

ДОСЛІДЖЕННЯ

ПОРУШЕННЯ ПРАВ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В СФЕРІ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

1. Вступ.....	3
1.1. Актуальність проблеми.....	3
1.2. Мета та завдання дослідження.....	3
1.3. Об'єкт і предмет дослідження.....	4
1.4. Методологія дослідження.....	4
1.5. Визначення ключових понять.....	4
2. Електронна комерція як середовище для порушень прав ІВ.....	6
2.1. Роль інтернет-платформ у сучасній торгівлі.....	6
2.2. Особливості порушень прав ІВ в онлайн-середовищі.....	7
2.3. Види платформ і каналів розповсюдження.....	8
3. Основні механізми зловживання платформами.....	9
3.1. Торгівля підробками через електронну комерцію.....	9
3.2. Зловживання системами доставки.....	11
3.3. Відновлення акаунтів і шахрайські мережі.....	12
3.4. Використання Telegram і соціальних мереж.....	14
3.5. Маскування товарів і дублювання контенту.....	15
4. Види ризиків і наслідки порушень.....	17
4.1. Економічні наслідки для правовласників і держави.....	17
4.2. Ризики для здоров'я і безпеки споживачів.....	18
4.3. Підрив довіри до електронної комерції.....	19
4.4. Соціальні та культурні наслідки.....	20
5. Реакція інституцій та платформ.....	21
5.1. Міжнародна практика протидії порушенням ІВ.....	22
5.2. Національне законодавство України.....	25
5.3. Політики платформ щодо захисту прав ІВ.....	30
5.4. Приклади позитивної практики.....	32
6. Інструменти захисту прав ІВ.....	33
6.1. Адміністративні інструменти на платформах.....	34
6.2. Судовий та позасудовий захист.....	34
6.3. Співпраця з митними та правоохоронними органами.....	36
6.4. Онлайн-медіація як сучасний інструмент захисту прав ІВ.....	36
6.5. Технологічні рішення та автоматизація.....	41
6.6. Інформування, просвіта та профілактика.....	45
7. Висновки та рекомендації.....	45
7.1. Підсумки дослідження.....	45
7.2. Рекомендації для онлайн-платформ.....	46
7.3. Рекомендації для державних органів.....	47
7.4. Рекомендації для правовласників та бізнесу.....	47

1. Вступ

1.1. Актуальність проблеми

Онлайн-платформи та маркетплейси є важливою складовою сучасної міжнародної торгівлі, оскільки забезпечують широку доступність товарів і послуг та сприяють спрощенню транскордонних торговельних операцій. Водночас зазначені платформи дедалі частіше використовуються для розповсюдження контрафактної продукції, незаконного використання торговельних марок, а також порушення авторських і суміжних прав, що створює суттєві ризики для правовласників, споживачів та економічних інтересів держав.

Порушення прав інтелектуальної власності (ІВ) в Інтернеті спричиняє як безпосередні економічні збитки для компаній, так і ширші соціальні наслідки. Цифри підтверджують, що онлайн-платформи є основним каналом збуту контрафактної продукції, завдяки своїй доступності, масштабності та відносній анонімності для продавців. У звіті Entrupy "State of the Fake 2024"¹ зазначено, що серед перевірених товарів у сфері моди частка виявлених підробок становила 8,4%, при цьому найчастіше фальсифікуються продукція таких брендів, як Louis Vuitton і Prada. Entrupy — це міжнародна компанія, що спеціалізується на розробці технологій для автентифікації товарів за допомогою штучного інтелекту та комп'ютерного зору. Дані, представлені у звіті, базуються на результатах фактичних перевірок фізичних товарів на вторинному ринку та в онлайн-продажах, що дозволяє вважати їх практичним і релевантним індикатором масштабів проблеми.

В Україні ця проблема особливо актуальна через активне зростання електронної комерції на внутрішньому та міжнародному ринках. Багато споживачів, зокрема з початком повномасштабної війни, переключилися на онлайн-формати, а дистрибуція стала основним каналом реалізації товарів. Наявність контрафактної продукції на цих платформах ставить під сумнів ефективність саморегулювання і викликає запит на посилення державного та міжнародного контролю.

1.2. Мета та завдання дослідження

Метою дослідження є комплексний аналіз сучасних викликів, пов'язаних із порушенням прав інтелектуальної власності в онлайн-середовищі, а також вивчення ефективності наявних механізмів правового захисту на українському та міжнародному рівнях.

Завдання дослідження:

- визначити характерні особливості та масштаби порушень прав ІВ в електронній комерції;
- проаналізувати найпоширеніші схеми зловживань інтернет-платформами;
- дослідити наявні політики платформ і їхню ефективність;

¹ Entrupy. State of the Fake 2024 [Електронний ресурс]. – Режим доступу: <https://www.entrupy.com/report/state-of-the-fake-report-2024/>

- вивчити національну та міжнародну правову базу протидії;
- надати оцінку загрозам для держави, бізнесу та споживачів;
- сформулювати комплексні рекомендації.

1.3. Об'єкт і предмет дослідження

Об'єктом дослідження виступає електронна комерція як середовище для порушення прав інтелектуальної власності, а також діяльність онлайн-платформ у цій сфері.

Предметом дослідження є механізми, форми та масштаби порушення прав ІВ, інституційні, правові та технологічні інструменти реагування, а також регуляторні підходи до протидії в національному та міжнародному контексті. Дослідження також включає аналіз судової практики, адміністративних процедур, політик модерації контенту, використання ШІ та інших цифрових рішень для моніторингу порушень.

1.4. Методологія дослідження

Використано правовий аналіз, контент-аналіз політик платформ, аналіз кейсів, статистичні дані, порівняльно-правовий аналіз.

1.5. Визначення ключових понять

Електронна комерція (e-commerce) – сукупність комерційних процесів, що здійснюються в цифровому середовищі, зокрема через Інтернет. Включає продаж товарів і послуг, обробку платежів, укладання договорів і обмін інформацією.

Онлайн-платформа – будь-який цифровий ресурс, який забезпечує взаємодію продавців і покупців. Це можуть бути маркетплейси, соціальні мережі, месенджери, спеціалізовані сайти.

Маркетплейс – онлайн-платформа, яка агрегує пропозиції від багатьох незалежних продавців і дозволяє здійснювати продаж і купівлю товарів чи послуг через єдиний інтерфейс.

Інтернет-магазин – окремий веб-сайт, створений одним продавцем для реалізації своїх товарів чи послуг онлайн. Інтернет-магазини можуть функціонувати незалежно або бути частиною маркетплейсу.

Контрафактні товари – а) товари, що є предметами порушення прав інтелектуальної власності на торговельну марку в Україні, на яких без дозволу міститься позначення, тотожне із охоронюваною в Україні торговельною маркою стосовно одного й того самого виду товарів, або яке є схожим настільки, що його можна сплутати торговельною маркою; б) товари, що є предметами порушення прав інтелектуальної власності на географічне зазначення в Україні й містять назву чи термін або описуються за допомогою назви чи терміна, які захищені таким географічним зазначенням; в) будь-яка упаковка, етикетка, наліпка, брошура, інструкція з експлуатації, гарантія чи інший документ такого типу, навіть якщо вони представлені окремо, які є предметами

порушення інтелектуальної власності на торговельну марку або географічне зазначення, які містять позначення, назву або термін, тотожні із охоронюваною в торговельною маркою чи географічним зазначенням, або які є схожими настільки, що їх можна сплутати з такою торговельною маркою чи зазначенням, використовуватися географічним та які стосовно одного й того самого виду товарів, щодо якого охороняється торговельна марка в Україні чи географічне зазначення.

Фальсифікована продукція – продукція, виготовлена з порушенням технології або неправомірним використанням знака для товарів та послуг, чи копіюванням форми, упаковки, зовнішнього оформлення, а так само неправомірним відтворенням товару іншої особи.

Верифікація продавця – процедура підтвердження достовірності інформації про продавця, яка може включати перевірку документів, ідентифікацію особи, підтвердження контактних даних.

Послуга проміжного характеру в інформаційній сфері – послуга з передачі та/або зберігання інформації та присвоєння мережевих ідентифікаторів. Якщо послуга надається особою, яка є ініціатором передачі інформації, має змогу впливати на вибір одержувача інформації або може змінювати зміст інформації, що передається, така послуга не є послугою проміжного характеру в інформаційній сфері.

Постачальники послуг проміжного характеру в інформаційній сфері – постачальники електронних комунікаційних послуг, оператори послуг платіжної інфраструктури, реєстратори (адміністратори), що присвоюють мережеві ідентифікатори, та інші суб'єкти, що забезпечують передачу та зберігання інформації з використанням інформаційно-комунікаційних систем.

2. Електронна комерція як середовище для порушень прав ІВ

2.1. Роль інтернет-платформ у сучасній торгівлі

Онлайн-платформи відіграють ключову роль у трансформації глобальної економіки, змінюючи способи продажу, доставки та споживання товарів і послуг. Упродовж останніх десятиліть вони перетворилися не лише на канали дистрибуції, а й на середовище, в якому формується конкурентне середовище, реалізуються маркетингові стратегії, а також, на жаль, відбуваються системні порушення прав інтелектуальної власності.

У межах України активно функціонують кілька великих електронних платформ, які охоплюють сегменти маркетплейсів, онлайн-каталогів, платформ оголошень і нішевих онлайн-магазинів. Ці платформи відрізняються за моделлю роботи (B2C, C2C, B2B), типом продавців, ступенем модерації контенту та політиками ідентифікації продавців. Ці онлайн-ресурси охоплюють різні сегменти ринку – від універсальних маркетплейсів до нішевих платформ та сервісів оголошень. За загальними оцінками, найбільші платформи в Україні у 2023 році мали сукупно понад 60 мільйонів відвідувань на місяць, що свідчить про надзвичайно високий рівень цифрової комерційної активності в країні.

Онлайн-платформи забезпечують низку переваг:

- зручність і швидкість придбання товару;
- доступ до широкого асортименту продукції;
- порівняння цін та можливість читати відгуки;
- спрощення доступу малих підприємців до ринку;
- розвиток дропшипінгу та доставки у віддалені регіони (платформи часто інтегровані з логістичними операторами, що дозволяє здійснювати доставку навіть у віддалені регіони без складської інфраструктури з боку продавця).

Однак ці ж характеристики створюють умови для активного поширення контрафактної продукції. За результатами звіту EUIPO «Intellectual Property Crime Threat Assessment» (2022)², понад 70% фальсифікованої косметики та парфумерії, які потрапляють до споживачів, поширюються через онлайн-платформи. В Україні ця тенденція посилюється через обмежений контроль за продавцями, відсутність жорстких вимог до підтвердження походження товарів і недостатню прозорість процедур модерації.

Окрему роль відіграє динаміка участі малих продавців. У багатьох випадках акаунти продавців на платформах реєструються від імені фізичних осіб-підприємців із мінімальним пакетом верифікації. Це створює прогалини у механізмах ідентифікації правопорушників та ускладнює притягнення їх до відповідальності, оскільки акаунти часто реєструються без належної перевірки та можуть бути легко замінені після

² EUIPO, Intellectual Property Crime Threat Assessment, 2022 [Електронний ресурс]. – Режим доступу: <https://www.euipo.europa.eu/en/publications/ip-crime-threat-assessment-2022>

блокування. Це дає змогу недобросовісним продавцям обходити відповідальність, змінювати акаунти після блокування й повторно завантажувати товари, що порушують права ІВ.

Крім того, велика кількість «незалежних» сайтів, створених на основі універсальних конструкторів онлайн-магазинів, часто використовується як дублюючі дзеркала маркетплейсів або як приховані майданчики для продажу контрафакту з уникненням модерації.

У зв'язку зі стрімкою цифровізацією торгівлі, розвитком маркетплейсів та зростанням обсягів транзакцій в електронному середовищі, спостерігається посилення глобальної тенденції до зростання порушень прав інтелектуальної власності саме в онлайн-сегменті. Основні канали розповсюдження контрафактної продукції дедалі частіше зміщуються в цифровий простір — зокрема на маркетплейси, платформи електронної комерції та соціальні мережі. У більшості випадків порушення прав ІВ фіксуються саме на платформах, які не мають дієвого механізму попереднього контролю за контентом або верифікації продавців, що створює прогалини у системі онлайн-захисту.

Таким чином, онлайн-платформи є не лише важливим інструментом розвитку електронної торгівлі, але й високоризиковим середовищем з точки зору охорони прав інтелектуальної власності. Їхня роль у динаміці порушень ІВ потребує особливої уваги як з боку держави, так і з боку самих платформ через необхідність впровадження механізмів превентивного контролю, прозорості продавців і тісної співпраці з правовласниками, а також порівняльного аналізу з міжнародною практикою щодо політик платформ у сфері захисту прав інтелектуальної власності. Наприклад, великі міжнародні гравці, такі як Amazon чи Alibaba, вже кілька років впроваджують програми з верифікації продавців (Brand Registry, IP Protection Platform), а також алгоритми машинного навчання для автоматичного виявлення потенційно підробленого контенту.

У Європейському Союзі, згідно з Регламентом Digital Services Act (DSA)³, встановлюються нові зобов'язання для великих платформ щодо прозорості, звітності та оперативного реагування на порушення. Подібні ініціативи можуть бути використані як орієнтир для українського ринку.

2.2. Особливості порушень прав ІВ в онлайн-середовищі

Порушення прав інтелектуальної власності в електронній комерції мають низку характерних рис, що відрізняють їх від офлайн-порушень та значно ускладнюють виявлення і реагування. Передусім, йдеться про високий рівень анонімності продавців. Багато з них діють під вигаданими іменами, не надаючи підтвердження особи чи юридичного статусу, що унеможливорює або значно ускладнює їх ідентифікацію у випадку порушення прав ІВ.

³ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [Електронний ресурс]. – Режим доступу: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>

Ще однією характерною ознакою є використання фіктивних акаунтів або масова реєстрація акаунтів з метою швидкого відновлення діяльності після блокування. порушники часто використовують цілі мережі акаунтів, де одні відповідають за розміщення товарів, інші — за фінансові операції, а ще інші — за логістику та спілкування з клієнтами.

Поширеною практикою є маскування під справжні бренди. Це здійснюється через візуальну імітацію оригінальних товарів — використання фірмових логотипів, кольорової гами, пакування, стилістики фотографій. Часто на фото зображуються справжні брендові речі, а покупцеві фактично доставляється підробка. У ряді випадків порушники свідомо змінюють найменування брендів або допускають орфографічні помилки, щоб обійти автоматичні фільтри.

Також поширене використання соціальних мереж і месенджерів (зокрема, Telegram) для обміну посиланнями, QR-кодами, завершення угод і обходу політик платформи. У деяких випадках справжній продаж відбувається не на маркетплейсі, а через канал або чат, який маскується під консультацію чи акцію.

Порушники нерідко використовують схеми, що дозволяють уникати митного контролю. Це включає дрібні партії товару, декларування як особистих посилок, розділення упаковки, інструкцій та самого товару з подальшим збиранням на локальному рівні.

