УДК 340.122:004.8
DOI https://doi.org/10.24144/2307-3322.2025.92.1.19

УКРАЇНСЬКИЙ ДОСВІД РОЗВИТКУ НАУКОВИХ ПІДХОДІВ ДО ІНСТИТУТУ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ У СФЕРІ ІНТЕРНЕТ-ПРАВОПОРУШЕНЬ

Скоморовський В.Б.,
доктор юридичних наук, професор,
професор кафедри теорії та історії держави і права,
Університет економіки та права «КРОК»
ORCID: 0000-0002-1020-2322

Степаненко Н.В.,
доктор філософії в галузі «Право», доцент,
доцент кафедри теорії та історії держави і права,
Університет економіки та права «КРОК»
ORCID: 0000-0001-6216-2206

Скоморовський В.Б., Степаненко Н.В. Український досвід розвитку наукових підходів до інституту юридичної відповідальності у сфері інтернет-правопорушень.

У статті проаналізовано стан наукових досліджень інституту юридичної відповідальності за правопорушення в мережі Інтернет. Оцінено еволюцію підходів до регулювання інтернет-відносин, визначено основні напрями вдосконалення законодавства та механізмів протидії комп'ютерним злочинам. Зокрема, досліджено проблему формування міжгалузевих правових відносин в умовах стрімкої інформатизації та поширення доступу до мережі Інтернет, що потребує спеціалізованих нормативних і практичних заходів.

Виявлено, що серед ключових аспектів правового регулювання важливе місце займають захист інформаційних ресурсів, гарантування прав осіб на доступ до персональних даних, баланс інтересів у суспільних інформаційних відносинах та протидія транснаціональним комп'ютерним злочинам. Акцентується увага на високій латентності правопорушень в Інтернеті, що вимагає застосування більш жорстких заходів правового реагування, детінізації таких правопорушень та удосконалення процедур документування протиправної діяльності.

Проаналізовано сучасні підходи до визначення місця вчинення злочинів міжнародного характеру з використанням комп'ютерних технологій, у тому числі розгляд Інтернету як окремого віртуального простору. Визначено потребу системного підходу до формування національної нормативної бази, уніфікації законодавства та врахування міжнародних стандартів, зокрема положень Європейської конвенції про кіберзлочинність.

Наголошено на важливості кодифікації національного інформаційного законодавства та інтеграції норм щодо правопорушень в Інтернеті в єдину систему для забезпечення функціональної самостійності інституту юридичної відповідальності. Узагальнено, що ефективне правове реагування на цифрові злочини потребує комплексного підходу, міжнародної координації та вдосконалення механізмів захисту прав і свобод користувачів у сучасному інформаційному суспільстві. Обґрунтовано необхідність розширення інструментарію превентивних заходів у сфері кібербезпеки, зокрема шляхом удосконалення процедур ідентифікації користувачів, запровадження ефективних механізмів взаємодії між державними органами та приватними суб'єктами цифрової інфраструктури, а також розвитку спеціалізованої експертної та технічної спроможності правоохоронних органів.

Ключові слова: юридична відповідальність, правопорушення, Інтернет, комп'ютерні злочини, кібербезпека, міжнародне співробітництво, права людини, кодифікація законодавства, інформаційні відносини.

Skomorovsky V.B., Stepanenko N.V. Ukrainian experience in developing scientific approaches to the institution of legal liability in the field of Internet offenses.

The article analyzes the state of scientific research on the institute of legal liability for offenses on the Internet. The evolution of approaches to regulating Internet relations is assessed, the main directions of improving legislation and mechanisms for combating computer crimes are identified. In particular, the problem of forming interdisciplinary legal relations in the conditions of rapid informatization and the spread of access to the Internet, which requires specialized regulatory and practical measures, is investigated.

It is revealed that among the key aspects of legal regulation, an important place is occupied by the protection of information resources, guaranteeing the rights of individuals to access personal data, the balance of interests in public information relations and combating transnational computer crimes. Attention is focused on the high latency of offenses on the Internet, which requires the application of more stringent legal response measures, de-shadowing of such offenses and improving procedures for documenting illegal activities.

