АДМІНІСТРАТИВНЕ ПРАВО І ПРОЦЕС; ФІНАНСОВЕ ПРАВО; ІНФОРМАЦІЙНЕ ПРАВО

УДК 347.77:004.056
DOI https://doi.org/10.32782/TNU-2707-0581/2026.3/13

Гнедюк В. Л.
https://orcid.org/0009-0007-8025-0876
Український науково-дослідний інститут спеціальної техніки та судових експертиз
Служби безпеки України

ЗАХИСТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ (ЮРИДИЧНІ АСПЕКТИ ЗАХИСТУ ВІД ВИТОКІВ ТА ЗЛОМІВ)

У статті здійснено комплексний аналіз юридичних аспектів захисту прав інтелектуальної власності від витоків інформації та несанкціонованих втручань в інформаційно-комунікаційні системи в межах чинного законодавства України. Досліджено теоретико-правові засади охорони інтелектуальної власності відповідно до положень Книги четвертої Цивільного кодексу України та спеціального законодавства у сфері авторського права й захисту інформації. Обґрунтовано, що в умовах цифровізації значна частина об'єктів інтелектуальної власності існує в електронній формі, що підвищує ризики їх незаконного отримання, копіювання, модифікації та поширення.

Проаналізовано правову природу комп'ютерних програм і баз даних як об'єктів авторського права, а також особливості правового режиму комерційної таємниці. Встановлено, що витік інформації за наявності об'єкта права інтелектуальної власності набуває значення юридичного факту, який може спричиняти цивільно-правові та кримінально-правові наслідки залежно від характеру посягання.

Окрему увагу приділено кримінально-правовим механізмам захисту, передбаченим Кримінальним кодексом України, зокрема щодо порушення авторського права, несанкціонованого втручання в роботу інформаційних систем та незаконного збирання відомостей, що становлять комерційну таємницю. Розкрито проблеми розмежування складів злочинів, доведення факту незаконного доступу та встановлення розміру завданої шкоди. Висвітлено значення цивільно-правових способів захисту та превентивних механізмів, зокрема впровадження режиму комерційної таємниці, укладення договорів про нерозголошення та належного документування режиму доступу до інформації.

Зроблено висновок про міжгалузевий характер системи захисту інтелектуальної власності в цифровому середовищі та необхідність удосконалення процесуальних механізмів роботи з електронними доказами й гармонізації національного законодавства з сучасними викликами кібербезпеки.

Ключові слова: *інтелектуальна власність, витік інформації, несанкціоноване втручання, комерційна таємниця, комп'ютерна програма, цивільно-правовий захист.*

Постановка проблеми. Цифровізація суспільних відносин та зростання ролі нематеріальних активів у структурі національної економіки істотно підвищили значення інтелектуальної власності як об'єкта правової охорони. Значна частина результатів інтелектуальної, науково-технічної та творчої діяльності функціонує в електронній формі та обертається в межах інформаційно-комунікаційних систем, що водночас зумовлює підвищені ризики їх незаконного отримання, копіювання, модифікації та поширення.

Чинне законодавство України, зокрема положення Цивільного кодексу України, Закону України «Про авторське право і суміжні права», а також

норми кримінального законодавства щодо несанкціонованого втручання в роботу інформаційних систем, формує нормативну основу охорони прав інтелектуальної власності. Проте зростання кількості витоків інформації, зломів інформаційно-комунікаційних систем і незаконного використання програмного забезпечення та комерційної таємниці свідчить про наявність практичних проблем у сфері їх правозастосування.

Особливої актуальності набувають питання належної юридичної кваліфікації таких посягань, визначення об'єкта порушення, доведення факту незаконного доступу та встановлення розміру завданої шкоди. Ускладнення викликає також недостатня регламентація внутрішніх режимів захисту конфіденційної інформації суб'єктами господарювання, що знижує ефективність судового захисту.

У зв'язку з цим виникає потреба у комплексному дослідженні юридичних аспектів захисту інтелектуальної власності від витоків та зломів у межах чинного законодавства України з метою удосконалення механізмів правової охорони відповідних об'єктів в умовах сучасних кіберзагроз.

Аналіз останніх досліджень і публікацій. Проблематика захисту прав інтелектуальної власності в умовах цифровізації та зростання кіберзагроз активно досліджується у сучасній юридичній науці. У працях I. Babetska [5] та A. Polishchuk [8] акцентується увага на необхідності вдосконалення системи захисту інтересів правовласників та гармонізації національного законодавства з європейськими стандартами. V. Cherneha [6] аналізує механізм правового регулювання відносин у сфері інтелектуальної власності та співвідношення цивільно-правових і публічно-правових засобів охорони.