Окремої уваги заслуговує дублювання контенту — розміщення ідентичних оголошень на кількох платформах під різними обліковими записами. Це дозволяє зменшити ризики втрати аудиторії у разі блокування окремого акаунту та забезпечити постійну присутність у видачі пошукових систем. Більш того, продавці використовують SEO-оптимізований опис товару, що ускладнює виявлення порушення навіть технічними засобами.

Таким чином, порушення прав інтелектуальної власності в онлайн-середовищі відзначаються постійною мінливістю, значною технічною складністю та здатністю швидко адаптуватися до нових умов, що суттєво ускладнює протидію таким явищам.

Ефективна протидія таким порушенням потребує системного підходу, що включає модернізоване законодавство, міжплатформену співпрацю, впровадження автоматизованих механізмів моніторингу та активну участь правовласників у захисті своїх прав.

2.3. Види платформ і каналів розповсюдження

Сфера електронної комерції в Україні та світі охоплює широкий спектр цифрових майданчиків, що відрізняються за форматом, цільовою аудиторією та рівнем модерації. Порушення прав інтелектуальної власності трапляються не лише на універсальних маркетплейсах, а й у нішевих інтернет-магазинах, соціальних мережах, месенджерах і навіть на спеціалізованих форумах.

Умовно канали розповсюдження контрафактної продукції в онлайні можна класифікувати за такими категоріями:

Централізовані маркетплейси. Це великі онлайн-платформи, що агрегують пропозиції від багатьох продавців. Хоча більшість таких платформ впроваджує певні інструменти контролю, через обсяг пропозицій та складність ідентифікації порушень, вони залишаються вразливими до контрафакту.

Інтернет магазини. Це окремі веб-сайти, що можуть бути створені швидко на основі шаблонних конструкторів. Вони нерідко використовуються як дублюючі або резервні точки продажу після блокування на великих платформах.

Платформи оголошень і соціальні мережі. Розміщення контенту, що порушує права ІВ, часто відбувається у вигляді приватних оголошень, «акцій» або постів з коментарями. Соціальні мережі використовуються як інструмент первинного контакту або перенаправлення покупця на інший ресурс.

Месенджери (Telegram, Viber тощо). Через анонімність і шифрування повідомлень месенджери стали зручним інструментом для завершення угод, інструктажу щодо оплати та доставки. Вони також використовуються для створення закритих груп, де розповсюджується контрафактний товар.

Платформи, що здійснюють діяльність на території України, але зареєстровані за кордоном. Платформи, які діють поза межами української юрисдикції, становлять особливу складність для реагування на порушення. Через це правовласники часто не мають оперативного доступу до механізмів видалення контрафактного контенту або отримання інформації про порушників.

Кожен із каналів має свої технічні та правові особливості, які впливають на швидкість поширення порушень, складність їх виявлення та ефективність реагування. Важливо розуміти, що зловмисники часто комбінують кілька каналів: наприклад, реклама розміщується в соцмережі, контакт — через месенджер, а продаж завершується на незалежному сайті. Це ускладнює виявлення цілісного ланцюга порушення та вимагає міжплатформеного аналізу.

3. Основні механізми зловживання платформами

3.1. Торгівля підробками через електронну комерцію

Торгівля підробками через електронну комерцію залишається одним із наймасштабніших і найбільш загрозливих каналів порушення прав інтелектуальної власності у світі. За даними спільного звіту OECD та EUIPO "Mapping Global Trade in Fakes 2025"⁴, обсяг незаконної торгівлі контрафактними товарами у 2021 році склав близько 467 млрд доларів США, що становить орієнтовно 2,3% світового імпорту. У

⁴ OECD/EUIPO. Mapping Global Trade in Fakes 2025: Global Trends and Enforcement Challenges [Електронний ресурс]. – Режим доступу: https://www.oecd.org/en/publications/mapping-global-trade-in-fakes-2025_94d3b29f-en/full-report.html

Європейському Союзу цей показник є ще вищим — частка підробленої продукції серед загального обсягу імпорту досягла 4,7%.

Онлайн-продажі контрафактної продукції створюють значні ризики для споживачів, завдають економічних збитків правовласникам і негативно впливають на розвиток чесної конкуренції на цифрових ринках. Сучасні зловмисники активно використовують онлайн-механізми для маскуванню товарів, створення підставних акаунтів і швидкого відновлення заблокованих оголошень, що суттєво ускладнює боротьбу з порушеннями.

У світі електронної комерції також розповсюджені випадки використання сторонніх платформ для дублювання пропозицій. Наприклад, деякі зловмисники створюють незалежні інтернет-магазини через платформи типу Shopify, WooCommerce або Wix, де продають товари, які виглядають як оригінальні, але насправді є підробками. Ці ресурси часто використовуються для повторного запуску підробленого контенту після видалення з основної платформи.

Відповідь на зростаючі виклики, великі міжнародні платформи впроваджують спеціалізовані програми: Amazon Brand Registry⁵, eBay VeRO⁶, Alibaba IP Protection Platform⁷. Ці механізми включають автоматичне виявлення контрафакту, блокування підозрілих оголошень, створення «чорних списків» продавців, а також активну співпрацю з правовласниками.

В Україні наразі відсутні обов'язкові державні вимоги до платформ щодо верифікації продавців. Водночас, відповідно до статті 7 Закону України «Про електронну комерцію», продавці зобов'язані надавати споживачам повну та достовірну контактну інформацію. Однак, вказівка даних та їх верифікація — це різні процеси. Закон зобов'язує продавця надати дані, але не вимагає від платформи обов'язково перевіряти їхню автентичність. Таким чином, платформи можуть технічно приймати інформацію без її фактичної перевірки, що створює прогалини у контролі та може бути використано недобросовісними продавцями.

Проте варто відзначити, що окремі ініціативи демонструють позитивну практику — зокрема, розробку політик модерації контенту та впровадження елементів саморегулювання на рівні окремих платформ.

Загалом, ситуація із продажем підробок в онлайн-середовищі вимагає посиленого комплексного підходу, що включатиме зобов'язання платформ щодо прозорості, верифікації, співпраці з правовласниками та оперативного реагування на скарги. Орієнтиром для національної практики може слугувати Регламент Digital Services Act (DSA), який вимагає від великих платформ забезпечення належного рівня контентної модерації, алгоритмічної прозорості та швидкого реагування на незаконний контент.

⁵ Amazon. Amazon Brand Registry [Електронний ресурс]. – Режим доступу: <https://sell.amazon.com/brand-registry>

⁶ eBay. Verified Rights Owner (VeRO) Program [Електронний ресурс]. – Режим доступу: <https://www.ebay.com/sellercenter/resources/verified-rights-owner-profiles>

⁷ Alibaba. Alibaba Intellectual Property Protection Platform [Електронний ресурс]. – Режим доступу: https://ipp.aidcgroup.net/index.htm?language=en_US#/ippHome

Рекомендації:

- Запровадження обов'язкових механізмів верифікації продавців на українських маркетплейсах.
- Розробка платформа-орієнтованих політик боротьби з підробками за прикладом Amazon, eBay, Alibaba.
- Створення національного реєстру заблокованих акаунтів за порушення ІВ.
- Розробка цифрової інфраструктури скарг і автоматизованого реагування на підозрілий контент.

3.2. Зловживання системами доставки

Одним із недостатньо врегульованих напрямів є використання систем доставки для маскуванню походження товарів, які порушують права інтелектуальної власності. Сучасні сервіси доставки дозволяють фізичним особам і невеликим компаніям відправляти товари без прямої ідентифікації одержувача або відправника, що ускладнює виявлення та документування фактів порушення прав ІВ.

Деякі платформи пропонують інтеграцію з поштовими й кур'єрськими службами, що дозволяє автоматично створювати накладні без перевірки змісту відправлень. У випадках, коли контрафактні товари доставляються у «поштомат», фактична ідентифікація покупця або отримувача може бути ускладнена, особливо якщо вона здійснюється через тимчасові або неавтентифіковані акаунти.

Злочинці також користуються перевагами міжнародної доставки, зокрема послугами транзитних складів, які перепаковують товари та надсилають їх із іншої країни під виглядом нових, аби уникнути ідентифікації або оподаткування. Водночас брак злагодженої взаємодії між платформами, логістичними компаніями й митними органами створює прогалини у відстеженні переміщення підробок.

Приклад із практики України:

У березні 2023 року Бюро економічної безпеки України (БЕБ) викрило масштабну схему постачання компонентів і виготовлення підробленої парфумерної продукції в Одеській області⁸.

Товари реалізовувалися через онлайн-канали, зокрема сайти, соціальні мережі та месенджери, а доставка здійснювалася через поштові оператори без належного контролю. Вилучено продукції на загальну суму понад 9,2 млн грн та виявлені канали поставки компонентів для виробництва.

У ході додаткових обшуків у магазині, де реалізовувались парфуми, та у складських приміщеннях передмістя Одеси, детективи знайшли близько 4 тисяч ящиків з

⁸ Бюро економічної безпеки України. БЕБ на Одещині викрило схему поставки з-за кордону компонентів для виготовлення підробленої парфумерії [Електронний ресурс]. – Режим доступу: <https://esbu.gov.ua/news/beb-na-odeshchyni-vykrylo-skhemu-postavky-z-za-kordonu-komponentiv-dlia-vyrobnnytstva-pidroblenoi-parfumerii>

флаконами, дозаторами, розпилювачами для виготовлення підробленої продукції на суму понад 8 млн грн.

Також детективи БЕБ провели обшук митного посту «Південний порт» та виявили майже 140 тис. пляшок для розливної парфумерії на загальну суму понад 1,2 млн грн.

Встановлено, що пляшки з безбарвного скла в асортименті доставлені в Україну з Польщі. Одержувач товару – підприємство, що належить власнику бізнесу з виготовлення контрафактної парфумерної продукції.

Цей кейс ілюструє, як використання анонімних каналів доставки дозволяє порушникам масштабувати незаконну діяльність та уникати відповідальності. На практиці зловмисники можуть легко повторно організувати логістику після блокування одного з каналів – особливо коли контроль на етапі доставки обмежений.

Прикладом міжнародного підходу до вирішення цього питання є ініціативи Всесвітньої митної організації (WCO) та впровадження систем попереднього електронного декларування товарів, а також автоматизованих систем ризик-менеджменту для виявлення сумнівних відправлень.

Рекомендації:

- Розробка вимог до інтеграції платформ із службами доставки щодо передачі інформації про відправника й товар.
- Впровадження обов'язкової верифікації одержувачів при отриманні товарів з ознаками порушення ІВ.
- Посилення контролю з боку митних органів за транзитними поставками із підвищеним ризиком контрафакту.
- Налагодження обміну інформацією між логістичними операторами, платформами та державними органами.

3.3. Відновлення акаунтів і шахрайські мережі

Одним із найбільш поширених способів уникнення відповідальності на онлайн-платформах є системне відновлення заблокованих акаунтів та використання шахрайських мереж. Зловмисники, які поширюють контрафакт або інший незаконний контент, створюють численні акаунти, які швидко блокуються модераторами платформ, але потім замінюються новими.

Механізми зловживань:

Мультиаккаунтинг: Створення великої кількості акаунтів на одній або кількох платформах, які використовуються паралельно або по черзі для розповсюдження забороненого контенту.

Використання фейкових або підставних даних: Для реєстрації акаунтів застосовують підроблені документи, віртуальні номери телефонів, проксі-сервери та VPN для приховування геолокації.

Шахрайські мережі: Координація груп з кількох осіб, які займаються створенням, керуванням та захистом таких акаунтів, часто надають послуги з обходу блокувань іншим порушникам.

Відновлення акаунтів: Використання технічних і юридичних лазівок для апеляції або повторної активації акаунтів після блокувань, іноді з подачею фальшивих скарг на законних користувачів для відволікання модераторів. Людина порушує правила — її акаунт блокують. Але вона звертається до служби підтримки з апеляцією, щоб повернути акаунт. Через політику платформ, яка передбачає право на апеляцію, акаунти іноді відновлюють навіть порушникам.

Причини, чому це відбувається повторно:

- Платформи гарантують захист від необґрунтованих блокувань, тому надають користувачам право апеляції.
- Модератори не завжди можуть швидко й точно перевірити кожну скаргу через великий обсяг акаунтів і запитів.
- Визначити навмисне порушення часто складно, особливо при автоматизованому моделюванні.

Через це порушники можуть повертатися знову і знову, що суттєво ускладнює боротьбу з ними.

Український контекст:

В Україні ці практики набули широкого поширення на великих маркетплейсах, онлайн-магазинах і платформах оголошень. Відсутність єдиної централізованої бази заблокованих акаунтів ускладнює їхню ідентифікацію та доведення системності порушень. Деякі порушники організовують мережі з десятків чи сотень акаунтів, що дозволяє швидко відновити присутність після видалення.

В Україні рекомендується впроваджувати світові практики моніторингу та контролю акаунтів, зокрема автоматизовані системи виявлення порушень, що вже застосовуються на провідних міжнародних платформах.

Міжнародна практика:

Крупні міжнародні маркетплейси (Amazon, eBay, AliExpress) використовують системи централізованого моніторингу акаунтів і співпрацюють із правоохоронними органами через програми Brand Protection і IP Enforcement. Вони впроваджують багатофакторну аутентифікацію, вимоги до верифікації продавців та блокування за IP-адресами.

Європейський Регламент DSA зобов'язує платформи надавати прозору звітність щодо видалення акаунтів і заохочує міжплатформений обмін інформацією про порушників.

Рекомендації:

- Створити централізовану базу даних заблокованих акаунтів із доступом для платформ і правоохоронних органів.
- Запровадити обов'язкову двофакторну аутентифікацію та жорсткіші вимоги до верифікації продавців.
- Впроваджувати інструменти автоматизованого аналізу поведінки користувачів для виявлення аномалій.
- Проводити навчальні кампанії для користувачів щодо ризиків шахрайства і методів захисту.

3.4. Використання Telegram і соціальних мереж

У сучасному цифровому середовищі Telegram є глобальною проблемною платформою, яку активно використовують продавці контрафактної продукції та інші порушники прав інтелектуальної власності для обходу фільтрів і модерації на офіційних маркетплейсах і в соціальних мережах. Завдяки відносній анонімності і високій швидкості поширення інформації, Telegram дозволяє ефективно організовувати продажі поза межами контролю платформ.

Основні механізми:

Посилання та QR-коди

Покупцям часто надсилають прямі посилання або QR-коди, які перенаправляють їх на альтернативні «дзеркала» офіційних сайтів або на спеціально створені акаунти, де можливо безперешкодно завершити покупку. Ці дзеркала дозволяють зберігати функціональність сайту, водночас уникаючи санкцій і блокувань, які застосовуються основними платформами.

Прихований маркетинг у соцмережах

Використання сторіз із посиланнями на зовнішні ресурси, коментарі під популярними публікаціями, а також розміщення псевдооглядів і «рекомендацій» — це поширені практики прихованої реклами. Вони створюють ілюзію органічного інтересу, що ускладнює виявлення і блокування незаконної реклами.