The article analyzes modern approaches to determining the place of commission of international crimes using computer technologies, including consideration of the Internet as a separate virtual space. The need for a systematic approach to the formation of a national regulatory framework, unification of legislation and consideration of international standards, in particular the provisions of the European Convention on Cybercrime, is identified. The importance of codifying national information legislation and integrating norms on Internet offenses into a single system is emphasized to ensure the functional independence of the institution of legal liability. It is summarized that an effective legal response to digital crimes requires a comprehensive approach, international coordination and improvement of mechanisms for protecting the rights and freedoms of users in the modern information society. The need to expand the toolkit of preventive measures in the field of cybersecurity is substantiated, in particular by improving user identification procedures, introducing effective mechanisms for interaction between state bodies and private entities of digital infrastructure, as well as developing specialized expert and technical capacity of law enforcement agencies.

Key words: legal liability, offenses, Internet, computer crimes, cybersecurity, international cooperation, human rights, codification of legislation, information relations.

Постановка проблеми. Юридична відповідальність за правопорушення в Інтернеті ускладнюється швидким розвитком інформаційного простору та появою нових, часто транснаціональних, видів правопорушень, контроль над якими складний. Національне законодавство наразі є фрагментарним і не завжди враховує особливості інтернет-діяльності, такі як анонімність користувачів, труднощі визначення місця правопорушення та порушення прав інтелектуальної власності. Для ефективного регулювання необхідний системний підхід, узгодження норм із міжнародними стандартами та вдосконалення механізмів захисту прав і свобод користувачів у кіберпросторі.

Мета статті – проаналізувати стан наукових досліджень та законодавчого регулювання юридичної відповідальності за правопорушення в мережі Інтернет в Україні.

Стан опрацювання проблематики. За основу дослідження взяті роботи Калюжного Р., Гавловського В., Цимбалюка В., Антипова В., Гуцалюка М., Кравчука С., Храбана С., Ягодзінського С. та ін.

Виклад основного матеріалу. Попри те, що українська правова наука здебільшого представлена сучасними дослідженнями, вона має значний історичний досвід ґрунтовного вивчення питань інформаційного права. Зокрема, у статті Р. Калюжного, В. Гавловського та В. Цимбалюка «Питання концепції реформування інформаційного законодавства України» наголошується на складнощах розвитку інформаційних досліджень в Україні. Автори підкреслюють, що процес інформатизації спричинює формування складних міжгалузевих предметів суспільних відносин та відповідних об'єктів правового регулювання, що потребують особливої уваги та спеціалізованого підходу. Як приклад науковці наводять мережу Інтернет та пов'язані з нею ризики правопорушень. Вони також відзначають, що з огляду на перспективи стрімкого поширення доступу до Інтернету в Україні постане питання його регулювання як невід'ємного елементу функціонування сучасного суспільства. Серед пріоритетних напрямів автори визначили:

- забезпечення умов для розвитку та захисту різних форм власності на інформацію та інформаційні ресурси;

- організація та керівництво створенням та розвитком державних регіональних інформаційних систем і мереж, забезпечення їх сумісності та взаємодії в єдиному інформаційному просторі України;
- правове регулювання, спрямоване на створення умов для якісного та ефективного надання необхідної інформації громадянам, органам державної влади, органам місцевого самоврядування, державним та приватним організаціям, об'єднанням, використовуючи державні інформаційні ресурси та сучасні інформаційні технології;
- забезпечення балансу інтересів у суспільних інформаційних відносинах, зокрема в галузі національної безпеки, що включає інформаційну безпеку;
- гарантування реалізації конституційних прав осіб (приватних немайнових) на режим доступу до персональних даних – інформації про громадян та їх спільноти (організації) у контексті інформатизації державних органів управління;
- Створення дієвих юридичних механізмів для запобігання державному та недержавному зловживанню [1, с. 18].

Зрештою, піднята й висвітлена в публікації парадигма багато у чому залишається актуальною та не втрачає свого значення в контексті проблеми юридичної відповідальності за правопорушення в мережі Інтернет. В дечому запропоновані авторами напрямки перегукуються з положеннями Концепції Національної програми інформатизації, прийнятої Верховною Радою України 04.02.1998 [2].