Окремий напрям досліджень представлений у роботі A. Loianych [7], де розглядаються проблеми застосування чинного законодавства до об'єктів, створених із використанням штучного інтелекту, що ускладнює визначення суб'єктів права та меж правової охорони в цифровому середовищі. Питання кримінально-правового захисту та доказування несанкціонованих втручань у кіберпросторі висвітлено у праці V. Tarasenko [3], який звертає увагу на складність фіксації електронних доказів і розмежування складів злочинів.

Нормативну основу досліджень становлять положення Цивільного кодексу України [4], Закону України «Про авторське право і суміжні права» [2] та Кримінального кодексу України [1]. Водночас комплексний аналіз витоків інформації та зломів як форм порушення прав інтелектуальної власності з урахуванням міжгалузевого характеру правового регулювання потребує подальшого наукового опрацювання.

Постановка завдання. Метою статті є комплексний аналіз юридичних механізмів захисту інтелектуальної власності від витоків інформації та несанкціонованих втручань у цифровому середовищі в межах чинного законодавства України.

Для досягнення цієї мети поставлено такі завдання:

– дослідити теоретико-правові засади охорони інтелектуальної власності в умовах цифровізації;

– проаналізувати правову природу витоків інформації та зломів як форм порушення прав інтелектуальної власності;

– охарактеризувати кримінально-правові та цивільно-правові способи захисту у випадках незаконного доступу до охоронюваної інформації;

– визначити роль превентивних механізмів у мінімізації ризиків витоків;

– окреслити проблемні питання правозастосування та сформулювати напрями їх вирішення.

Виклад основного матеріалу дослідження. Правове регулювання відносин у сфері інтелектуальної власності в Україні ґрунтується на положеннях Книги четвертої Цивільного кодексу України. Відповідно до статті 418 ЦК України право інтелектуальної власності становить право особи на результат інтелектуальної, творчої діяльності або на інший об'єкт, визначений законом. Таким чином, інтелектуальна власність у національній правовій системі розглядається як сукупність особистих немайнових та майнових прав [4].

Особисті немайнові права забезпечують правовий зв'язок автора з результатом творчої діяльності, тоді як майнові права надають можливість дозволяти чи забороняти використання об'єкта та отримувати винагороду. Нематеріальний характер об'єктів інтелектуальної власності зумовлює їх економічну вразливість у разі відсутності належного правового захисту.

Відповідно до Закону України «Про авторське право і суміжні права» комп'ютерні програми та бази даних охороняються як літературні твори. Такий підхід забезпечує їм повний обсяг авторсько-правового захисту, однак цифрова форма існування цих об'єктів підвищує ризики несанкціонованого доступу та копіювання [2].

Правовий режим комерційної таємниці визначається статтею 505 Цивільного кодексу України. Інформація визнається комерційною таємницею

за умови її секретності, наявності комерційної цінності та вжиття адекватних заходів щодо збереження конфіденційності. Відтак правова охорона залежить від належного встановлення режиму доступу до відповідної інформації та її документального закріплення у внутрішніх актах суб'єкта господарювання [4].

Інтелектуальна власність у цифровому середовищі перебуває на перетині цивільного та інформаційного законодавства. Оскільки значна частина об'єктів функціонує в електронній формі та зберігається в інформаційно-комунікаційних системах, зростає ризик їх незаконного отримання, копіювання або модифікації. Саме ця обставина зумовлює необхідність правової оцінки відповідних посягань у межах чинного законодавства України.

У цьому контексті витоки інформації та несанкціоновані втручання в інформаційно-комунікаційні системи підлягають кваліфікації з урахуванням правового режиму об'єкта, на який спрямоване посягання. Вирішальним є не лише факт технічного доступу до інформації, а й характер прав, що охороняються законом щодо відповідного результату інтелектуальної діяльності.

Зокрема, несанкціонований доступ до комп'ютерної програми, її копіювання або модифікація без згоди правовласника становлять порушення майнових прав автора чи іншого суб'єкта авторського права відповідно до Закону України «Про авторське право і суміжні права». Оскільки комп'ютерна програма охороняється як літературний твір, будь-яке відтворення або інше використання поза межами встановлених законом винятків потребує дозволу правовласника. Відсутність такого дозволу трансформує технічну дію у правопорушення у сфері інтелектуальної власності.