Загрози та виклики:

Відсутність прямого контролю: Telegram як месенджер не регулюється так жорстко, як офіційні маркетплейси, і має складну архітектуру для моніторингу, що дозволяє каналам працювати з високим рівнем анонімності.

Технічна складність блокування: регулярна зміна назв каналів, використання нових посилань і QR-кодів ускладнюють роботу правоохоронців та платформ.

Поширення дезінформації: псевдоогляди й коментарі можуть вводити споживачів в оману, підвищуючи ризики купівлі неякісної чи небезпечної продукції.

Рекомендації:

- Розробка спеціалізованих інструментів моніторингу Telegram-каналів із застосуванням штучного інтелекту та аналітики тексту для виявлення незаконних оголошень і посилань.
- Співпраця правоохоронних органів із адміністраторами месенджерів для оперативного блокування каналів, що порушують права ІВ.
- Інформаційні кампанії серед споживачів щодо ризиків купівлі товарів поза офіційними каналами.
- Міжнародна координація у боротьбі з транскордонною торгівлею контрафактом через месенджери.

3.5. Маскування товарів і дублювання контенту

Порушники прав інтелектуальної власності все частіше використовують складні техніки маскування товарів і дублювання контенту, щоб обійти системи модерації маркетплейсів і соціальних платформ. Ці методи значно ускладнюють ідентифікацію та припинення нелегальної діяльності.

Основні форми маскування і дублювання:

Маскування товарів

Зміна описів і ключових слів. Порушники використовують синоніми, помилки, спеціальні символи або коди замість прямих назв брендів і товарів, щоб уникнути пошукових алгоритмів та фільтрів. Аналітичні дані OECD/EUIPO вказують, що значна частина товарів, які зловживають онлайн-фільтрами, використовують змінені описи та фото для маскування. Це ускладнює автоматичне виявлення контрафакту.

Візуальне дублювання з варіаціями. Дублювання зображень із незначними змінами: кадрування, накладання водяних знаків, зміна фону або кольору, що допомагає уникнути виявлення через системи розпізнавання зображень (computer vision).

Розпізнавання зображень (computer vision) — це технологія штучного інтелекту, яка дозволяє комп'ютерам «бачити» і аналізувати візуальну інформацію, таку як фотографії чи відео. А саме, це здатність комп'ютера розпізнавати об'єкти, текст, кольори, форми і навіть складніші патерни на зображеннях — так, як це робить людина, але автоматично і швидко. У контексті маркетплейсів і захисту прав інтелектуальної власності:

- Технології розпізнавання зображень допомагають платформам автоматично виявляти копії фотографій товарів (наприклад, підробки), навіть якщо зображення трохи змінені (обрізані, змінений фон тощо).
- Це дозволяє ефективніше блокувати незаконний контент, який порушує авторські права або права на торговельні марки. Наприклад, якщо порушник завантажує фото оригінального бренду з незначними змінами, система розпізнає схожість і позначає оголошення для перевірки.

Ця технологія широко застосовується у великих міжнародних маркетплейсах (Amazon, eBay) і соцмережах для боротьби з контрафактом.

Дублювання контенту

Створення «дзеркальних» сайтів і акаунтів. порушники створюють копії офіційних сайтів та акаунтів на інших доменах або платформах із мінімальними відмінностями в назві чи оформленні. Це дозволяє їм швидко відновлювати продаж після блокування основних ресурсів.

Використання автоматизованих ботів для масового дублювання. Автоматизовані системи генерують тисячі варіантів оголошень із незначними змінами, що унеможлиблює їх швидке видалення.

Використання різних платформ і каналів. Після блокування на маркетплейсі порушники активно переміщують контент у соціальні мережі, месенджери або на спеціально створені телеграм-канали, де дублюють оголошення із прихованими посиланнями та QR-кодами

У Європейському Союзі Digital Services Act (DSA) встановлює нові обов'язки для онлайн-платформ, зокрема маркетплейсів. Платформи зобов'язані впроваджувати сучасні технології для виявлення та боротьби з дублюванням і маскуванню контенту, а також регулярно проводити випадкові перевірки товарів і звітувати про ефективність заходів із забезпечення безпечного цифрового середовища. Крім того, DSA передбачає оперативне реагування на повідомлення про порушення та обов'язок забезпечувати прозорість алгоритмів модерації й видалення контенту.

Ці вимоги особливо актуальні для боротьби з маскуванню контрафактних товарів, коли продавці навмисно змінюють описи, зображення або ключові слова, щоб уникнути виявлення.

На форумах продавців Amazon (зокрема Reddit) неодноразово повідомлялося про ситуації, коли облікові записи блокувалися після скарг на порушення прав інтелектуальної власності, а продавці оперативно створювали нові акаунти — інколи протягом 24 годин. Після створення нових облікових записів вони дублювали попередні оголошення, використовуючи мінімально змінені фото і нові, навмисно модифіковані описи товарів. Такі дії дозволяють тимчасово обійти автоматичні алгоритми виявлення і продовжувати продаж, хоча це суперечить правилам платформи.

Подібні схеми спостерігаються і в Україні, зокрема на локальних маркетплейсах. Контрафактні товари часто повторно з'являються після блокування — під зміненими назвами, у інших товарних категоріях або на новостворених облікових записах. Іноді продавці свідомо надають оманливу або неповну інформацію про товар для приховування його походження.

Такі практики вимагають посилення верифікації продавців, впровадження механізмів виявлення пов'язаних акаунтів, моніторингу дубльованого контенту та системного контролю з боку платформ.

У міжнародній практиці окремі платформи вже впровадили комплексні технічні рішення для виявлення пов'язаних облікових записів із метою запобігання дублюванню контенту та обходу обмежень після блокування.

Зокрема, Amazon та eBay активно використовують багаторівневі алгоритми для аналізу IP-адрес, платіжних реквізитів, контактної інформації, пристроїв доступу та поведінкових ознак користувачів. Такі системи дозволяють виявляти технічні й фінансові зв'язки між акаунтами та оперативно реагувати на спроби відновлення діяльності після блокування.

Застосування подібних механізмів уможливлює більш ефективну протидію повторному розміщенню контрафактного контенту, у тому числі у випадках, коли порушники намагаються дублювати оголошення з мінімально зміненими даними або створювати нові облікові записи для продовження продажів.

Впровадження подібних комплексних алгоритмів на українських маркетплейсах є доцільним кроком для підвищення ефективності захисту прав інтелектуальної власності та мінімізації ризиків зловживань з боку недобросовісних продавців.

4. Види ризиків і наслідки порушень

У сучасному глобалізованому світі стрімке зростання електронної комерції та міжнародної торгівлі створило як значні можливості для економічного розвитку, так і серйозні виклики в сфері захисту прав інтелектуальної власності. Незважаючи на те, що розширення глобальних ланцюгів постачання сприяє інноваціям і ефективності, воно також стало каналом для поширення контрафактної продукції, що завдає шкоди правовласникам, державам, споживачам та суспільству в цілому.

Незаконна торгівля контрафактними товарами підриває верховенство права, завдає серйозної шкоди економіці, створює ризики для здоров'я споживачів, шкодить довірі до цифрових каналів торгівлі та навіть сприяє розвитку організованої злочинності. Зловживання онлайн-платформами та зонами вільної торгівлі лише посилює ці загрози. У цьому розділі буде розглянуто ключові наслідки таких порушень та ризики, що виникають для правовласників, держави, споживачів і суспільства в цілому.

4.1. Економічні наслідки для правовласників і держави

Одним із найпомітніших економічних наслідків порушення прав інтелектуальної власності на онлайн-платформах є втрата доходів і частки ринку для правовласників. Коли компанія стає об'єктом порушення прав ІВ — наприклад, через появу на маркетплейсах контрафактної продукції, що копіює її товари чи послуги, — це безпосередньо впливає на обсяги продажів. Порушники часто реалізують підробки за значно нижчими цінами, не несучи витрат на розробку, контроль якості, маркетинг або

ліцензування. Така недобросовісна конкуренція приваблює частину споживачів і послаблює позиції легального виробника на ринку.

Окрім прямих втрат у доходах, правовласник може поступово втрачати частку ринку на користь суб'єктів, які використовують незаконно привласнені технології, дизайни або бренди. Це особливо критично у високо конкурентних галузях, де швидкість реакції на інновації та захист бренду визначають довгострокову стійкість бізнесу. Компанії, які систематично зазнають порушень прав ІВ, повідомляють про скорочення обсягів продажів, втрату клієнтської бази, а в деяких випадках — навіть про вимушене згортання інвестицій у нові продукти чи вихід з ринку.

У підсумку, втрата доходів і ринкової частки не лише підриває фінансову стабільність конкретної компанії, а й створює викривлення на ринку, де легальні гравці стикаються з конкуренцією з боку тих, хто не дотримується ані законодавчих норм, ані етичних стандартів. Така ситуація є особливо небезпечною в онлайн-середовищі, де порушення можуть поширюватися швидко і масово, а виявлення правопорушника ускладнене через анонімність платформ.

На додаток до безпосередніх втрат для окремих компаній та державних бюджетів, контрафакт і піратство мають ширші соціально-економічні наслідки. Згідно з дослідженнями таких організацій як Організація економічного співробітництва та розвитку (OECD) та Європейського відомства з інтелектуальної власності (EUIPO) порушення прав ІВ негативно впливають на міжнародну торгівлю, обсяги прямих іноземних інвестицій, інноваційну активність, рівень зайнятості, а також сприяють зростанню злочинності та шкодять довкіллю. Хоча кількість комплексних оцінок у цій сфері залишається обмеженою через нестачу порівняльних міждержавних даних, наявні емпіричні дослідження вказують на те, що слабкі режими захисту ІВ стримують економічне зростання та послаблюють інвестиційну привабливість.

4.2. Ризики для здоров'я і безпеки споживачів

Контрафактна продукція, що поширюється через онлайн-платформи, становить серйозну загрозу для здоров'я, безпеки та добробуту споживачів. Виробництво таких товарів зазвичай здійснюється без дотримання базових стандартів якості та безпеки, а отже — поза межами державного регулювання та контролю. Це створює високий ризик потрапляння на ринок товарів, виготовлених із несертифікованих, токсичних або дефектних матеріалів.

Особливо небезпечними є підробки в категоріях лікарських засобів, харчових продуктів і добавок, дитячих іграшок, косметики, електроніки та автозапчастин. За оцінками міжнародних організацій, ці групи товарів не лише регулярно з'являються серед предметів митного вилучення, але й безпосередньо пов'язані з серйозними ризиками для здоров'я людей — від алергічних реакцій до загроз життю. В окремих випадках споживачі навіть можуть не підозрювати, що купують підробку, через її зовнішню схожість із оригінальним продуктом.

У 2023 році звіт Review of Notorious Markets for Counterfeiting and Piracy⁹, підготовлений Office of the United States Trade Representative Executive Office of the President, спеціально присвятив увагу саме впливу контрафактних товарів на здоров'я і безпеку споживачів. У розділі "Issue Focus: The Potential Health and Safety Risks Posed by Counterfeit Goods" детально проаналізовано серйозні ризики, пов'язані з тим, що виробництво підробок зазвичай здійснюється поза регуляторним контролем і вимогами безпеки. Це призводить до появи неякісних, неефективних і часто небезпечних продуктів. Документ виділяє найбільш ризиковані категорії товарів, зокрема: дитячі іграшки, автозапчастини, електроніку, лікарські засоби, косметику, одяг і взуття. Частина з цих майданчиків поєднує легальну й нелегальну діяльність, інші ж — функціонують виключно як платформи поширення контрафакту.

Також у звіті зазначено, що порушники все частіше адаптуються до змін ринку та швидко реагують на попит — наприклад, виготовляють нові партії популярних товарів під виглядом брендових, використовуючи агресивну рекламу, SEO-маніпуляції та рор-уроголошення. З метою уникнення митного виявлення вони часто розділяють доставку упаковки, інструкцій і самого товару, збираючи виріб уже на локальному рівні.

Увагу слід звернути на те, що близько 60 % небезпечної контрафактної продукції постачається саме через міжнародні поштові та кур'єрські служби, здебільшого для реалізації в онлайн-сегменті. При цьому Китай та Гонконг і надалі залишаються основними країнами походження таких товарів. Така ситуація свідчить про високий рівень потенційного ризику для споживачів, оскільки значна частина підробленої продукції поширюється через електронну торгівлю та, як правило, не проходить належних процедур перевірки і контролю, що зумовлено перевантаженням митних органів - згідно зі звітом OECD/EUIPO Dangerous Fakes: Trade in Counterfeit Goods that Pose Health, Safety and Environmental Risks, 2022¹⁰.

Підсумовуючи, споживання контрафактних товарів — це не лише порушення прав ІВ, а й серйозний ризик для життя та здоров'я.

4.3. Підрив довіри до електронної комерції

Онлайн-покупки наразі становлять майже 20% усіх роздрібних витрат, що свідчить про стрімке зростання електронної комерції. Однак це зростання супроводжується одночасним збільшенням кількості контрафактної продукції, що продається онлайн. Цей факт серйозно підриває довіру споживачів до брендів і загалом до електронної комерції.

⁹ Office of the United States Trade Representative. 2023 Review of Notorious Markets for Counterfeiting and Piracy [Електронний ресурс]. – Режим доступу: https://ustr.gov/sites/default/files/2023_Review_of_Notorious_Markets_for_Counterfeiting_and_Piracy_Notorious_Markets_List_final.pdf

¹⁰ OECD/EUIPO. Dangerous Fakes: Trade in Counterfeit Goods that Pose Health, Safety and Environmental Risks, 2022 [Електронний ресурс]. – Режим доступу: https://www.oecd.org/en/publications/dangerous-fakes_117e352b-en/full-report/component-7.html#chapter-d1e2055

За даними Corsearch¹¹ — компанії, що спеціалізується на захисті брендів та наданні відповідних послуг, 46% споживачів у Великій Британії припинили купувати на певному онлайн-майданчику через отримання підроблених товарів, а 44% підтвердили, що перестали купувати певний бренд, оскільки побоювались, що його продукція може бути підробкою. Крім того, 57% тих, кого обдурили, повідомили про наявність підробок на онлайн-майданчику.

Дослідження американської компанії MarkMonitor¹², яка займається розробкою програмного забезпечення для захисту брендів від інтернет-підробок, шахрайства, піратства та кіберсквотингу, підтверджує ці тенденції: 22% покупців, дізнавшись, що придбали підробку, зазначили, що їхнє сприйняття бренду суттєво погіршилося, 26% зовсім припинили купувати товари цього бренду, а 27% попереджають про це родину і друзів. Така втрата довіри може призвести до масштабного падіння лояльності клієнтів і значних репутаційних втрат для брендів.

Ця ситуація становить серйозну загрозу не лише для окремих компаній, а й для всієї електронної комерції, оскільки підробки породжують сумніви у споживачів щодо якості і безпеки товарів, які вони замовляють онлайн. Якщо покупці боятимуться бути ошуканими або купити неякісний товар, це значно стримає розвиток онлайн-ринків і знизить загальний рівень продажів.

