/server/api/core/bitstreams/0a3ae7df-6993-490d-9eae-d5a6d1cab8d1/content>

15. Про цифровий контент та цифрові послуги. Закон України від 10.08.2023 р. № 3321–IX. Верховна Рада України. Законодавство України. URL: https://t.ly/o__DJ.

16. Інтелектуальна власність в цифровій економіці: проблеми теорії і практики (колективна монографія) за наук. ред. канд. екон. наук. доцента Г.О. Андрощука. К.: Інтерсервіс, 2025. 452 с. URL <https://drive.google.com/file/d/16xDa1LRj52vOFVJv6oYVaIptpNtyvDoF/view>

17. Бутнік-Сіверський, О.Б. Цифрові платформи на шляху цифровізації економіки інтелектуальної власності // Удосконалення законодавства та механізму реалізації захисту прав інтелектуальної власності в умовах післявоєнного відновлення України. Секція 6. «Управління проєктами. Перспективи розвитку проєктного та нейроменеджменту, інформаційних технологій управління, технологій створення та використання об’єктів права інтелектуальної власності, трансферу технологій»: збірник наукових праць за матеріалами V Міжнародної науково-практичної інтернет-конференції, 23–24 березня 2023 р. – Київ, 2023. – С. 29-32. URL <https://dspace.nuft.edu.ua/items/da76854c-f835-4922-af60-0e94318e03aa>

~~~~~ \* \* \* ~~~~~