Аналогічний підхід застосовується до баз даних. Незаконне копіювання їх структури або змісту, якщо така база охороняється як об'єкт авторського права чи як складений твір, порушує виключні майнові права. Водночас у разі, коли база даних містить інформацію з обмеженим доступом, відповідні дії можуть поєднувати порушення авторських прав із порушенням режиму конфіденційності.

Незаконне отримання технологічної документації, виробничих алгоритмів або іншої інформації, що перебуває під режимом комерційної таємниці, утворює посягання на права інтелектуальної власності. У цьому випадку правова кваліфікація дій залежить від доведеності встановлення такого режиму та факту його порушення [6, с. 63].

Правове регулювання зазначених відносин має міжгалузевий характер. Закон України «Про авторське право і суміжні права» визначає обсяг виключних прав та способи їх захисту; Закон України «Про захист інформації в інформаційно-комунікаційних системах» встановлює організаційні та технічні засади охорони інформації; норми Кримінального кодексу України передбачають відповідальність за несанкціоноване втручання в роботу інформаційних систем та незаконне використання об'єктів інтелектуальної власності.

Таким чином, витік інформації не може розглядатися виключно як технічний інцидент або наслідок кіберзагрози. За наявності об'єкта права інтелектуальної власності він набуває значення юридичного факту, що породжує цивільно-правові, а за певних умов і кримінально-правові наслідки. Саме це зумовлює необхідність детального аналізу юридичної кваліфікації відповідних правопорушень та визначення меж відповідальності суб'єктів, причетних до незаконного доступу чи розповсюдження охоронюваної інформації [8, с. 74–75].

Оскільки витоки інформації та несанкціоновані втручання можуть набувати ознак суспільно небезпечних діянь, що посягають на охоронювані законом права інтелектуальної власності, виникає необхідність аналізу механізмів кримінально-правового реагування. У зв'язку з цим доцільно звернутися до положень Кримінального кодексу України, які встановлюють відповідальність за відповідні порушення у цифровому середовищі.

Кримінально-правовий захист інтелектуальної власності виступає найбільш суворим засобом реагування держави на посягання, що завдають істотної шкоди майновим та немайновим правам правовласників. У цифровому середовищі витоки інформації та несанкціоновані втручання в інформаційно-комунікаційні системи можуть набувати ознак кримінально караних діянь за умови наявності передбачених законом об'єктивних і суб'єктивних ознак складу злочину.

Кримінальний кодекс України містить низку норм, спрямованих на охорону прав інтелектуальної власності як безпосередньо, так і опосередковано через захист інформаційної безпеки та режиму конфіденційності. Для систематизації кримінально-правових норм, що забезпечують захист прав інтелектуальної власності, доцільно узагальнити їх безпосередній об'єкт посягання та зміст кримінально караного діяння (табл. 1).

Практичне застосування зазначених норм пов'язане з необхідністю чіткого розмежування

Таблиця 1

Кримінально-правові норми, що забезпечують захист прав інтелектуальної власності

Норма КК України	Об'єкт посягання	Суть кримінально караного діяння	Значення для захисту ІВ
Стаття 176	Авторські та суміжні права	Незаконне відтворення, розповсюдження, інше використання творів, комп'ютерних програм, баз даних	Безпосередній захист майнових прав інтелектуальної власності
Стаття 361	Безпека інформаційно-комунікаційних систем	Несанкціоноване втручання в роботу ІКС, що призводить до витоку, блокування чи модифікації інформації	Охорона цифрового середовища, в якому існують об'єкти ІВ
Стаття 361–2	Інформація з обмеженим доступом	Незаконний збут або розповсюдження інформації, отриманої шляхом несанкціонованого доступу	Захист конфіденційної інформації, зокрема комерційної таємниці
Стаття 231	Комерційна таємниця	Незаконне збирання або використання відомостей з метою заподіяння шкоди суб'єкту господарювання	Кримінально-правова охорона режиму комерційної таємниці

складів злочинів та доведення їх обов'язкових елементів. Особливого значення набуває встановлення:

– факту незаконного доступу до інформаційних ресурсів;

– наявності об'єкта права інтелектуальної власності або режиму комерційної таємниці;

– розміру заподіяної матеріальної шкоди;

– причинно-наслідкового зв'язку між діянням і наслідками.

Недостатність доказової бази або помилки у визначенні об'єкта посягання можуть призвести до перекваліфікації діяння або відмови у притягненні до кримінальної відповідальності. Це свідчить про необхідність комплексного підходу до фіксації цифрових доказів та належного документування режиму охорони інформації [1].