Додатково, через поширення підробок знижується довіра до електронних платформ та маркетплейсів, особливо коли останні не здатні ефективно протидіяти незаконній торгівлі. Відсутність належного контролю і прозорості поглиблює сумніви користувачів, а поширення високоякісних “суперпідробок” ускладнює розпізнавання підробок навіть для досвідчених покупців. Для відновлення і підтримки довіри необхідно, щоб власники брендів та онлайн-платформи активно використовували сучасні технології моніторингу і захисту.

Отже, підрив довіри споживачів через поширення підробок — одна з ключових загроз для розвитку електронної комерції, яку необхідно долати системними заходами, поєднуючи технології, законодавство і співпрацю між бізнесом і платформами.

4.4. Соціальні та культурні наслідки

Поширення контрафактної продукції має не лише економічні та безпекові, а й глибокі соціальні та культурні наслідки. Контрафактна продукція підриває соціальні цінності, сприяє поширенню злочинності та негативно впливає на культурне різноманіття.

Один з основних соціальних наслідків — підрив довіри до правової системи та органів державної влади, які, з погляду громадян, не можуть ефективно захистити права споживачів і правовласників. Масовість контрафакту, особливо в електронній комерції, часто створює відчуття безкарності для правопорушників. Це сприяє розширенню

¹¹ Corsearch. UK Consumers Shun Online Marketplaces Due to Counterfeit Goods, 2023 [Електронний ресурс]. – Режим доступу: <https://corsearch.com/content-library/ebooks/counterfeit-products-are-endemic-and-it-is-damaging-brand-value/>

¹² Potter Clarkson. How Does Counterfeiting Impact Online Brand Protection? [Електронний ресурс]. – Режим доступу: <https://www.potterclarkson.com/insights/how-does-counterfeiting-affect-brands/>

тіньової економіки та зміцненню організованої злочинності, яка активно використовує прибутки від незаконної торгівлі для фінансування інших кримінальних дій.

З культурної точки зору, контрафактна продукція знецінює інтелектуальну працю, особливо у сфері креативних індустрій — музики, кінематографу, дизайну, моди, літератури. Втрата доходів і визнання для творців знижує мотивацію до створення нового культурного продукту, ускладнює професійне зростання митців та гальмує розвиток культурної ідентичності. Як підкреслюється у звіті OECD “The Economic Impact of Counterfeiting and Piracy”¹³, у країнах з низьким рівнем захисту прав ІВ зростає культурна залежність від імпорту, тоді як локальні ініціативи залишаються фінансово незахищеними.

Також поширення підробок і піратства формує спотворене уявлення про вартість і цінність оригінального продукту, особливо серед молоді. У разі якщо доступ до нелегального контенту або контрафактної продукції стає нормою, формується толерантність до порушення прав ІВ, що поглиблює розрив між споживачькою поведінкою і етичними стандартами. Це призводить до негативних показників в покурці підробок - згідно з дослідженням Office of the United States Trade Representative Executive Office of the President¹⁴ понад 40% молодих онлайн-споживачів не вважають покупку підробок серйозним порушенням, особливо якщо продукт коштує дешевше або “виглядає як оригінал”.

Крім того, незаконна торгівля контрафактом часто експлуатує вразливі соціальні групи - наприклад, використовує дешеву або дитячу працю в країнах з низьким рівнем правового регулювання. Це не лише поглиблює соціальну нерівність, а й перешкоджає досягненню Цілей сталого розвитку, особливо в контексті гідної праці, економічного зростання, миру та справедливості.

Таким чином, боротьба з контрафактом має не лише правовий та економічний вимір, а й важливий соціокультурний вимір. Системні порушення прав інтелектуальної власності іпідпривають культурну цінність інновацій, демотивують творців, підтримують тіньову економіку і нормалізують неетичну поведінку, особливо у цифровому середовищі.

5. Реакція інституцій та платформ

Цей розділ присвячений дослідженню національного правового регулювання електронної комерції та заходів захисту прав інтелектуальної власності на українських платформах електронної комерції.

Для проведення аналізу застосовано поєднання якісного та кількісного підходів. Основним інструментом став контент-аналіз відкритих джерел, зокрема офіційних сайтів

¹³ OECD. The Economic Impact of Counterfeiting and Piracy [Електронний ресурс]. – Режим доступу: https://www.oecd.org/content/dam/oecd/en/publications/reports/2008/06/the-economic-impact-of-counterfeiting-and-piracy_g1gh906c/9789264045521-en.pdf

¹⁴ Office of the United States Trade Representative. Special 301 Report, 2023 [Електронний ресурс]. – Режим доступу: https://ustr.gov/sites/default/files/2023_Review_of_Notorious_Markets_for_Counterfeiting_and_Piracy_Notorious_Markets_List_final.pdf

25 провідних українських платформ. Було здійснено систематичний перегляд умов користування, розділів про публікацію товарів, контактних форм і документів, що прямо чи опосередковано стосуються прав ІВ. Крім того, аналітика базується на порівняльному аналізі з міжнародними практиками (Amazon, eBay, Alibaba), що дозволяє виявити структурні відмінності та рівень наближеності українських платформ до європейських і глобальних стандартів. Також проаналізовано приклади позитивної практики на українському ринку електронної комерції.

Слід зауважити, що УКРНОІВІ ініціював проведення анонімного опитування серед українських платформ електронної комерції із метою отримання актуальної інформації щодо практик захисту прав інтелектуальної власності. Водночас, у зв'язку з обмеженим рівнем зворотного зв'язку, подальший аналіз було зосереджено на відкритих джерелах.

УКРНОІВІ і надалі залишається відкритим до конструктивного діалогу з представниками ринку електронної комерції, оскільки залучення платформ до таких ініціатив сприяє не лише вдосконаленню державної політики у сфері ІВ, а й підвищенню довіри користувачів, покращенню репутаційних позицій бізнесу та зниженню ризиків правових конфліктів.

5.1. Міжнародна практика протидії порушенням ІВ

Світові онлайн-майданчики напружували цілу систему інструментів для боротьби з контрафактом і піратством. Розглянемо кілька знакових прикладів.

Amazon – один із лідерів у сфері захисту ІВ. На Amazon діє програма Brand Registry, до якої станом на 2023 рік приєдналися вже понад 700 тисяч брендів. Зареєстровані правовласники можуть швидко скажитись на порушення через зручний інтерфейс і навіть отримують доступ до інструменту Project Zero¹⁵, що дозволяє їм самостійно видаляти підроблені лістинги без участі адміністраторів.

Amazon інвестував понад \$1 млрд у системи захисту брендів і задіяв 15 тисяч співробітників для протидії контрафакту. Як наслідок, понад 99% порушень виявляються і блокуються проактивно, ще до того як їх помітять самі бренди. Такого рівня досягли завдяки штучному інтелекту: Amazon перевіряє нових продавців (у 2022 році заблоковано 800 тис. спроб реєстрації підозрілих акаунтів) та аналізує характеристики товарів на відповідність оригіналу.

Крім того, Amazon створив підрозділ Counterfeit Crimes Unit¹⁶, який співпрацює з поліцією і митницею по всьому світу, допомагаючи відстежувати і притягувати до відповідальності виробників і продавців підробок. За 2022 рік Amazon ініціював понад 1300 судових позовів чи передав справ до слідства проти контрафакторів. Така комплексна стратегія (верифікація, AI-моніторинг, інструменти для брендів, юридичний тиск) робить Amazon одним з найбезпечніших майданчиків щодо ІВ. Показово, що

¹⁵ Amazon. Project Zero [Електронний ресурс]. – Режим доступу: <https://sell.amazon.com/brand-registry/project-zero>

¹⁶ Amazon. Counterfeit Crimes Unit [Електронний ресурс]. – Режим доступу: <https://trustworthyshopping.aboutamazon.com/counterfeitcrimesunit>

кількість скарг від брендів на Amazon знижується – на 35% менше у 2022 проти 2021¹⁷, оскільки фейки просто не доходять до покупця.

eBay – піонер інтернет-торгівлі, який ще у 1998 році запустив програму VeRO (Verified Rights Owner)¹⁸ для захисту прав. Програма VeRO дозволяє правовласникам надсилати сповіщення про будь-які лоти, що порушують їхні права, – після отримання такого сповіщення eBay терміново видаляє список і повідомляє продавця. Власники ТМ, авторських прав, патентів можуть зареєструватися в VeRO, отримати підтверджений статус і тоді їхні скарги обробляються дуже швидко (іноді протягом годин).

eBay також веде постійний діалог з найбільшими брендами: створюються “чорні списки” заборонених до продажу предметів (наприклад, певні лімітовані колекції), ключові слова для фільтрації. Сам eBay не настільки проактивний, як Amazon, у сенсі AI-сканування (принаймні відкритих даних менше). Однак у політиках eBay чітко зазначено: “Контрафактні, підроблені або неавтентичні товари заборонені до продажу, і за їх виставлення акаунт може бути заблоковано”. eBay застосовує санкції до повторних порушників: якщо продавець раз за разом порушує (отримує скарги VeRO), його акаунт закривають назавжди.

За останні роки eBay також впровадив програму авторизації: окремі категорії товарів (наприклад, дизайнерські сумки) можуть продавати тільки перевірені продавці. Бренди видають таким продавцям “дозволи”, і eBay допускає їх до списку, а інших ні. Ця практика поступово звужує простір для фейків.

Отже, eBay робить ставку на тісний контакт з правовласниками та жорстку реакцію на скарги – VeRO працює давно і доволі ефективно (за даними eBay, більшість лістингів з порушеннями знімаються протягом 24 годин після скарги, а багато і завчасно).

Alibaba¹⁹ – китайський гігант електронної комерції, що мав історично проблеми з навалюю підробок, але останніми роками докладав значних зусиль для покращення ситуації. Alibaba Group створила комплексну систему IP Protection Platform (IPP): правовласники можуть реєструвати свої права і подавати скарги через єдиний портал на різні платформи групи (Alibaba.com, 1688.com, AliExpress, Taobao тощо). Скарги обробляються досить оперативно – Alibaba заявляє, що 96% заяв видаляють сумнівні лістинги протягом 24 годин.

Також Alibaba впровадила програму “Good Faith Takedown”: якщо бренд має високий рейтинг достовірності скарг, його нові скарги виконуються практично негайно, без детального ручного аналізу. Це спростило життя великим компаніям, які раніше скаржилися на бюрократію в AliExpress. Крім того, Alibaba застосовує технології big data

¹⁷ U.S. Chamber of Commerce. New Amazon Report Shows Dedication to Protecting Brands and Customers [Електронний ресурс]. – Режим доступу: <https://www.uschamber.com/intellectual-property/new-amazon-report-shows-dedication-to-protecting-brands-and-customers#:~:text=Amazon%20recently%20published%20its%20third,platform%20are%20safe%20and%20authentic>

¹⁸ eBay. eBay Verified Rights Owner Program and Intellectual Property Policy [Електронний ресурс]. – Режим доступу: <https://export.ebay.com/en/regulations/ebay-policies/ebay-verified-rights-owner-program-and-intellectual-property-policy/>

¹⁹ WIPO Magazine. Intellectual Property and E-Commerce: Alibaba's Perspective [Електронний ресурс]. – Режим доступу: <https://www.wipo.int/web/wipo-magazine/articles/intellectual-property-and-e-commerce-alibabas-perspective-40514>

та машинного навчання: відстежує аномальні патерни (наприклад, новий продавець раптом виставив 1000 найменувань відомих брендів за низькими цінами – його автоматично перевірять або заблокують).

Ще один крок – Alibaba у 2017 році створила альянс з 30 великими брендами (Intel, Swarovski, Louis Vuitton тощо) для обміну інформацією про тренди контрафакту і спільної протидії. Під тиском цих брендів Alibaba навіть запустила Intellectual Property Joint-Force System, де бренди і платформа разом відстежують підозрілі товари – через пару років ця система отримала схвальні відгуки від учасників.

Також Alibaba працює з китайською поліцією для накриття підпільних фабрик. У 2020 році, за їх звітом, було допомогли вилучити більше 300 млн підроблених товарів на суму ~\$700 млн. Отже, Alibaba рухається від репутації “розсадника фейків” до “прозорого партнерства з брендами”. Хоч повністю проблему ще не вирішено (через масштаб платформи), міжнародна спільнота визнає прогрес Alibaba у захисті ІВ

Інші міжнародні практики

E-commerce платформи всієї Європи і США часто об’єднуються в добровільні ініціативи. Так, діє Меморандум ЄС²⁰ про протидію торгівлі підробками в інтернеті, підписаний такими платформами як Amazon, eBay, Alibaba, Rakuten, Facebook та правовласниками (Nike, Adobe, Philips та ін.) ще у 2016 році. Сторони домовились про спільні підходи: швидкий обмін інформацією про нові види фейків, удосконалення механізмів notice-and-takedown, впровадження “notice-and-stay-down” (щоб видалений контрафакт не з’являвся знову). У новій редакції 2021 року меморандуму додано положення про проактивний моніторинг – великі платформи зобов’язалися використовувати автоматизовані фільтри для виявлення очевидних підробок.

Паралельно деякі соцмережі теж ввели прямі заборони на продаж контрафакту і спростили процедури скарг. Meta (Facebook²¹ і Instagram²²) чітко забороняє продаж контрафакту та активно застосовує заходи для захисту інтелектуальної власності. Платформи забезпечили прості та зрозумілі механізми подання скарг (notice-and-takedown), які дозволяють брендам видаляти контрафактні пости, рекламу та профілі. Meta також застосовує передові технології: машинне навчання, автоматичні фільтри та пошук зображень для виявлення й блокування контрафактного контенту ще до його публікації або реклами.

Etsy²³ (маркетплейс хендмейду) зіткнувся з проблемою продажу підробних товарів “під виглядом вінтажних” і відреагував створенням Trust and Safety команди, яка перевіряє

²⁰ European Commission. Memorandum of Understanding on the Sale of Counterfeit Goods via the Internet (Updated 2021) [Електронний ресурс]. – Режим доступу: <https://ec.europa.eu/docsroom/documents/18023/attachments/1/translations/>

²¹ Meta. Facebook Help Center. Reporting Intellectual Property Violations [Електронний ресурс]. – Режим доступу: <https://www.facebook.com/help/399224883474207>

²² Meta. Instagram Help Center. Intellectual Property Policies [Електронний ресурс]. – Режим доступу: <https://help.instagram.com/intellectualproperty>

²³ Etsy. Etsy Transparency Report 2023 [Електронний ресурс]. – Режим доступу: https://storage.googleapis.com/etsy-extfiles-prod/2023_Transparency_Report.pdf?ref=news

сумнівні лістинги, та ввів обов'язкові підтвердження авторства для продавців власних виробів, щоб уникати порушення авторських прав.

Google²⁴ як платформа інтернет-реклами теж долучається: у Ads діє політика, що забороняє рекламувати сайти, які продають підробки, – за порушення Google блокує рекламний акаунт. Це важливо, бо унеможливорює просування контрафакту через пошукову рекламу.