В. Антипов у дослідженні «Види транснаціональних злочинів за класифікацією ООН та їх поширеність в Україні» відзначає, що відповідальність за «комп'ютерну злочинність» на порядку денному має бути жорсткішою за ряд звичних правопорушень [3, с. 77]. Автор зауважує на тому, що винесення класифікацією ООН «комп'ютерних злочинів» в окрему транснаціональну групу протиправних дій має віднайти відповідну реакцію з боку держав у вигляді еквівалентних законодавчих змін для протидії цим правопорушенням і формуванні спеціального правозастосування в частині юридичної відповідальності винних суб'єктів. Як взірець стимулу до трансформації поглядів до юридичної відповідальності за правопорушення в мережі Інтернет і механізми її застосування автор наводить крадіжку й інші форми посягання на інтелектуальну власність. Зокрема, за В. Антиповим поняття «крадіжка інтелектуальної власності» включає в себе порушення прав авторів і виконавців, а також незаконне використання знаків охорони авторського права і торгових марок. Спокусу незаконно відтворити захищені твори і продати їх дешевше або за ту ж ціну велике, особливо в країнах із нерозвиненою економікою. Обсяги збитків країн-виробників важко піддаються вимірюванню в грошовому вираженні. Тільки від нелегального використання програмного забезпечення, як підрахувала Асоціація американських видавців програмного забезпечення, збиток становить 7,5 млрд дол. в рік (дані актуальні на 2000 рік, відносно сьогодення ці показники менші у 40 разів). Підробку знаків охорони авторського права не можуть здійснити дрібні підприємства або підприємці-одинаки. Тут необхідні координація і налагоджена система збуту часто на транснаціональному рівні [3, с. 78].

Крізь призму кримінальних деліктів одну з перших спроб охарактеризувати специфіку юридичної відповідальності за правопорушення в мережі Інтернет зробив М. Гуцалюк. Вчений навів у статті основні «комп'ютерні правопорушення», серед яких названі: 1) несанкціонований доступ або доступ до мереж чи інформації з порушенням правил доступу; 2) незаконне перехоплення даних, їхнє акумулювання каналами збору й засобами комп'ютерної інформації; 3) пошкодження інформації, її модифікація чи трансформація з протиправною метою; 4) комп'ютерне шахрайство; 5) розповсюдження порнографічних матеріалів; 6) правопорушення в контексті захисту авторського права. Фактично, М. Гуцалюк при розгляді питання правопорушень в мережі Інтернет зупиняється переважно на тих протиправних діях, поширення яких прямо пропорційне роботі мережі Інтернет, не надаючи таким чином комплексної оцінки питанню юридичної відповідальності. Примітно, що науковець у матеріалі посилається на зміст указу Президента України «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Internet та забезпечення широкого доступу до цієї мережі в України». Даний документ серед іншого в тодішніх умовах постановив такі принципові заходи для подальшої адаптації правової системи до масштабування мережі Інтернет, як: «1) вдосконалення правового регулювання діяльності суб'єктів інформаційних відносин, виробництва, використання, поширення та зберігання електронної інформаційної продукції, захисту прав на інтелектуальну власність, посилення відповідальності за порушення

встановленого порядку доступу до електронних інформаційних ресурсів всіх форм власності, за навмисне поширення комп'ютерних вірусів; 2) встановлення відповідальності за поширення через мережу Інтернет інформації, розповсюдження чи обнародування якої заборонено відповідно до законодавства, за навмисне поширення комп'ютерних вірусів, порушення встановленого порядку доступу до інформаційних ресурсів усіх форм власності» [5]. Це один із перших нормативно-правових актів, який окреслив такі принципові напрямки діяльності в контексті досліджуваного питання.

У теоретичному сенсі щодо проблеми методології юридичної відповідальності за правопорушення в мережі Інтернет свій вклад у 2003 році зробив С. Кравчук. Науковець констатував, що високий рівень латентності правопорушень, що скоєні за допомогою Інтернету, примушує опрацьовувати більш жорсткі та репресивні заходи до порушників з метою детінізації таких правопорушень і скорочення їхньої кількості. Як приклад С. Кравчук наводить ситуацію з професійного досвіду, коли у м. Хмельницький у 2003 році розслідувався ряд фактів втручання у комп'ютерні мережі більш ніж 40 клієнтів (здебільшого органів державної влади та державних установ) через одну з комп'ютерних фірм, котра надавала на той час Інтернет-послуги. Вірус проникав до систем, розсилався адресатам через пошту та інші налаштовані бездротові комунікації між пристроями, копіював дані. Вірус надсилав отримані файли зловмисникам, які використовували цю інформацію для подальших правопорушень, у тому числі щодо банківських і фінансових операцій. Власне цей випадок, на його погляд, є наочним свідченням неординарності правопорушень, що вчиняються у інфопросторі Інтернету.

