

ПРАВОВИЙ МЕХАНІЗМ ЗАХИСТУ ПРАВ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В КІБЕРПРОСТОРИ

LEGAL MECHANISM FOR PROTECTING INTELLECTUAL PROPERTY RIGHTS IN CYBERSPACE

Тарасенко В.О.,
магістр права

Сучасний світ переживає цифрову трансформацію, що докорінно змінює традиційні суспільні відносини. Кіберпростір, який ще нещодавно сприймався як допоміжне середовище, став повноцінним полем для економічної, соціальної та культурної діяльності. У цьому контексті захист прав інтелектуальної власності набуває особливого значення, оскільки цифрові технології, з одного боку, відкривають безпрецедентні можливості для створення й поширення творів, а з іншого – створюють нові виклики для їх правового захисту.

Стрімкий розвиток інформаційно-комунікаційних технологій, поширення соціальних мереж, хмарних сервісів та інших інструментів призвели до масового обігу об'єктів інтелектуальної власності в мережі. Це значно спрощує доступ до контенту, але водночас робить його надзвичайно вразливим до неправомірного використання, включаючи піратство, незаконне копіювання, поширення та інші форми порушень. Існуючі національні правові системи, що формувалися в епоху аналогових технологій, часто виявляються не готовими до адекватного реагування на ці виклики. Транскордонний характер кіберпростору, відсутність чітких територіальних меж, анонімність порушників і надзвичайно висока швидкість поширення контенту вимагають переосмислення традиційних підходів до захисту прав.

Таким чином, актуальність теми обумовлена необхідністю розробки ефективних правових механізмів, які б враховували специфіку цифрового середовища. Дослідження правових інструментів захисту інтелектуальної власності в кіберпросторі є не лише теоретично значущим, але й має важливе практичне значення. Воно дозволить виявити прогалини в чинному законодавстві та запропонувати конкретні шляхи вдосконалення регулювання. Це, своєю чергою, сприятиме стимулюванню інновацій, захисту інтересів правласників та забезпеченню правової стабільності в умовах цифрової економіки.

Ключові слова: інтелектуальна власність, кіберпростір, правовий захист, кібербезпека, кіберзлочинність, авторське право, промислова власність.

The modern world is undergoing a digital transformation that is fundamentally changing traditional social relations. Cyberspace, which was recently perceived as an auxiliary environment, has become a full-fledged field for economic, social and cultural activities. In this context, the protection of intellectual property rights is of particular importance, since digital technologies, on the one hand, open up unprecedented opportunities for the creation and distribution of works, and on the other hand, create new challenges for their legal protection. The rapid development of information and communication technologies, the spread of social networks, cloud services and other tools have led to the mass circulation of intellectual property objects on the network. This greatly simplifies access to content, but at the same time makes it extremely vulnerable to misuse, including piracy, illegal copying, distribution and other forms of infringement. Existing national legal systems, which were formed in the era of analogue technologies, often turn out to be unprepared to adequately respond to these challenges. The cross-border nature of cyberspace, the lack of clear territorial boundaries, the anonymity of violators and the extremely high speed of content distribution require a rethinking of traditional approaches to the protection of rights.

Thus, the relevance of the topic is due to the need to develop effective legal mechanisms that would take into account the specifics of the digital environment. The study of legal instruments for the protection of intellectual property in cyberspace is not only theoretically significant, but also has important practical significance. It will identify gaps in the current legislation and suggest specific ways to improve regulation. This, in turn, will help stimulate innovation, protect the interests of rightholders and ensure legal stability in the digital economy.

Key words: intellectual property, cyberspace, legal protection, cybersecurity, cybercrime, copyright, industrial property.

Постановка проблеми. Розвиток інформаційно-комунікаційних технологій та розширення глобального кіберпростору докорінно змінили умови створення, поширення та захисту об'єктів інтелектуальної власності. Технології, такі як штучний інтелект (ШІ), хмарні сховища, блокчейн та Інтернет речей (IoT), стали не лише інструментами для інновацій, але й джерелом нових загроз. Об'єкти ІВ, що існують у цифровій формі, легко копіюються, модифікуються та поширюються, що робить традиційні правові механізми недостатньо ефективними. Тенденція щодо зростання кіберзлочинності, створює критичну необхідність посилення правового захисту.