В підсумку, міжнародна практика демонструє, що комплексний підхід “фільтруй, реагуй, співпрацюй” є найефективнішим. Одні інвестують в технології фільтрації, інші створюють потужні канали співпраці з правовласниками, соціальні мережі інтегрують політики проти фейків у свої стандарти спільноти. Українським платформам є на що орієнтуватися: багато з описаного вже частково впроваджується, а з наближенням до європейського ринку ця тенденція тільки посилиться.

5.2. Національне законодавство України

Нормативно-правова база України у сфері електронної комерції та захисту прав інтелектуальної власності наразі складається з низки актів, основні з яких розглянемо нижче.

Закон України «Про електронну комерцію»²⁵ регулює правові відносини у сфері електронної комерції під час вчинення електронних правочинів, зокрема закладає основи діяльності онлайн-платформ та інших електронних посередників, зокрема продавців, маркетплейсів, платформ оголошень, хостинг-провайдерів та інших посередників.

Онлайн-платформи, залежно від моделі діяльності, можуть мати різний статус:

- якщо вони лише надають технічну можливість для розміщення контенту (оголошень) і не втручаються у процес продажу – вони є постачальниками послуг проміжного характеру в інформаційній сфері,
- якщо ж вони виступають стороною правочину або контролюють процес продажу (наприклад, обробляють замовлення, здійснюють оплату чи доставку), вони також вважаються повноцінними суб'єктами електронної комерції, з усіма відповідними обов'язками перед покупцем.

Для продавців (суб'єктів електронної комерції) Закон у статті 7 передбачає обов'язок надавати споживачам достовірну інформацію про себе: найменування, адресу, контактні дані, реєстраційні та податкові реквізити тощо. Водночас законодавство не передбачає обов'язку платформ здійснювати перевірку достовірності цих даних, що створює прогалини у механізмах попереднього контролю.

²⁴ Google. Google Ads Policy – Counterfeit Goods [Електронний ресурс]. – Режим доступу: <https://support.google.com/adspolicy/answer/176017?hl=en>

²⁵ Закон України «Про електронну комерцію» від 03.09.2015 № 675-VIII [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/675-19#n2>

Закон визначає правовий статус постачальників послуг проміжного характеру в інформаційній сфері (наприклад, хостинг-провайдерів та онлайн-платформ) – і закріплює для них принцип обмеженої відповідальності за порушення у сфері електронної комерції, у тому числі за порушення прав інтелектуальної власності (статті 9, 17 Закону України «Про електронну комерцію»), за умови, що вони не змінюють зміст інформації, не є її ініціаторами і, після отримання достовірного повідомлення про порушення (наприклад, прав ІВ), вживають швидких дій для обмеження доступу до відповідного контенту.

Ключові положення:

1. Постачальники послуг проміжного характеру в інформаційній сфері не є сторонами правочину щодо товарів чи послуг, крім самих інформаційних послуг (доступ до інтернету, реєстрація доменів тощо).
2. Постачальники послуг проміжного характеру в інформаційній сфері не несуть відповідальності за зміст інформації, яку користувачі розміщують або пересилають, за умови що вони:
 - a. не ініціюють передачу контенту;
 - b. не визначають одержувача;
 - c. не змінюють зміст повідомлень.
3. Для хостинг-провайдерів, які надають тимчасове зберігання, закон дозволяє автоматичне проміжне зберігання інформації без відповідальності, за умови, що:
 - a. не змінюється зміст;
 - b. забезпечується доступ згідно з промисловими стандартами;
 - c. при отриманні інформації про порушення – доступ блокується;
 - d. у разі видалення контенту у початковому джерелі – провайдер обмежує доступ до відповідаючого контенту.
4. Для тієї ж групи хостинг-провайдерів, що здійснюють постійне зберігання на запит користувача, застосовується аналогічний механізм: відповідальність настає лише після отримання відомостей про незаконну діяльність, включно з порушенням авторських прав, і якщо провайдер не вжив швидких заходів для обмеження доступу.
5. Якщо такий постачальник виходить за межі технічного посередництва – ініціює передачу, вибирає отримувача чи змінює контент – він втрачає цей захист. У такому разі він відповідальна за весь зміст, і зобов'язаний:
 - a. надавати контактну інформацію (найменування, адресу, електронну пошту, ідентифікатори, ліцензії тощо);
 - b. дотримуватися оподаткування за зазначену вартість послуг.

У межах цього закону постачальники послуг проміжного характеру в інформаційній сфері звільняються від відповідальності за контент за визначених умов – це відповідає принципу «safe harbour», закріпленого в праві ЄС (зокрема, у Директиві 2000/31/ЄС про

електронну комерцію)²⁶, згідно з яким технічні посередники не відповідають за незаконний контент, якщо дотримуються певних умов.

Закони України “Про авторське право і суміжні права”²⁷ та “Про охорону прав на знаки для товарів і послуг”²⁸ – визначають обсяг прав інтелектуальної власності та способи їх захисту. У новій редакції Закону “Про авторське право і суміжні права” від 01.12.2022 року розширено інтернет-складову: статтею 56 цього Закону вперше закріплено порядок припинення порушень авторського права і суміжних прав з використанням мережі Інтернет.

Стаття 56 Закону України “Про авторське право і суміжні права” визначає докладний адміністративний порядок дій, яких мають дотримуватись онлайн-платформи, хостинг-провайдери та власники веб-сайтів у разі порушення авторського права або суміжних прав в інтернеті. Ця процедура стала ключовим елементом у правовому регулюванні електронної комерції, оскільки встановлює чіткий механізм «notice-and-takedown» – від моменту звернення правовласника до власника веб-сайту або хостинг-провайдера до обов’язку обмежити доступ до контенту або відновити його у разі необґрунтованої заяви. Вона також вводить відповідальність за бездіяльність, строки реагування, стандарти ідентифікації сторін і способи комунікації. Таким чином, стаття спрямована на забезпечення оперативного захисту прав ІВ в онлайн-середовищі, мінімізуючи зловживання та балансуючи інтереси правовласників, провайдерів і користувачів.

Стаття 57 Закону України “Про авторське право і суміжні права” встановлює обов’язки постачальників послуг хостингу – ключових технічних посередників в екосистемі електронної комерції – із забезпечення дотримання прав інтелектуальної власності в мережі Інтернет. Зокрема, провайдери хостингових послуг зобов’язані передбачати у договорах із користувачами положення, що забороняють розміщення контенту з порушенням авторського та суміжних прав, а також вимагати надання достовірної контактної інформації. За умови дотримання цих вимог та виконання процедури реагування на порушення, визначеної статтею 56, постачальники звільняються від відповідальності за дії своїх клієнтів, що забезпечує баланс між захистом прав ІВ та стабільним функціонуванням онлайн-платформ.

Статтею 58 Закону “Про авторське право і суміжні права” визначена відповідальність провайдерів послуг обміну контентом. Ця стаття встановлює правила та відповідальність для платформ, які організовують обмін великими обсягами користувацького контенту (наприклад, відеохостинги, стрімінгові сервіси, соцмережі). Якщо такі провайдери не мають дозволу на розміщення об’єктів авторського права і при цьому не вжили достатніх заходів для попередження і припинення порушень, вони несуть відповідальність незалежно від факту повідомлення. Стаття визначає перелік

²⁶ Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) [Електронний ресурс]. – Режим доступу: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32000L0031>

²⁷ Закон України «Про авторське право і суміжні права» від 01.12.2022 № 2811-IX [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2811-20#Text>

²⁸ Закон України «Про охорону прав на знаки для товарів і послуг» від 15.12.1993 № 3689-XII [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/3689-12#Text>

заходів, які провайдер повинен вжити, щоб уникнути відповідальності, критерії оцінки належності цих дій, а також винятки для неприбуткових або невеликих платформ. Вона покликана стимулювати великі платформи до активної співпраці з правовласниками й запобігання піратству.

Водночас у сфері захисту прав на торговельну марку в Інтернеті спеціального адміністративного механізму «notice-and-takedown» поки не закріплено — відповідне порушення розглядається в межах загального судового або адміністративного порядку. Втім, відповідно до Закону України «Про охорону прав на знаки для товарів і послуг», такі порушення також можуть бути підставою для звернення до платформи з вимогою припинити незаконне використання торговельної марки, особливо якщо це стосується фейкових акаунтів, несанкціонованого маркування товарів або використання торговельної марки у рекламі.

У цьому контексті онлайн-платформи електронної комерції — особливо маркетплейси, соцмережі та сайти оголошень — можуть і повинні запроваджувати внутрішні процедури перевірки скарг на порушення прав на ТМ за аналогією з процедурою, передбаченою статтями 56–58 Закону про авторське право. Важливим стає формування превентивної політики (terms of service), обов'язку користувача вказувати достовірні контактні дані, а також оперативної модерації контенту, що порушує права ІВ. Такий підхід дозволяє забезпечити більшу передбачуваність, прозорість і швидкість у реагуванні на правопорушення в сфері електронної комерції.

Закон України «Про захист прав споживачів»²⁹ — містить визначення фальсифікованої продукції (виготовлена з порушенням технології або неправомірним використанням знака для товарів та послуг, чи копіюванням форми, упаковки, зовнішнього оформлення, а так само неправомірним відтворенням товару іншої особи) і забороняє продаж фальсифікату (стаття 6). Цей закон дозволяє споживачу подати скаргу до Державної служби України з питань безпечності харчових продуктів та захисту споживачів (Держпродспоживслужби), якщо він придбав підробку в Інтернеті. Закон також розширює можливості громадських споживчих організацій — вони можуть ініціювати експертизи та звертатися з пропозиціями про припинення реалізації фальсифікату (стаття 25). У свою чергу, Держпродспоживслужба має право вилучати фальсифіковану продукцію з ринку, проводити перевірки та відбір проб, накладати штрафи, видавати приписи та звертатися до суду з приводу порушень (стаття 26) .

Кримінально-правовий захист прав інтелектуальної власності в Україні передбачено, зокрема, статтями 176, 177, 229 та 231 Кримінального кодексу України³⁰, які встановлюють відповідальність за:

Порушення авторського права і суміжних прав (ст. 176);

²⁹ Закон України «Про захист прав споживачів» від 12.05.1991 № 1023-ХІІ [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/1023-12#Text>

³⁰ Кримінальний кодекс України від 05.04.2001 № 2341-ІІІ [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/2341-14#Text>

Порушення прав на винахід, корисну модель, промисловий зразок, топографію інтегральної мікросхеми, сорт рослин, раціоналізаторську пропозицію (ст. 177);

Незаконне використання знака для товарів і послуг, фірмового найменування, кваліфікованого зазначення походження товару (ст. 229);

Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю (ст. 231).

На практиці застосування кримінально-правових механізмів у сфері інтелектуальної власності є обмеженим, що зумовлено складністю збирання доказової бази, у тому числі в онлайн-продажах, та переважним фокусом правоохоронних органів на інших пріоритетних напрямках.

Особливої актуальності ця проблема набуває в умовах стрімкого розвитку електронної комерції, де значна частина порушень прав ІВ відбувається на маркетплейсах, у соціальних мережах та на спеціалізованих торговельних онлайн-майданчиках. Поширеним явищем є продаж підробленої продукції, неправомірне використання торговельних марок у найменуванні акаунтів чи описах товарів, копіювання контенту або бездозвільне використання авторських зображень та відео в онлайн-рекламі.

У сфері митного контролю в Україні застосовуються положення статей 397–403 Митного кодексу України³¹, які регламентують правила сприяння захисту прав інтелектуальної власності під час переміщення товарів через митний кордон України.

Зокрема, ці статті встановлюють такі основні механізми:

- Порядок митного контролю і митного оформлення товарів, що містять об'єкти права інтелектуальної власності (ст. 397);
- Митний реєстр об'єктів права інтелектуальної власності (ст. 398);
- Призупинення митного оформлення товарів на підставі даних митного реєстру (ст. 399);
- Призупинення митного оформлення товарів за ініціативою митного органу (ст. 400);
- Достроковий випуск товарів, митне оформлення яких призупинено за підозрою у порушенні прав інтелектуальної власності (ст. 400-1);
- Знищення товарів, митне оформлення яких призупинено за підозрою у порушенні прав інтелектуальної власності (ст. 401);
- Особливості призупинення митного оформлення та знищення невеликих партій товарів, що переміщуються (пересилаються) через митний кордон України у міжнародних поштових та експрес-відправленнях (ст. 401-1);
- Зміна маркування на товарах та їх упаковці (ст. 402);
- Особливості здійснення митними органами контролю щодо окремих товарів (ст. 402-1);

³¹ Митний кодекс України від 13.03.2012 № 4495-VI [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/4495-17#Text>

- Взаємодія митних органів з іншими органами державної влади у сфері захисту права інтелектуальної власності (ст. 403);

Ці положення є важливими не лише для традиційної торгівлі, але й у контексті електронної комерції, адже значна частина онлайн-замовлень передбачає міжнародне пересилання товарів, що потенційно порушують права інтелектуальної власності. Ефективна робота митниці у виявленні та блокуванні ввезення фальсифікованої продукції, зокрема через маркетплейси, сприяє запобіганню подальшому поширенню контрафакту на внутрішньому ринку.

Як кримінально-правовий, так і митний механізми повинні адаптуватися до нових викликів цифрової економіки, включно з розробкою спеціалізованих інструментів реагування на порушення прав ІВ в онлайн-продажах, спрощеними процедурами доступу до цифрових доказів і встановленням стандартів співпраці між державними органами, правовласниками та адміністраціями платформ електронної комерції.

Таким чином, українське законодавство поки не містить комплексного регулювання діяльності онлайн-платформ і маркетплейсів щодо запобігання порушенням прав ІВ з боку третіх осіб. Відсутність спеціальних процедур модерації контенту, обов'язкової верифікації продавців та єдиних стандартів реагування на скарги створює підвищені ризики для правовласників.

Наразі Україна активно працює над гармонізацією законодавства із законодавством Європейського Союзу, у тому числі щодо поступового впровадження елементів Digital Service Act (DSA). Відповідні зміни передбачають адаптацію вимог щодо прозорості алгоритмів, посилення модерації контенту, впровадження процедур реагування на порушення та підвищення відповідальності онлайн-платформ.

Впровадження відповідних елементів DSA, а також розвиток процедур позасудового вирішення спорів, зокрема онлайн-медіації, є актуальними напрямками вдосконалення національної системи захисту прав інтелектуальної власності, особливо в умовах зростання обсягів торгівлі в онлайн-середовищі.

Урахування сучасних викликів потребує розробки нових законодавчих підходів, які дозволяють ефективно захищати права інтелектуальної власності у цифровому середовищі, забезпечити верифікацію продавців і створити дієві механізми контролю на рівні платформ.

5.3. Політики платформ щодо захисту прав ІВ

Результати контент-аналізу свідчать про системну відсутність або недостатній рівень інституціоналізації політик захисту інтелектуальної власності на більшості українських онлайн-платформах. У рідкісних випадках такі політики формально присутні, однак інтегровані у загальні умови користування або правила публікації контенту без окремого процедурного супроводу. Зміст таких положень здебільшого обмежується декларативними заборонами на розміщення контрафактної продукції, при цьому

відсутній опис механізмів розгляду заяв, відповідальності сторін, а також стандартів взаємодії з правовласниками.