Отже, кримінально-правові механізми відіграють ключову роль у системі захисту інтелектуальної власності від зломів і витоків інформації, забезпечуючи реагування на найбільш небезпечні форми порушень. Водночас кримінальна відповідальність є крайньою формою державного впливу та застосовується за наявності всіх ознак складу злочину. Її реалізація не виключає можливості паралельного використання цивільно-правових способів захисту, що у сукупності забезпечують цілісну систему правової охорони.

Оскільки кримінально-правові засоби застосовуються лише за наявності складу злочину та мають характер крайнього державного реагування, ефективний захист прав інтелектуальної власності потребує використання ширшого спектра юридичних інструментів. У цьому контексті особливого значення набувають цивільно-правові способи захисту, а також превентивні механізми мінімізації ризиків витоків і несанкціонованих втручань.

Цивільно-правовий захист прав інтелектуальної власності ґрунтується на загальних положеннях статті 16 Цивільного кодексу України, відповідно до яких кожна особа має право на судовий захист свого порушеного, невизнаного або оспорюваного права. У сфері інтелектуальної власності зазначене положення конкретизується спеціальними нормами цивільного законодавства, що передбачають можливість застосування різних способів захисту залежно від характеру порушення [4].

У разі витоку інформації або несанкціонованого втручання правовласник вправі вимагати визнання свого права, припинення порушення, відшкодування завданої майнової шкоди, стягнення компенсації, а також вилучення та знищення контрафактних матеріалів чи незаконно виготовлених копій. Вибір конкретного способу захисту залежить від обставин справи, обсягу завданої шкоди та можливості її доведення.

Особливого значення набуває проблема доказування факту витоку та визначення розміру шкоди. У практиці це пов'язано з необхідністю проведення комп'ютерно-технічних експертиз, аналізу електронних журналів доступу, встановлення вартості нематеріальних активів та оцінки втраченої вигоди. Відсутність належної фіксації порушення або документального підтвердження правового режиму інформації істотно ускладнює реалізацію права на судовий захист.

Таким чином, цивільно-правові механізми забезпечують відновлення порушених прав та компенсацію заподіяної шкоди, доповнюючи кримінально-правову охорону та забезпечуючи багаторівневу систему правового реагування на посягання у цифровому середовищі [3, с. 315].

Запобігання витокам інформації та зломам інформаційно-комунікаційних систем є ключовим

елементом системи охорони інтелектуальної власності. Превентивна складова ґрунтується на поєднанні норм цивільного, трудового та інформаційного законодавства з практикою корпоративного управління.

Насамперед ідеться про запровадження режиму комерційної таємниці шляхом визначення переліку відомостей, що підлягають охороні, встановлення порядку доступу до них та закріплення відповідних положень у внутрішніх нормативних актах. Не менш важливим є укладення договорів про нерозголошення (NDA), а також включення до трудових договорів умов щодо збереження конфіденційної інформації та відповідальності за її розголошення.

Додатково значення мають організаційні заходи, зокрема регламентація доступу до інформаційних ресурсів, розмежування повноважень працівників, ведення обліку електронних операцій та застосування технічних засобів захисту. Належне документальне оформлення режиму охорони інформації є передумовою ефективного судового захисту, оскільки саме воно підтверджує наявність об'єкта правової охорони та факт порушення встановлених правил.

Таким чином, превентивні механізми не лише зменшують імовірність посягань, а й створюють доказову основу для подальшого захисту прав у разі їх порушення [5, с. 201].

Незважаючи на наявність нормативно визначених способів захисту, правозастосовна практика у сфері протидії витокам та несанкціонованим втручанням характеризується низкою системних труднощів, зокрема складністю доведення факту незаконного доступу, встановлення юрисдикції у випадках транскордонних кіберправопорушень, ідентифікації правопорушників, а також визначення розміру завданої майнової та нематеріальної шкоди. Додаткові ускладнення пов'язані з недостатньою процесуальною регламентацією фіксації та дослідження цифрових доказів. Вирішення зазначених проблем потребує удосконалення процесуальних механізмів роботи з електронними доказами, нормативного уточнення методик оцінки збитків від порушення прав інтелектуальної власності, розвитку міжнародного співробітництва у сфері кібербезпеки, а також запровадження уніфікованих стандартів документування режиму охорони конфіденційної інформації на рівні суб'єктів господарювання. Реалізація цих векторів сприятиме підвищенню ефективності правового захисту інтелектуальної власності в умовах цифрової трансформації [7, с. 8–9].