Метою статті є дослідження сучасного правового механізму захисту прав інтелектуальної власності у кіберпросторі.

Стан дослідження. Проблема правового захисту інтелектуальної власності у кіберпросторі активно досліджується як в Україні, так і за її межами. Важливий внесок у розробку теоретичних та практичних аспектів цієї тематики зробили такі українські науковці-правники: О. Д. Зайчук, В. С. Ковальський, Р. А. Майданник, О. О. Дуда, С. Д. Лучик, В. Є. Лучик, І. М. Корнілова. О. Д. Зайчук, у своїх працях, акцентує увагу на загальних питаннях інтелектуальної власності. В. С. Ковальський досліджує авторське право. Праці Р. А. Майданника присвячені цивільно-правовим аспектам інтелектуальної

власності. О. О. Дуда зосереджує увагу на проблемах кіберзлочинності. Окремі аспекти кібербезпеки та захисту ІВ у сучасних умовах висвітлюються в роботах С. Д. та В. Є. Лучиків, а питання кіберпромислового шпигунства – у працях І. М. Корнілової. Така кількість наукових праць свідчить про значну увагу наукової спільноти до цієї проблематики.

Виклад основного матеріалу. Цифрова трансформація призвела до еволюції самого поняття інтелектуальної власності. Якщо раніше об'єкти ІВ існували переважно у матеріальній формі, то сьогодні вони здебільшого є нематеріальними активами. Наприклад, програмне забезпечення, бази даних, цифровий контент, алгоритми ШІ та об'єкти, що створюються за його допомогою, вимагають нових підходів до правового регулювання. Захист цих об'єктів у кіберпросторі стикається з низкою фундаментальних проблем.

Відповідно до положень статті 418 Цивільного кодексу України право інтелектуальної власності – це право особи на результат інтелектуальної, творчої діяльності або на інший об'єкт права інтелектуальної власності [1].

Згідно із нормами статті 420 Цивільного кодексу України до об'єктів права інтелектуальної власності належать:

- літературні та художні твори;
- комп'ютерні програми;
- компіляції даних (бази даних);

- виконання;
- фонограми, відеограми, програми організацій мовлення;
- наукові відкриття;
- винаходи, корисні моделі, промислові зразки;
- компонування напівпровідникових виробів;
- раціоналізаторські пропозиції;
- сорти рослин, породи тварин;
- комерційні (фірмові) найменування, торговельні марки (знаки для товарів і послуг), географічні зазначення;
- комерційні таємниці.

Інтернет не має фізичних кордонів, що ускладнює застосування національних законів. Порушник може знаходитися в одній країні, а об'єкт ІВ – в іншій, що створює конфлікт юрисдикцій. Зловмисники часто використовують анонімні мережі та інструменти, щоб приховати свою особистість, що ускладнює їх притягнення до відповідальності. Цифровий контент може бути скопійований та поширений у масових масштабах за лічені секунди, що робить реакцію правоохоронних органів запізнілою.

Сучасний кіберпростір є ареною для різноманітних кіберзлочинів, що безпосередньо загрожують правам ІВ. Ці загрози є більш витонченими та масштабними, ніж традиційні злочини, і вимагають комплексних заходів захисту.

Слід зауважити, що один із найнебезпечніших видів правопорушень у кіберпросторі щодо інтелектуальної власності – це кіберпромислове шпигунство. Кіберпромислове шпигунство – це свідоме незаконне, неетичне, несанкціоноване отримання у кіберпросторі неавторизованим користувачем доступу до комерційної таємниці на користь приватних структур для отримання конкурентних переваг, економічної вигоди. На відміну від звичайного шпигунства, кіберпромислове шпигунство використовує методи, як-от злам комп'ютерних мереж, встановлення шкідливого програмного забезпечення, що дозволяє непомітно отримувати доступ до конфіденційної інформації. Це є серйозною загрозою для конкурентоспроможності компаній та національної безпеки [12, с. 248–249].