Це свідчить про недостатній ступінь формалізації політик у сфері ІВ та про те, що відповідні зобов'язання або не розглядаються онлайн-платформами як пріоритетні, або залишаються у сфері добровільного саморегулювання.

Превентивні заходи: характер та ефективність

У більшості проаналізованих випадків превентивні інструменти захисту ІВ є обмеженими або суто номінальними. Застосовуються переважно реактивні механізми, зокрема:

- модерація вручну контенту після отримання скарги;
- деактивація окремих оголошень або акаунтів на підставі підтвердженого порушення;
- верифікація бізнес-користувачів на етапі реєстрації у вигляді надання основних реєстраційних документів (лише на обмеженій кількості платформ).

Автоматизовані механізми попереднього сканування контенту, виявлення потенційно порушуючих оголошень або алгоритми фільтрації за ключовими словами майже не застосовуються. Основна увага платформ зосереджена на контролі за дотриманням етичних норм, рекламних обмежень або вимог безпеки, тоді як права ІВ залишаються на периферії регуляторного поля.

Механізми подання та розгляду скарг

Порядок подання скарг на порушення прав ІВ здебільшого не є уніфікованим або стандартизованим. Близько половини досліджених платформ надають лише загальні канали комунікації (форма зворотного зв'язку, електронна пошта служби підтримки), без виділення окремої категорії для скарг, пов'язаних з ІВ. Лише окремі приклади демонструють існування спеціалізованого механізму подання скарг із вказівкою на перелік необхідних доказів, очікуваний строк розгляду, а також можливі санкції щодо порушника.

Проблемною залишається також відсутність прозорості процедури відстеження статусу скарги, відсутність чіткої комунікації з правовласником, а також фактична невизначеність у питанні ролі платформи як посередника між сторонами конфлікту. У низці випадків прямо зазначено, що спори між користувачами (включно з питань ІВ) мають вирішуватись в судовому порядку, без участі самої платформи.

Ключові структурні проблеми

Серед основних виявлених проблемних аспектів, що перешкоджають ефективному захисту прав ІВ на українських платформах, варто виокремити:

- відсутність централізованих політик або регламентів, що визначають стандарти взаємодії з правовласниками;

- мінімальна автоматизація у сфері виявлення порушень, що унеможлиблює масштабний контроль контенту;
- непередбачуваність процедур розгляду скарг, включаючи відсутність фіксованих строків та прозорості;
- відсутність механізму відповідальності за рецидивні порушення;
- повна відсутність проактивного моніторингу: платформи не виявляють порушення самостійно, очікуючи звернення правовласника.

5.4. Приклади позитивної практики

Незважаючи на загальний недостатній рівень забезпечення захисту прав ІВ на онлайн-платформах, окремі платформи демонструють позитивну динаміку. Зокрема:

- деякі маркетплейси вже адаптували базові елементи моделі «notice and takedown», яка передбачає видалення контенту на підставі вмотивованої скарги;
- реалізовано процедури верифікації бізнес-користувачів, що знижує ризики анонімної торгівлі контрафактом;
- наявні випадки ефективної співпраці з правовласниками, що призводили до блокування значної кількості нелегітимного контенту — особливо у чутливих категоріях товарів, таких як брендові парфуми, техніка та одяг.

Приклад Prom.ua

Prom.ua – велика платформа з фокусом на малий бізнес і маркетплейс-модель, реалізувала обов'язкову верифікацію продавців, а також здійснює вибірккову перевірку ліцензій або сертифікатів відповідності для певних категорій товарів. Скарги правовласників приймаються через спеціалізовану форму та можуть призводити до блокування продавця або припинення публікації його товарів.

Prom.ua запровадив прозору систему звітності та співпраці з правовласниками³². Вони регулярно публікують Звіт щодо захисту авторського права, де наводять статистику видалених товарів та опрацьованих скарг. У 2024 році Prom видалив майже мільйон позицій порушників і зменшив середній час реакції до 21 хвилини³³. Це свідчить про реально працюючу систему “notice and takedown” на національному рівні.

Приклад OLX Україна

OLX Україна – одна з найбільших платформ оголошень вже реалізувала розділ, присвячений забороні порушення прав ІВ, у якому чітко вказано на неприпустимість розміщення підробок. Крім того, вона активно модерує контент, а також співпрацює з

³² Prom.ua. Центр підтримки: Звіти щодо захисту авторського права [Електронний ресурс]. – Режим доступу: <https://support.prom.ua/hc/uk/sections/27557388464285>

³³ Prom.ua. Звіт щодо захисту авторського права [Електронний ресурс]. – Режим доступу: <https://support.prom.ua/hc/uk/articles/18237035925661-%D0%97%D0%B2%D1%96%D1%82-%D1%89%D0%BE%D0%B4%D0%BE-%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83-%D0%B0%D0%B2%D1%82%D0%BE%D1%80%D1%81%D1%8C%D0%BA%D0%BE%D0%B3%D0%BE-%D0%BF%D1%80%D0%B0%D0%B2%D0%B0-2024#:~:text=950>

правовласниками в процесі видалення оголошень, що порушують авторські права або права на торговельні марки.

Замість пасивного спостереження, OLX Україна долучився до просвітницької кампанії “Довіряй оригіналу” (Trust the Original)³⁴ спільно з Українським національним офісом інтелектуальної власності та інновацій (далі – УКРНОІВІ). У рамках цієї кампанії платформа інформує продавців і покупців про небезпеки контрафакту, роз’яснює правила та закликає не продавати і не купувати підробки. Це позитивний приклад соціальної відповідальності бізнесу.

Отже, досвід українських платформ, таких як Prom.ua та OLX Україна, демонструє поступову інтеграцію міжнародних підходів до захисту прав інтелектуальної власності. Незважаючи на обмежений рівень нормативного тиску, реалізовані ними ініціативи свідчать про наявність потенціалу для формування внутрішніх механізмів саморегулювання та підвищення стандартів у сфері захисту інтелектуальної власності в електронній комерції.

Співпраця з правоохоронними органами

У сфері захисту прав інтелектуальної власності важливою є співпраця платформ електронної комерції з правоохоронними органами. Такі платформи можуть відігравати активну роль, зокрема надаючи дані про продавців, сприяючи розслідуванням та співпрацюючи у судових процесах. Хоча в офіційних повідомленнях не завжди розкриваються назви сервісів, участь маркетплейсів у виявленні та припиненні онлайн-продажу контрафактної продукції є позитивною тенденцією.

У 2024 році БЕБ спільно з Кіберполіцією викрили групу осіб, які незаконно продавали підроблені гаджети під відомим брендом. Підробки рекламували та продавали на вебсайтах, Instagram-сторінці та telegram-каналах. Покупцям пропонували широкий асортимент техніки: зарядні пристрої, навушники, смартгодинники тощо. Брендovanу продукцію надсилали поштою по всій території України. Вилучено понад 4 тис. одиниць контрафактної продукції, а збитки правовласника оцінили у 25 млн грн³⁵.

6. Інструменти захисту прав ІВ

Онлайн-платформи та маркетплейси, як ключові інструменти електронної комерції, створюють як нові можливості для правовласників, так і суттєві ризики порушень прав інтелектуальної власності. У відповідь на ці виклики сформувалася система правових і технічних інструментів, яка охоплює як внутрішні механізми реагування, що впроваджуються самими платформами, так і зовнішні способи захисту — зокрема, судові та позасудові процедури. Міжнародна практика підтверджує, що належним чином

³⁴ Український національний офіс інтелектуальної власності та інновацій (УКРНОІВІ) та онлайн-платформа OLX.UA, Кампанія «Trust the Original» [Електронний ресурс]. – Режим доступу: <https://nipo.gov.ua/ne-daj-sebe-pidrobity/>

³⁵ Бюро економічної безпеки України. БЕБ та Кіберполіція викрили мережу з продажу підробленої техніки відомого бренду [Електронний ресурс]. – Режим доступу: <https://esbu.gov.ua/news/beb-ta-kiberpolitsiia-vykryly-merezhu-z-prodazhu-pidroblenoi-tekhniky-vidomoho-brendu>

реалізовані механізми notice-and-takedown (Дослідження Understanding WIPO's Role in Copyright Protection and International Enforcement, Legal IP Strategies Staff, 2024)³⁶, адміністративні процедури реагування на скарги, а також альтернативні способи вирішення спорів можуть забезпечити оперативне й ефективне припинення порушень прав інтелектуальної власності в цифровому середовищі.

6.1. Адміністративні інструменти на платформах

Адміністративні інструменти захисту прав інтелектуальної власності на інтернет-платформах — це внутрішні механізми, які передбачають можливість правовласників або їх уповноважених осіб подавати скарги на порушення прав інтелектуальної власності.

У межах Digital Millennium Copyright Act (DMCA)³⁷ — американського закону про авторське право, ухваленого у 1998 році — встановлено механізм захисту інтернет-платформ від відповідальності за розміщений користувачами контент за умови своєчасного реагування на скарги правовласників. DMCA передбачає процедуру notice-and-takedown, за якою платформа зобов'язується оперативно видалити або заблокувати доступ до контенту чи товару після отримання належним чином оформленої скарги. Ці інструменти є першим і найбільш оперативним рівнем захисту прав ІВ у цифровому середовищі, що дозволяє значно скоротити шкоду від порушень та мінімізувати необхідність залучення судових інстанцій.

Міжнародні дані підтверджують ефективність процедури notice-and-takedown: відповідно до дослідження Berkeley/USC³⁸, більшість звернень результативні, хоча існують ризики зловживань.

В українській практиці адміністративні інструменти захисту прав ІВ на платформах починають активно застосовуватися в контексті маркетплейсів та соціальних мереж. Так, великі маркетплейси, як-от Prom.ua, OLX, Rozetka, впровадили механізми обробки скарг правовласників з подальшим блокуванням або видаленням контрафактної продукції. Аналогічні процедури застосовують і соціальні мережі — Meta, YouTube, TikTok — у співпраці з українськими правовласниками, що значно підвищує оперативність реагування на порушення.

6.2. Судовий та позасудовий захист

Судовий та позасудовий захист прав інтелектуальної власності залишається ключовим механізмом у випадках, коли адміністративні інструменти на платформах не забезпечують повного або своєчасного відновлення порушених прав.

³⁶ WIPO. Understanding WIPO's Role in Copyright Protection and International Enforcement, Legal IP Strategies Staff, 2024 [Електронний ресурс]. — Режим доступу: <https://legalipstrategies.com/wipos-role-in-copyright-protection/>

³⁷ Digital Millennium Copyright Act (DMCA) of 1998, Public Law 105–304, United States Copyright Law [Електронний ресурс]. — Режим доступу: <https://www.copyright.gov/legislation/dmca.pdf>

³⁸ CREATe. 21 for 2021: Notice and Takedown in Copyright Intermediary Liability [Електронний ресурс]. — Режим доступу: <https://www.create.ac.uk/blog/2021/06/25/21-for-2021-notice-and-takedown-in-copyright-intermediary-liability/>

Судовий механізм захисту прав інтелектуальної власності передбачає звернення правовласника до компетентного суду з позовом про відновлення порушеного права, припинення порушення та, за потреби, стягнення компенсації.

Однією з основних форм такого захисту в Україні є подання правовласником позову про припинення порушення авторського права та стягнення компенсації. Такий механізм передбачений статтею 53 Закону України «Про авторське право і суміжні права» і застосовується у випадках, коли об'єкт авторського права — наприклад, музичний твір, відеоконтент, програмне забезпечення або літературний твір — був незаконно використаний без згоди правовласника. У сфері електронної комерції такі порушення найчастіше проявляються у вигляді несанкціонованого використання контенту на маркетплейсах, платформах онлайн-продажу, стрімінгових сервісах або в рекламних оголошеннях. Судовий захист у цьому випадку дає змогу не лише зупинити порушення (через зобов'язання видалити контент, заблокувати акаунт продавця або припинити розповсюдження контрафактної продукції), а й стягнути з порушника грошову компенсацію. Така форма захисту є ефективним інструментом протидії цифровому піратству, комерціалізації чужого контенту без дозволу, а також системному порушенню прав у межах електронної комерції.

Позасудовий (альтернативний) захист прав інтелектуальної власності — це механізм, який дозволяє сторонам вирішувати суперечки без звернення до суду, зазвичай шляхом медіації, арбітражу та інших процедур альтернативного врегулювання спорів (ADR). Цей підхід забезпечує гнучкість, конфіденційність, економію часу й зниження витрат, водночас зберігає ділові стосунки між сторонами. Процедури ADR передбачають:

Медіацію — двосторонній або багатосторонній переговорний процес із присутністю нейтральної сторонньої особи (медіатора), яка допомагає сторонам знайти взаємоприйнятне рішення;

Арбітраж — формальний, але швидший та менш витратний за суд альтернативний спосіб, який завершується обов'язковим рішенням арбітражного трибуналу.

За даними WIPO³⁹, у 2024 році через WIPO Arbitration and Mediation Center було врегульовано 858 спорів у галузі інтелектуальної власності, з них 77 % стосувалися авторського права та цифрового контенту. Це свідчить про швидке зростання ADR-практик (на 25 % порівняно з попереднім роком).

У сфері доменних спорів⁴⁰ за процедурою UDRP WIPO зафіксовано понад 6 000 звернень у 2023 році, з яких 93 % завершилися позитивно для правовласників.

Таким чином, ADR-інструменти в сфері інтелектуальної власності — набувають дедалі ширшого застосування. Вони є дієвим доповненням до судових процедур, особливо в

³⁹ WIPO Arbitration and Mediation Center. WIPO ADR Highlights 2024: WIPO Out-of-Court IP Dispute Resolution Services Continue to Grow [Електронний ресурс]. – Режим доступу: <https://www.wipo.int/amc/en/center/summary2024.html>

⁴⁰ World Trademark Review. Recent Trends in WIPO Arbitration and Mediation [Електронний ресурс]. – Режим доступу: <https://www.worldtrademarkreview.com/guide/the-guide-ip-arbitration/third-edition/article/recent-trends-in-wipo-arbitration-and-mediation>

конфліктах, що стосуються цифрового контенту, співпраці між платформами та ліцензійних договорів, сприяючи своєчасному й ефективному вирішенню спорів.

6.3. Співпраця з митними та правоохоронними органами

Ефективна боротьба з порушеннями прав інтелектуальної власності в Україні неможлива без тісної взаємодії між митними та правоохоронними органами. Така співпраця сприяє своєчасному виявленню та припиненню незаконного ввезення контрафактної продукції, що негативно впливає на економіку та репутацію легальних виробників. Митні органи виконують функцію першої лінії оборони, перешкоджаючи незаконному ввезенню та вивезенню контрафактної продукції, що шкодить легальним виробникам і правовласникам. Законодавство України передбачає механізми обміну інформацією та спільного реагування між митницею, поліцією, прокуратурою та іншими правоохоронними структурами.