Висновки. Проведений аналіз засвідчує, що захист інтелектуальної власності від витоків інформації та несанкціонованих втручань у цифровому середовищі має міжгалузевий характер і здійснюється шляхом поєднання цивільно-правових, кримінально-правових і превентивних механізмів. Витік інформації за наявності об'єкта права інтелектуальної власності набуває значення юридичного факту, що потребує належної кваліфікації з урахуванням об'єкта посягання та розміру шкоди. Ефективність захисту залежить від належного документування режиму охорони інформації, якості фіксації цифрових доказів і чіткого розмежування складів правопорушень, що зумовлює потребу вдосконалення нормативних і процесуальних механізмів реагування на кіберпосягання.

Подальші наукові розвідки доцільно спрямувати на розроблення методик оцінки збитків від цифрових порушень прав інтелектуальної власності, удосконалення процесуальних стандартів роботи з електронними доказами, а також на дослідження моделей гармонізації національного законодавства з міжнародними підходами у сфері кібербезпеки та охорони конфіденційної інформації.

Список літератури:

1. Кримінальний кодекс України: Закон України №2341-III від 05.04.2001. URL: https://zakon.rada.gov.ua/laws/show/2341–14#Text (дата звернення: 24.02.2026).

2. Про авторське право і суміжні права: Закон України №2811-IX від 01.12.2022. URL: https://zakon. rada.gov.ua/laws/show/2811–20#Text (дата звернення: 25.02.2026).

3. Тарасенко В. О. Правовий механізм захисту прав інтелектуальної власності в кіберпросторі. *Юридичний науковий електронний журнал.* 2025. № 6. С. 313–316. DOI: https://doi.org/10.32782/2524–0374/2025–6/63

4. Цивільний кодекс України: Закон України № 435-IV від 16.01.2003. URL: https://zakon. rada.gov.ua/laws/show/435–15 (дата звернення: 24.02.2026).

5. Babetska I. System of protection of the interests of intellectual property subjects. *Visegrad Journal on Human Rights*. 2025. № 2. P. 199–205. DOI: https://doi.org/10.61345/1339–7915.2025.2.28

6. Cherneha V. Mechanizm for legal regulation of intellectual property relations in Ukraine. *Юридичний вісник.* 2023. № 3. С. 59–71. DOI: https://doi.org/10.32782/yuv. v3.2023.8

7. Loianych A. Problem issues of applying current legal regulations to AI-created objects. Entrepreneurship. *Economy and Law*. № 2. P. 5–10. DOI: https://doi.org/10.32849/2663–5313/2024.2.01

8. Polishchuk A. Consideration of intellectual property law in the context of European Union practice. *Law. Human. Environment*. 2024. № 15 (1). С. 70–84. DOI: https://doi.org/10.31548/law/1.2024.70

Gnediuk V. L. PROTECTION OF INTELLECTUAL PROPERTY (LEGAL ASPECTS OF PROTECTION AGAINST LEAKS AND HACKING)

T*he article provides a comprehensive analysis of the legal aspects of protecting intellectual property rights against information leaks and unauthorized interference in information and communication systems within the framework of the current legislation of Ukraine. The theoretical and legal foundations of intellectual property protection are examined in accordance with Book Four of the Civil Code of Ukraine and special legislation in the field of copyright and information protection. It is substantiated that in the context of digitalization, a significant proportion of intellectual property objects exist in electronic form, which increases the risks of their unlawful acquisition, copying, modification, and dissemination.*

The legal nature of computer programs and databases as objects of copyright is analyzed, along with the specific features of the legal regime of trade secrets. It is established that an information leak, where an intellectual property object is involved, acquires the status of a legal fact that may entail civil and criminal liability depending on the nature of the infringement.

Particular attention is paid to criminal law mechanisms of protection provided by the Criminal Code of Ukraine, including violations of copyright, unauthorized interference with information systems, and unlawful collection of information constituting a trade secret. The article highlights the issues of distinguishing between elements of criminal offenses, proving unauthorized access, and determining the amount of damage caused. It also emphasizes the importance of civil law remedies and preventive mechanisms, including the establishment of a trade secret regime, the conclusion of non-disclosure agreements (NDAs), and proper documentation of information access procedures.

The study concludes that the system of intellectual property protection in the digital environment has an intersectoral nature and requires further improvement of procedural mechanisms for handling electronic evidence, as well as harmonization of national legislation with contemporary cybersecurity challenges.

Keywords: *intellectual property, information leak, unauthorized interference, trade secret, computer program, civil law protection.*

Дата першого надходження статті до видання: 01.04.2026
Дата прийняття статті до друку після рецензування: 06.05.2026
Дата публікації (оприлюднення) статті: 30.05.2026