Сучасний фішинг є одним із найпоширеніших методів викрадення облікових даних. Кіберзлочинці використовують різні методи, які обманним шляхом змушують співробітників компаній надавати доступ до особистих або корпоративних даних, наприклад, паролів або номерів кредитних карток. Для цього вони використовують електронну пошту, текстові повідомлення та телефонні дзвінки. За допомогою фішингу зловмисники доставляють вірусні програми в ІТ-системи компанії. Протягом 2022 року кількість російських спроб фішингу проти України зросла на 250%. Найбільш потужні кібератаки були здійснені в перші чотири місяці 2022 року. Основною їх ціллю стали понад 150 державних установ і головному мішенню було Міністерство оборони України. Після здійснення фішингових атак, російські хакери використовували шкідливе програмне забезпечення «wirep», за допомогою якого намагалися стерти критичні дані. Основним методом боротьби з фішингом є кібергігієна співробітників [9, с. 874].

Несанкціоноване копіювання, розповсюдження та використання цифрового контенту (фільми, музика, книги, програмне забезпечення) є однією з найпоширеніших форм кіберзлочинності.

Для ефективного захисту ІВ у кіберпросторі необхідне скоординоване міжнародне співробітництво. Система міжнародних договорів та інституцій є основою цього механізму, але вимагає адаптації до сучасних викликів.

Варто зауважити, що одним із найважливіших міжнародних документів щодо захисту прав ІВ у кіберпросторі є Угода про торговельні аспекти прав інтелектуальної власності (TRIPS). Вона встановлює мінімальні

стандарти захисту ІВ для країн-членів Світової організації торгівлі (СОТ) та є основою для багатьох національних законодавств. Слід підкреслити, що окрім Угоди про торговельні аспекти прав інтелектуальної власності важливе значення також відіграють Бернська конвенція та Паризька конвенція, які регулюють захист авторського права та промислової власності відповідно.

Попри важливість цих договорів для встановлення міжнародних стандартів, залишаються проблеми з їх імплементацією на національному рівні. Багато країн, що розвиваються, і найменш розвинених країн відчувають труднощі з приведенням свого внутрішнього законодавства у відповідність до міжнародних зобов'язань через обмежені правові, технічні та фінансові можливості. Відмінності в правових традиціях, інституційних структурах та рівнях економічного розвитку ще більше ускладнюють цей процес. У деяких випадках упровадження міжнародних норм призводить до правової невизначеності або неузгодженості з чинним національним законодавством. Застосування міжнародних стандартів часто вимагає не лише внесення змін до законодавства, але і створення або реформування судових та адміністративних інституцій, що може перевищувати ресурсні можливості деяких країн [10].

Важливо зазначити, що у захисті прав інтелектуальної власності у кіберпросторі важливу роль відіграють міжнародні організації. Всесвітня організація інтелектуальної власності (ВОІВ) відіграє центральну роль у гармонізації міжнародного законодавства та наданні послуг з міжнародної реєстрації об'єктів ІВ. Європейський Союз також активно працює над створенням єдиних правил, наприклад, через Загальний регламент про захист даних (GDPR) та Акт про кіберстійкість (Cyber Resilience Act), які впливають на захист даних та ІВ в Європі.

ЄС розробив одну з найбільш розвинених та інтегрованих регіональних систем захисту інтелектуальної власності. У рамках своєї внутрішньої ринкової політики ЄС гармонізує законодавство у сфері інтелектуальної власності в державах-членах за допомогою директив і регламентів, як-от Регламент ЄС про торговельні марки та Регламент Співтовариства про промислові зразки. Заснування Відомства інтелектуальної власності ЄС (EUIPO) в Аліканте (Іспанія) сприяло централізованій процедурі реєстрації торговельних марок і промислових зразків, що діє на території всього Євросоюзу. Підхід ЄС ґрунтується на забезпеченні балансу між захистом прав власників та суспільними інтересами, особливо в таких сферах, як авторське право, фармацевтика та географічні зазначення. До того ж ЄС бере активну участь у міжнародних переговорах, роблячи свій внесок у розвиток глобальних норм інтелектуальної власності, забезпечуючи при цьому узгодженість зі своїм внутрішнім правопорядком [10].

Попри наявність міжнародних рамок, існують значні проблеми з їх імплементацією та правозастосуванням. Різні правові системи, юрисдикційні бар'єри та відсутність єдиних механізмів притягнення до відповідальності ускладнюють боротьбу з кіберзлочинами.