Ключовим інструментом у цій взаємодії є проведення спільних заходів, митних оглядів та перевірок, які базуються на аналітичних даних та повідомленнях про підозрілу діяльність. Важливим аспектом є також впровадження сучасних технологій моніторингу та контролю, що підвищує швидкість і якість реагування на випадки порушень. За останні роки співпраця між органами значно посилилася завдяки запровадженню чітких процедур взаємодії та обміну інформацією, що сприяє зниженню обсягів контрафактної продукції на ринку.

Важливу роль у цьому процесі відіграє Центр спостереження з питань порушень прав інтелектуальної власності⁴¹, який функціонує при УКРНОІВІ. Центр виконує аналітичні, комунікаційні та координаційні функції, забезпечує інформаційну підтримку митних і правоохоронних органів, сприяє виявленню порушень на онлайн-платформах і маркетплейсах та організовує відповідні інформаційно-просвітницькі кампанії.

Крім того, Центр спостереження організовує заходи для представників митних, правоохоронних органів та бізнесу, проводить аналітичні дослідження щодо обсягів і тенденцій порушень прав ІВ на маркетплейсах, а також розвиває експертний нетворкінг у цій сфері.

6.4. Онлайн-медіація як сучасний інструмент захисту прав ІВ

З огляду на масштабну роль маркетплейсів у сучасній електронній комерції, медіація стає ключовим механізмом для швидкого та ефективного вирішення спорів щодо порушення прав інтелектуальної власності, що виникають у цифровому середовищі.

Онлайн-медіація - це форма альтернативного вирішення спорів (ADR), яка проводиться із залученням нейтрального посередника (медіатора) через цифрові платформи, без необхідності фізичної зустрічі сторін конфлікту.

⁴¹Доступно за посиланням: <https://nipo.gov.ua/ukr-tsentr-sposterezhennia-porushen-ip-prav/>

Цей механізм дозволяє ефективно врегульовувати спори, що виникають у зв'язку з порушенням авторських прав, патентів, товарних знаків або інших об'єктів інтелектуальної власності в онлайн-середовищі.

Хто може бути сторонами медіації?

Учасник	Хто це?	Роль у медіації
Правовласник	Автори, компанії, власники ІВ	Захищають свої права, ініціюють або беруть участь у медіації
Продавець	Онлайн-магазини, підприємці	Вирішують питання використання контенту чи товарів
Платформа	Маркетплейси, хостинг-сервіси	Посередники, що забезпечують майданчик для торгівлі та можуть бути стороною конфлікту
Споживач	Користувачі, покупці	Можуть бути учасниками спору у випадках порушення прав ІВ

Навіщо потрібна онлайн-медіація у сфері ІВ?

Онлайн-медіація має низку характеристик, які зумовлюють її ефективність як механізму альтернативного вирішення спорів у сфері інтелектуальної власності, особливо в умовах цифровізації та глобалізації торгівлі.

1. Оперативність та економія часу

Однією з ключових переваг онлайн-медіації є суттєве скорочення строків розгляду спору. На відміну від традиційного судового провадження, яке у транскордонних спорах може тривати роками, медіація дозволяє досягти компромісного рішення упродовж кількох днів або тижнів. Це особливо важливо у випадках, коли затримка може мати прямі комерційні або репутаційні наслідки (наприклад, поширення плагіату або продаж контрафактної продукції).

2. Гнучкість процедури та креативність рішень

Процедура медіації не регламентується суворими процесуальними вимогами, що дозволяє сторонам самостійно визначати зручний формат комунікації (електронна пошта, відеозв'язок, месенджери), мову спілкування, а також час та темп переговорів.

Крім того, сторони мають змогу домовитися не лише про матеріальне відшкодування, але й про інші форми врегулювання, зокрема:

- укладення ліцензійної угоди;
- визнання співавторства;
- можливість спільної комерціалізації об'єкта ІВ;
- публічне спростування або вибачення.

3. Економічна доцільність

Онлайн-медіація є більш доступною в економічному плані порівняно із судовим процесом. Зменшуються витрати на судові збори, подорожі, юридичні послуги, переклад документів та подання позовів у кількох юрисдикціях. Це робить процедуру особливо привабливою для представників малого бізнесу, креативних індустрій, стартапів, які можуть бути обмежені в ресурсах.

4. Конфіденційність

Медіаційна процедура є закритою, а її результати не підлягають обов'язковому оприлюдненню. Це дозволяє сторонам зберегти конфіденційність комерційної інформації, уникнути публічного розголосу факту конфлікту та знизити потенційні репутаційні ризики.

5. Можливість збереження ділових відносин

Медіація передбачає співпрацю, а не протистояння. Це дозволяє зберегти або навіть покращити ділові стосунки між сторонами. Під час процедури створюється безпечний простір для конструктивного діалогу, що у багатьох випадках сприяє не лише припиненню спору, але й відкриває перспективи для подальшої взаємодії.

6. Транскордонна доступність

Онлайн-медіація дозволяє ефективно вирішувати спори між суб'єктами, що перебувають у різних країнах, юрисдикціях і часових поясах. Її застосування є особливо актуальним у таких ситуаціях, як:

- спори між українськими продавцями і міжнародними платформами (наприклад, Amazon, Etsy);
- порушення прав на доменні імена у глобальних зонах (.com, .eu тощо);
- незаконне використання цифрових об'єктів ІВ у хмарних сервісах, на вебсайтах або в соціальних мережах.

Приклади онлайн-медіації у сфері ІВ в Європейському Союзі.

У Європейському Союзі онлайн-медіація розвивається як ключовий елемент стратегії забезпечення безпеки електронної комерції та захисту прав споживачів і правовласників у цифровому середовищі. ЄС демонструє системний і багаторівневий підхід до впровадження механізмів альтернативного вирішення спорів, зокрема в онлайн-форматі (ODR – Online Dispute Resolution).

1. Європейська платформа ODR

Онлайн-платформа вирішення спорів (ODR Platform) була створена відповідно до Регламенту (ЄС) № 524/2013⁴² та функціонує під управлінням Європейської Комісії. Основні характеристики:

- Доступ до сертифікованих органів ADR у всіх країнах ЄС, а також Ісландії, Ліхтенштейні та Норвегії.
- Платформа дозволяє ініціювати вирішення спорів між споживачами та продавцями онлайн у транскордонному режимі.
- Всі інтернет-магазини зобов'язані розміщувати посилання на цю платформу на своїх сайтах, що сприяє її активному використанню.

Це створює прозорий і доступний механізм для врегулювання споживчих спорів, включаючи випадки неправомірного використання об'єктів ІВ у товарах або рекламі.

2. Власні ODR-системи на маркетплейсах

Великі торговельні платформи, які працюють в ЄС, активно впроваджують внутрішні ODR-механізми для врегулювання спорів між продавцями, покупцями та третіми сторонами (зокрема, правовласниками). Наприклад:

- eBay та аналогічні платформи щорічно обробляють десятки мільйонів спорів.
- Процес часто починається із автоматизованих переговорів між сторонами.
- У разі нерозв'язання спору пропонується медіація або інші ADR-методи з чіткими строками (наприклад, можливість подати претензію протягом 30 днів після доставки товару).

Ці підходи дозволяють швидко реагувати на порушення прав ІВ без звернення до суду, зберігаючи при цьому функціональність платформи та лояльність користувачів.

3. Участь міжнародних організацій: WIPO

Важливу роль у впровадженні онлайн-медіації у сфері ІВ в Європі та за її межами відіграє Центр арбітражу та медіації BOIB (WIPO ADR Center). Цей орган:

- Спеціалізується на онлайн-врегулюванні спорів у сфері ІВ.
- Пропонує ефективні процедури для вирішення конфліктів, пов'язаних із доменними іменами, авторськими правами, торговельними марками.

Є популярним серед ІТ-компаній, медіа-бізнесу, платформ з цифровим контентом.

Особливої популярності WIPO ADR набули у спрах про порушення прав ІВ в онлайн-просторі, які мають транскордонний характер.

⁴² Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Regulation on consumer ODR) [Електронний ресурс]. – Режим доступу: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R0524>

Огляд сучасного стану існування онлайн-платформи для вирішення спорів в Україні

Медіація офіційно визнана в Україні: 15 грудня 2021 року набув чинності Закон України «Про медіацію»⁴³, прийнятий 16 листопада 2021 року. Закон має рамковий характер, встановлює правовий статус медіатора, процедуру, вимоги й сфери застосування: цивільні, комерційні, трудові, адміністративні спори, а також деякі кримінальні випадки.

Україна адаптувала Керівні принципи Ради Європи з ODR, забезпечуючи відповідність стандартам справедливого судочинства, захисту даних тощо.

Затверджено урядові стратегії цифровізації судочинства, які передбачають електронні консультації, онлайн-вивчення справ, документообіг - зокрема для спрощених справ.

На сьогоднішній день в Україні система онлайн вирішення спорів перебуває на початковому етапі розвитку та не функціонує як повноцінний інструмент альтернативного вирішення правових конфліктів. Попри загальну тенденцію цифровізації у правовій сфері, онлайн-механізми для вирішення спорів застосовуються переважно у вузьких сферах - таких як електронна комерція або фінансові сервіси - та не мають належної нормативної підтримки.

Водночас варто зауважити, що певні ініціативи щодо запуску відповідних онлайн-платформ все ж здійснювались. Зокрема, реалізовувалися окремі пілотні проєкти, які мали на меті протестувати можливості цифрових інструментів для вирішення конфліктів у досудовому порядку. Наприклад, у рамках ініціатив деяких громадських організацій та за підтримки міжнародних партнерів тестувалися онлайн-платформи для медіації та досудового врегулювання спорів у сфері споживчого захисту.

Деякі фріланс-платформи також впроваджують внутрішні процедури вирішення спорів між замовниками та виконавцями, орієнтуючись на міжнародні моделі, як-от Upwork Dispute Resolution. Проте такі механізми поки не набули широкого поширення і найчастіше є частиною приватних сервісів конкретних платформ.

У сфері електронної комерції українські маркетплейси надають користувачам можливість звертатися зі скаргами до служби модерації, зокрема у випадках порушення прав інтелектуальної власності та інших спірних ситуацій. Втім, наразі ці процедури не передбачають застосування формалізованих механізмів альтернативного вирішення спорів.

Існують організації, які надають послуги проведення медіації в онлайн-форматі, зокрема у сфері інтелектуальної власності. Одним із таких прикладів є Центр медіації та посередництва при УкрНОІВІ⁴⁴, який спеціалізується на альтернативному врегулюванні спорів, що пов'язані з правами інтелектуальної власності, з використанням сучасних цифрових технологій.

⁴³ Закон України «Про медіацію» від 16.11.2021 № 1875-IX [Електронний ресурс]. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/1875-20#Text>

⁴⁴ Доступно за посиланням: <https://nipo.gov.ua/ukr-tsentr-sposterezhennia-porushen-ip-prav/>

Однією з найперспективніших сфер для запуску таких інструментів є інтелектуальна власність. Саме у цій галузі конфлікти часто мають транскордонний характер, виникають у цифровому середовищі, потребують оперативного реагування та не завжди потребують судового втручання. Водночас міжнародний досвід демонструє, що онлайн-медіація у сфері ІВ може бути ефективним інструментом, який поєднує швидкість, гнучкість та захист прав.

Онлайн-медіація у сфері інтелектуальної власності - це не просто зручний інструмент для вирішення спорів, а відповідь на виклики цифрової епохи. У час, коли створити ідею, продукт чи контент стало простіше, ніж будь-коли, питання їх захисту вимагає нових підходів.

6.5. Технологічні рішення та автоматизація

Захист прав інтелектуальної власності в онлайн-середовищі сьогодні неможливо уявити без широкого впровадження технологічних інструментів та автоматизованих рішень. У відповідь на зростання обсягів торгівлі на маркетплейсах, стрімку зміну способів порушень і використання організованих шахрайських мереж, провідні міжнародні платформи вже активно застосовують передові технології для виявлення, блокування і запобігання порушенням.

Зокрема, штучний інтелект та алгоритми машинного навчання стали основою технологічної стратегії найбільших платформ електронної комерції. За даними Amazon Brand Protection Report 2024⁴⁵, понад 99% контрафактних оголошень на платформі було виявлено ще до їхньої публікації завдяки автоматичній системі перевірки, яка аналізує тексти, зображення та поведінкові сигнали. Подібний підхід успішно використовують й інші міжнародні гравці, включаючи Alibaba та eBay.

Важливою складовою сучасних систем моніторингу стала технологія computer vision, яка дозволяє виявляти копії фотографій товарів навіть у випадках їхнього часткового редагування. Наприклад, Alibaba повідомляє, що їхні автоматизовані системи щодня обробляють понад 200 мільйонів товарних оголошень, виявляючи ознаки візуальних маніпуляцій, таких як зміна фону, кадрування чи додавання водяних знаків.

Для ефективної боротьби з системними порушеннями, пов'язаним із багаторазовою реєстрацією акаунтів, платформи активно впроваджують технології аналізу мереж користувачів. Зокрема, Amazon та eBay аналізують IP-адреси, платіжні реквізити, пристрої, браузерні відбитки та поведінкові патерни для виявлення пов'язаних акаунтів і запобігання їх повторній появі після блокування. Важливо, що ці технології дозволяють виявляти цілі шахрайські мережі та оперативно припиняти їх діяльність.

Ще одним значущим інструментом стали алгоритми для виявлення та блокування ботів. На багатьох платформах порушники використовують автоматизовані боти для масового створення фальшивих оголошень з незначними змінами для обходу фільтрів.

⁴⁵ Amazon. Amazon Brand Protection Report 2024 [Електронний ресурс]. – Режим доступу: <https://assets.aboutamazon.com/22/3b/a9c54c7940f683f90022a3d1aaec/amazon-bpr-2024-3-21-2024-final.pdf>

Сучасні технології дозволяють оперативно виявляти таку активність на основі аналізу нетипових схем розміщення контенту.

Окрему увагу в міжнародній практиці приділяють розвитку блокчейн-рішень для відстеження ланцюгів постачання та перевірки автентичності товарів. Наприклад, компанія Nike впровадила пілотну програму з використанням блокчейн-технологій, яка дозволяє споживачам перевірити справжність продукту через сканування QR-коду. Nike отримала патент на технологію "CryptoKicks"⁴⁶: фізичне взуття має унікальний ідентифікатор (ID), прив'язаний до цифрового токена в блокчейні, який зберігається у цифровому "лакери" власника — Digital Locker. Цей підхід дозволяє підтвердити автентичність та реєструвати право власності, навіть після перепродажу.

Окрім кейсів Amazon, Alibaba та Nike, важливою є технологічна інновація, запропонована британською компанією Opsydia⁴⁷. Ця компанія розробила унікальну лазерну технологію нанесення невидимих ID-кодів всередині структури алмазів. Позначки, які розміщуються на глибині менше одного мікрона, неможливо стерти або видалити без знищення самого дорогоцінного каменю. Такі коди закріплюються в блокчейн-реєстрах і дозволяють ідентифікувати походження алмазу, навіть після перепродажу. Це поєднання фізичного маркування та цифрової сертифікації створює безпрецедентно високий рівень захисту та простежуваності, який уже застосовується в ювелірній промисловості і потенційно може бути адаптований до інших високоризикових товарних категорій, зокрема годинників, витворів мистецтва, елементів авіаційної чи автомобільної техніки.