Одним з проявів комп'ютерної злочинності є порушення авторських прав, що включає несанкціоноване використання, створення та розповсюдження копій програмного забезпечення, несанкціонований продаж і незаконне копіювання інформації з вебсайтів або блогів за допомогою незаконних дій, таких як посилення та фрейми. Посилання (лінкінг, гіперлінкінг) забезпечує розміщення у структурі вебсайту елементів програмного коду, які дають можливість перейти на сторінку іншого вебсайту або переглядати її вміст без переходу на цю сторінку. В залежності від способу вбудови посилання в «тіло» сайту, є такі різновиди лінкінгу як звичайний лінкінг (розміщення на сайті гіперпосилання на стартову

сторінку іншого вебсайту) та діп лінкінг (розміщення гіперпосилання на будь-яку сторінку іншого вебсайту, крім стартової). До різновидів лінкінгу відносять ембедінг або інлайн лінкінг, який забезпечує включення частини коду іншої сторінки таким чином, що окремий об'єкт іншої сторінки (зображення, відео) відображається без потреби переходу на інший сайт. А також фреймінг («framing»), який включає цілі сторінки інших вебсайтів в окремі «фрейми» (секції), які не перетинаються між собою. Отже, при використанні посилань HTTP протокол не бачить відмінності між діп лінками, як не бачить різниці і між звичайним лінком та діплінком, оскільки технічно всі лінки є рівними. Однак такий підхід вводить в оману, що ці два веб-сайти, наприклад, мають однаковий домен і право власності. Також дозволяє переглядати контент без перегляду реклами на сайті. Фреймінг дозволяє користувачам лише отримувати доступ до захищеного авторським правом вмісту веб-сайту в браузері, який використовує користувач. Проте фреймери не несуть відповідальності за відтворення, передачу чи розповсюдження вмісту, захищеного авторським правом [9, с. 875].

Значну шкоду безпеці інформації компаній наносять так звані інсайдерські атаки. Інсайдерськими вважають спрямовані дії мотивованих суб'єктів, які мають легітимний доступ до інформаційних активів та навички для здобуття цінної інформації, знають уразливі місця інформаційних систем і бізнес-процесів, для завдання матеріальних збитків та/або репутаційних втрат організації. Такими мотивованими суб'єктами є працівники, колишні працівники, ділові партнери компанії. Дії інсайдерів можуть носити як злісний, навмисний, так і ненавмисний характер, тому їх важко передбачити і знешкодити. Через це фахівці оцінюють інсайдерські загрози як унікальний виклик для кібербезпеки, хоча за даними CERT Insider Threat Center, 75% інсайдерських дій залишаються непоміченими. Інсайдери мають набагато більше можливостей, ніж сторонні зловмисники, оскільки вони мають розширений доступ до систем і даних організації, щоб виконувати свою роботу. Також інсайдери в переважній більшості ознайомлені із заходами та процедурами безпеки свого роботодавця та можуть їх обійти. Відповідно до звіту ESET про витіки даних за 2023 рік, 19% із приблизно 5200 витоків даних були спричинені діями персоналу. У іншому дослідженні за 2022 рік кількість цих подій перевищила 6800, а організації витратили близько 15,4 мільйона доларів на рік на усунення наслідків [9, с. 875–874].

Україна робить значні кроки для адаптації свого законодавства до міжнародних стандартів та викликів кіберпростору. Захист ІВ в Україні регулюється низкою законів.

Закон України «Про авторське право і суміжні права» є основним нормативно-правовим актом, що регулює відносини у сфері авторського права. Цей закон адаптує українське законодавство до стандартів ЄС. Також важливими є Закони України «Про охорону прав на промислові зразки» та «Про охорону прав на винаходи та корисні моделі».

Варто зауважити, що українське законодавство передбачає як кримінальну, так і адміністративну відповідальність за порушення прав на об'єкти ІВ, особливо якщо це було вчинено з використанням комп'ютерної техніки. Відповідальність за такі порушення настає згідно ст.ст. 176, 177, 229 Кримінального кодексу України та Кодексу України про адміністративні правопорушення, що закріплено в статтях 51-2, 164-3, 164-6, 164-7, 164-9, 164-13, 345. Санкції цих статей передбачають такі види адміністративних стягнень, як штраф та конфіскація об'єкта адміністративного правопорушення [9, с. 873].

В умовах повномасштабної війни, що триває з 2022 року, Україна зіткнулася зі зростанням кількості кіберзлочинів, спрямованих проти ІВ, а також посиленням кіберзагроз з боку країни-агресора. Це вимагає від правоохоронних органів та державних інституцій посиленої уваги до питань кібербезпеки та захисту ІВ.

Правовий захист ІВ в кіберпросторі не може бути ефективним без використання сучасних технологічних та організаційних засобів. DRM-технології використовуються для контролю доступу до цифрового контенту та його використання, запобігаючи несанкціонованому копіюванню. Технологія блокчейн може бути використана для захисту ІВ шляхом створення незмінного та прозорого реєстру прав. Це дозволяє встановити авторство, дату створення та історію передачі прав. Цифрові водяні знаки та інші криптографічні методи дозволяють ідентифікувати оригінальні твори та відстежувати їх поширення в мережі.

Крім технологічних рішень, компанії повинні впроваджувати суворі політики кібербезпеки, проводити навчання для співробітників, а також регулярно оновлювати своє програмне забезпечення.

Притягнення до відповідальності за порушення прав ІВ у кіберпросторі є складним процесом. Однією з головних проблем є доказування. Для судового розгляду необхідно не лише довести факт порушення, а й ідентифікувати порушника та зібрати належні цифрові докази. Це вимагає від правоохоронних органів та судових експертів спеціальних знань та технічних засобів. Також виникають проблеми, пов'язані з трансграничним характером злочинів, коли необхідно взаємодіяти з правоохоронними органами інших країн [8, с. 668–669].

Висновки. Правовий механізм захисту прав інтелектуальної власності в кіберпросторі є складною, багаторівневою системою, яка перебуває в стані постійної еволюції. Це стосується як національного законодавства, так і міжнародного співробітництва. Ефективна протидія кіберзагрозам, пов'язаним з правами ІВ, можлива лише за умови скоординованих зусиль на всіх рівнях: від зміцнення законодавства та посилення правозастосовних процедур до підвищення обізнаності суспільства. Варто спрямувати зусилля наукової спільноти, законодавців, фахівців у галузі кібербезпеки на розробку уніфікованих міжнародних стандартів, впровадження інноваційних технологій для захисту ІВ та вдосконалення національних правових систем для більш ефективного реагування на сучасні кіберзагрози.

ЛІТЕРАТУРА

1. Цивільний кодекс України : Закон України від 16.01.2003 № 435-IV : станом на 10 серп. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text>
2. Про авторське право і суміжні права : Закон України від 01.12.2022 № 2811-IX : станом на 15 листоп. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/2811-20#Text>
3. Про охорону прав на промислові зразки : Закон України від 15.12.1993 № 3688-XII : станом на 31 груд. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/3688-12#Text>
4. Про охорону прав на винаходи і корисні моделі : Закон України від 15.12.1993 № 3687-XII : станом на 5 черв. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/3687-12#Text>
5. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 20 квіт. 2025 р. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
6. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>

7. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 : станом на 7 верес. 2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text
8. Погорілець М., Сорока С. Інтелектуальна власність у цифрову еру в контексті розвитку технологій. *Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична*. 2025. Вип. 44. URL: <https://doi.org/10.5281/zenodo.15340521>
9. Лучик С. Д., Лучик В. Є. Захист та кібербезпека інтелектуальної власності в Україні в умовах війни. *Наука і техніка сьогодні*. 2024. № 2 (30). С. 867–884. URL: [https://doi.org/10.52058/2786-6025-2024-2\(30\)-867-884](https://doi.org/10.52058/2786-6025-2024-2(30)-867-884)
10. Соколюк В. О. Міжнародно-правове співробітництво у сфері захисту прав інтелектуальної власності. 2025. URL: <https://doi.org/10.5281/zenodo.15315667>
11. Позняков С., Маньгора Т. До проблеми захисту права інтелектуальної власності в мережі інтернет. *Наукові інновації та передові технології*. 2024. № 3(31). URL: [https://doi.org/10.52058/2786-5274-2024-3\(31\)-660-671](https://doi.org/10.52058/2786-5274-2024-3(31)-660-671)
12. Корнілова І. М. Кіберпромислове шпигунство: сутність та наслідки. *Економічний простір*. 2024. № 190. С. 138–142. URL: <https://doi.org/10.32782/2224-6282/190-45>