На практиці міжнародні платформи також активно інтегрують WIPO ALERT – спеціалізовану базу Всесвітньої організації інтелектуальної власності, яка містить перелік сайтів, що системно порушують права ІВ. Це дозволяє платформам автоматично блокувати підозрілий контент без необхідності додаткових перевірок.

Ключовою вимогою європейського регулювання, зокрема Digital Services Act (DSA), стало забезпечення прозорості алгоритмів та публічна звітність. Платформи зобов'язані регулярно оприлюднювати дані щодо кількості виявлених порушень, часу реагування, ефективності своїх систем модерації та здійснювати незалежні аудити. Відповідні практики вже реалізовані на Amazon, eBay та AliExpress, які щороку публікують детальні звіти про боротьбу з контрафактом.

У межах обговорень на International IP Enforcement Summit 2025⁴⁸ було представлено низку додаткових технологічних рішень, які формують актуальні світові тренди в автоматизації захисту прав інтелектуальної власності.

Зокрема, Світова митна організація (WCO) акцентує увагу на впровадженні AI-підтриманого рентген-сканування та Smart Customs Portal для перевірки посилок у митних пунктах. Ці рішення дозволяють ефективніше виявляти підозрілі товари в умовах

⁴⁶ United States Patent and Trademark Office. US Patent No. US10505726B1. Digital Asset for Footwear [Електронний ресурс]. – Режим доступу: <https://patents.google.com/patent/US10505726B1/en>

⁴⁷ Institute of Physics. Opsydia: Previous Business Awards Winners [Електронний ресурс]. – Режим доступу: <https://www.iop.org/about/awards/business-awards/previous-business-awards-winners/opsydia>

⁴⁸ Доступно за посиланням: <https://www.euipo.europa.eu/en/landing-pages/international-ip-enforcement-summit-2025>

стрімкого зростання обсягів електронної комерції де понад 70% виявлених порушень пов'язані саме з електронною комерцією.

Особливої уваги заслуговує гібридна модель моніторингу CoreSearch⁴⁹, яка поєднує автоматизований AI-аналіз текстових і візуальних елементів товарних оголошень із обов'язковим залученням фахівця на фінальному етапі. Такий підхід забезпечує баланс між високою швидкістю обробки та необхідною якістю перевірки, а також дозволяє дотримуватися політик брендів і вимог законодавства.

Цікавою є практика LaLiga, яка запровадила власну AI-платформу для виявлення піратських трансляцій у реальному часі, із застосуванням технології "fingerprinting" — вбудованих унікальних кодів у відеопотік. Схожі рішення потенційно можуть бути використані й на маркетплейсах для маркування візуального контенту товарів з метою оперативного виявлення підробок.

Також обговорювались нові напрями використання AI для боротьби з піратством і торгівлею контрафактом у криптовалютних мережах і Darknet, зокрема в рамках проекту ISOP (Interpol)⁵⁰.

Водночас експерти звертають увагу на ризики, пов'язані з data poisoning (навмисним внесенням хибних даних для заплутування AI) та AI-hallucination (помилковою генерацією результатів без реальної підстави), що особливо актуально в контексті автоматизації модерації контенту.

Компанія CounterCheck⁵¹ презентувала використання AI для ризик-аналізу товарних потоків на складах, включно з RFID-маркуванням, баркодуванням та інтеграцією блокчейн-технологій для простежуваності постачання.

Компанія CounterCheck розробила систему, яка дозволяє автоматично перевіряти товари на складах за допомогою штучного інтелекту. Їхня технологія допомагає виявляти підозрілі партії товарів ще до того, як вони потрапляють на полиці магазинів або на онлайн-платформи.

Для цього компанія використовує:

- RFID-маркування: спеціальні мітки, які прикріплюються до товарів і дозволяють їх швидко знайти та перевірити за допомогою радіохвиль.
- Баркоди: стандартні штрих-коди, які система сканує для перевірки інформації про товар.
- Блокчейн: цифровий реєстр, де зберігається вся історія переміщення товару — від виробника до складу. Такий запис неможливо підробити.
- AI-ризик-аналіз: штучний інтелект автоматично аналізує походження товару, маршрути доставки, постачальників і порівнює ці дані з офіційними базами. Якщо

⁴⁹ Доступно за посиланням: <https://corsearch.com/>

⁵⁰ INTERPOL. Project I-SOP: INTERPOL Stop Online Piracy. Coordinating a Global Cross-Sector Response to Digital Piracy [Електронний ресурс]. — Режим доступу: <https://www.interpol.int/en/Crimes/Illicit-goods/Projects/Project-I-SOP>

⁵¹ Доступно за посиланням <https://www.countercheck.com/>

система виявляє розбіжності або підозрілі схеми, такий товар позначається для додаткової перевірки.

Ця технологія дозволяє компаніям і платформам виявляти потенційно контрафактні товари ще на етапі логістики та мінімізувати ризик їх потрапляння до споживачів.

Окремий сучасний виклик становить поширення контрафактних товарів через віртуальних інфлюенсерів (CGI), цифрових клонів (digital twins), тимчасові сторіс та приватні канали, такі як WhatsApp. Це вимагає від платформ оновлення алгоритмів і адаптації до нових каналів поширення. Серед перспективних напрямів Європейський Союз активно готується до впровадження цифрового продуктового паспорту (Digital Product Passport, DPP)⁵², який стане обов'язковим з 2027 року. Цей паспорт має містити інформацію про походження, склад, екологічні показники та інші ключові атрибути товару, що дозволить споживачам і платформам більш ефективно перевіряти автентичність продукції.

В Україні застосування подібних технологічних рішень наразі перебуває на початковому етапі. Українським маркетплейсам доцільно орієнтуватися на міжнародні стандарти та поступово впроваджувати сучасні технології автоматизації, зокрема:

- алгоритми автоматичного аналізу контенту на етапі передпублікаційної модерації;
- системи ідентифікації пов'язаних акаунтів з використанням аналізу IP-адрес, платіжних методів і поведінкових патернів;
- інтеграцію з міжнародними базами, такими як WIPO ALERT;
- розвиток технологій аналізу поведінки користувачів для виявлення шахрайських мереж;
- впровадження елементів блокчейн-рішень для прозорого контролю ланцюгів постачання;
- регулярну публічну звітність про виявлені порушення та роботу служб модерації;
- системну підготовку контент-модераторів з фокусом на питання захисту прав інтелектуальної власності.

Серед основних викликів для впровадження таких рішень в Україні залишаються: висока вартість розробки та підтримки власних технологічних систем, обмеженість технічних ресурсів, відсутність регуляторного зобов'язання щодо публічної звітності та низький рівень обізнаності серед бізнесу і споживачів про важливість прозорих механізмів захисту прав ІВ.

Успішне запровадження технологічних рішень українськими платформами потребує стратегічного бачення, готовності до інвестицій, а також належної державної підтримки через роз'яснення, консультації, а в перспективі – через поступове імплементація вимог, сумісних із європейським Digital Services Act. Такий підхід дозволить створити

⁵² European Commission. Digital Product Passport: Overview and Next Steps [Електронний ресурс]. – Режим доступу https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14382-Digital-product-passport-rules-for-service-providers_en

більш безпечне та конкурентоспроможне онлайн-середовище, здатне ефективно протидіяти порушенням прав інтелектуальної власності.

6.6. Інформування, просвіта та профілактика

В Україні інтелектуальна власність активно захищається через поєднання освітніх, інформаційних та профілактичних заходів. Ці ініціативи спрямовані на підвищення обізнаності громадян, підприємців та творчих особистостей щодо важливості захисту прав ІВ. УКРНОІВІ активно проводить освітні кампанії, семінари та вебінари, сприяючи формуванню культури поваги до інтелектуальної власності.

Одним із прикладів ефективної співпраці між державними установами та бізнесом є інформаційна кампанія Trust the Original, ініційована Центром спостереження з питань порушень прав інтелектуальної власності УКРНОІВІ спільно з онлайн-платформою OLX, яка вже згадувалась раніше. Ця кампанія спрямована на інформування споживачів про ризики придбання контрафактної продукції та важливість підтримки легальних виробників. Вона включає в себе освітні матеріали, публікації та інші ресурси. Такі ініціативи сприяють формуванню свідомого споживчого ставлення та підтримують розвиток чесного бізнес-середовища в Україні.

З огляду на успішний досвід співпраці з платформою OLX у межах кампанії Trust the Original, доцільно рекомендувати розширення подібних партнерств з іншими великими онлайн-платформами та маркетплейсами, що діють в Україні. Спільні інформаційні ініціативи з платформами сприяють не лише підвищенню рівня обізнаності споживачів, а й створюють додаткову цінність для самих платформ, оскільки забезпечують підвищення довіри з боку користувачів та зміцнюють їх репутацію.

7. Висновки та рекомендації

7.1. Підсумки дослідження

Онлайн-платформи та маркетплейси відіграють ключову роль у розвитку сучасної електронної комерції, спрощуючи доступ до ринку для продавців і створюючи зручність для споживачів. Водночас, саме ці платформи стають основним середовищем поширення контрафактної продукції та об'єктів, що порушують права інтелектуальної власності.

Проведене дослідження підтверджує:

- Відсутність дієвих бар'єрів для розміщення підробленої продукції на багатьох українських маркетплейсах.
- Недостатній рівень верифікації продавців, низьку прозорість і обмеженість у використанні сучасних технологічних рішень для автоматичного виявлення порушень.
- Обмежене застосування адміністративних, технологічних і судових інструментів для ефективного реагування на порушення прав ІВ в онлайн-середовищі.

- Високий рівень технічної мобільності та організованості шахрайських мереж, здатних швидко адаптуватися до блокувань і обходити наявні системи модерації.

Міжнародний досвід (Amazon, Alibaba, eBay, Nike, Opsydia) демонструє, що запровадження комплексних технологічних рішень, зокрема автоматизованої модерації, аналізу мультіакаунтів, верифікації продавців, впровадження блокчейн і RFID-маркування, а також публічної звітності, є найбільш ефективним шляхом для захисту прав ІВ у цифровому просторі.

Європейський Союз, у рамках впровадження Digital Services Act, встановлює нові вимоги до платформ щодо прозорості, публічної звітності та зобов'язань із забезпечення безпеки електронного ринку. Україна, враховуючи свої євроінтеграційні зобов'язання, має стратегічно рухатися в цьому напрямі, адаптуючи міжнародні практики та поетапно гармонізуючи законодавство.

7.2. Рекомендації для онлайн-платформ

Онлайн-платформи несуть безпосередню відповідальність за якість контенту, що розміщується на їхніх ресурсах. Вони мають можливість створювати технічні та організаційні умови, які або сприятимуть розповсюдженню контрафакту, або, навпаки, ефективно його обмежуватимуть. Саме тому впровадження сучасних систем верифікації, автоматизованої модерації та публічної звітності є ключовою умовою розвитку безпечного онлайн-середовища.

Рекомендації:

- Впровадити алгоритми автоматизованої передпублікаційної модерації товарів, що дозволять виявляти порушення ще до публікації оголошень.
- Запровадити обов'язкову перевірку достовірності даних продавців шляхом верифікації документів, контактів, платіжних реквізитів.
- Встановити системи виявлення пов'язаних акаунтів та шахрайських мереж, зокрема на основі аналізу IP-адрес, пристроїв, платіжних методів і поведінкових патернів.
- Розробити та оприлюднити чіткі правила реагування на скарги, із визначенням строків розгляду та відповідальності за їх порушення.
- Забезпечити регулярну публічну звітність про виявлені порушення, видалені товари та терміни реагування.
- Впровадити технологічні рішення на основі AI, блокчейн і RFID для забезпечення скринінгу товарів і попередження порушень.
- Інтегрувати платформи до міжнародних систем моніторингу, таких як WIPO ALERT, для оперативного виявлення порушень.
- Розглянути можливість участі у пілотних проектах із впровадження цифрового продуктового паспорта (DPP) для товарів високого ризику.
- Забезпечити регулярне навчання контент-модераторів, зокрема у сфері розпізнавання контрафактної продукції.

7.3. Рекомендації для державних органів

Держава виконує системоутворюючу роль у формуванні регуляторного середовища та забезпеченні балансу між розвитком електронної комерції та належним рівнем захисту прав інтелектуальної власності. Законодавчі та адміністративні інструменти, які запроваджує держава, мають забезпечити чіткі вимоги для платформ і ефективну координацію з правоохоронними та митними органами.

Рекомендації:

- Встановити обов'язкові мінімальні вимоги до верифікації продавців для всіх онлайн-платформ, із закріпленням контролюючих механізмів.
- Визначити вимоги до автоматизованої модерації контенту та передбачити відповідальність за їх невиконання.
- Запровадити обов'язкову публічну звітність онлайн-платформ щодо кількості порушень, термінів реагування та ефективності служб модерації.
- Посилити міжвідомчу співпрацю між Державною митною службою, Національною поліцією, судовою владою та платформами для забезпечення оперативного реагування на порушення.
- Розробити нормативну базу для впровадження цифрового продуктового паспорта (DPP), із поступовою гармонізацією з вимогами Digital Services Act.
- Активізувати участь у міжнародних ініціативах: I-SOP (Interpol), WCO, WIPO ALERT, для обміну інформацією та проведення спільних заходів з виявлення і протидії порушенням.
- Забезпечити державну підтримку впровадженню технологічних рішень на платформах, зокрема через консультаційні та інформаційні кампанії.
- Організувати програму підвищення кваліфікації для правоохоронних і митних органів, суддів і контент-модераторів платформ із фокусом на порушення прав ІВ в онлайн-середовищі.

7.4. Рекомендації для правовласників та бізнесу

Правовласники, виробники, постачальники та торговельні компанії є основними зацікавленими сторонами у забезпеченні захисту своїх прав. Їхня активна участь, як у моніторингу, так і в розвитку галузевих стандартів, є критично важливою для ефективного функціонування всієї системи протидії порушенням прав інтелектуальної власності.

Варто враховувати, що в Україні переважно застосовується принцип приватного обвинувачення: ініціювати кримінальне або адміністративне провадження можливо, як правило, лише за заявою правовласника. Це підвищує відповідальність і роль правовласників у своєчасному виявленні порушень та у вжитті заходів для їх припинення.

Рекомендації:

- Регулярно здійснювати моніторинг власних брендів на маркетплейсах і в соціальних мережах.
- Активно використовувати механізми подання скарг на онлайн-платформах та слідкувати за ефективністю їх розгляду.
- Впроваджувати технологічні рішення для маркування продукції: RFID-мітки, QR-коди, цифрові сертифікати, блокчейн-рішення для підтвердження автентичності.
- Розвивати власні юридичні та технічні служби захисту бренду, зокрема для оперативного реагування на порушення.
- Брати участь у формуванні галузевих стандартів та кодексів етики у сфері електронної комерції, ініціювати саморегулювання в галузі.