В. Гавловський застерігав від непослідовного реформування та розширення інформаційного законодавства, у тому числі в контексті запобігання правопорушенням в рамках функціонування мережі Інтернет. Вчений підкреслює, що: «національне (державне, публічне) право України містить значний обсяг нормативних актів, таких як закони та підзаконні акти, які безпосередньо або опосередковано регулюють взаємовідносини у сфері інформації в суспільстві. На своєму початковому етапі розвитку воно було фрагментарним і реагувало на конкретні ситуації. При цьому проблемі правопорушень в новій інноваційній сфері уваги майже не приділялося» [7, с. 174]. В розрізі екстраполяризації методології встановлення юридичної відповідальності за правопорушення в мережі Інтернет автор наводить помилки у підході польських законодавців. У цій країні основним підходом до правового регулювання Інтернету (в тогочасних реаліях) є фрагментарний та ситуаційний метод, який розробляється по мірі усвідомлення проблем і подолання соціальної невизначеності в органах державної влади щодо потреби в юридичному врегулюванні і захисті окремих суспільних відносин у сфері інформації. Цей підхід є характерним для системи законотворення англосаксонської правової традиції, де недоліки або невизначеність конкретних норм уточнюються при виникненні суперечок на рівні судової практики (судових рішень та прецедентів) і тлумачень відомих юристів, які визнаються джерелами публічного права [7, с. 175].

Продовжуючи лінію значущості цілісного підходу до становлення й реалізації юридичної відповідальності за правопорушення в мережі Інтернет можна згадати статтю С. Храбана і С. Ягодзінського «Правове врегулювання в умовах інформаційного суспільства». Автори підсумовують, що імплементація міжнародних стандартів суворості й дієвості механізмів юридичної відповідальності за правопорушення в Інтернеті є необхідною умовою відносно європейського майбутнього України. Зокрема, науковці звертають увагу на наступне: вступ України до Європейського Співтовариства та підписання Європейської конвенції про кіберзлочинність у 2001 році потребують перегляду національного інформаційного законодавства. Конвенція визначає види комп'ютерних злочинів і механізми міжнародного співробітництва для їх протидії, а відсутність системності у регулюванні може ускладнити або зробити неможливим її застосування.

І. Петренко, консолідуючи питання правових порушень у сфері Інтернет-відносин, окреслив такі ключові аспекти підходу до встановлення особливої юридичної відповідальності за правопорушення в мережі Інтернет:

- правове регулювання мережі Інтернет повинно включати активну участь інтернет-спільноти;
- при розробці юридичної основи для виокремлення специфіки правової відповідальності за правопорушення в межах Інтернету необхідно вживати системний підхід, що охоплює всі аспекти інтернет-відносин;

- при створенні вітчизняної нормативної бази для Інтернету важливо враховувати досвід інших країн і сприяти уніфікації законодавства та практики правозастосування;
- пріоритетом у правовому регулюванні є розробка та прийняття міжнародних правових актів, які встановлюють загальні стандарти для мережі Інтернет та включають питання протидії зловживанням правом та деліктам в Інтернеті. Зокрема, важливо, щоб держава якнайшвидше визначила правові рамки, в яких має функціонувати Інтернет, оскільки це суттєво впливає на усю систему захисту прав і свобод в Інтернеті [8, с. 199].

І. Борисенко притримується думки про потребу розмежування правопорушень суто інформаційного характеру в мережі Інтернет з усіма іншими можливими видами правопорушень. При цьому науковець відзначає, що пріоритетним напрямом унормування питання юридичної відповідальності за правопорушення в мережі Інтернет є розширення інструментарію протидії посяганням на право інтелектуальної власності та форм самозахисту такого права [9, с. 198]. В якості прикладу наводяться положення ст. 20 Закону України «Про охорону прав на знаки для товарів та послуг» від 15 грудня 1993 року (в редакції від 16.05.2008 року): «порушенням прав власника свідоцтва вважається також використання без його згоди в доменних іменах знаків та позначень, вказаних у пункті 5 статті 16 цього Закону» [10].

В. Гурковський з приводу взаємозалежності юридичної відповідальності та збільшення у суспільстві доступу до мережі Інтернет констатує, що вступ до глобального інформаційного простору призводить до виникнення багатьох правових проблем, які в першу чергу повинні бути вирішені на національному рівні законодавства. На його думку, оскільки правопорушення в мережі Інтернет можуть транскордонно поширюватися та відбуватися дуже швидко, основними напрямами удосконалення законодавства є:

- включення в національне законодавство відповідних вимог, які дозволяють ідентифікувати всіх користувачів Інтернету та їх зв'язок;
- спрощення процедур документування протиправної діяльності у сфері кіберзлочинності для правоохоронних органів;
- встановлення додаткових вимог до постачальників телекомунікаційних послуг та суб'єктів, що надають послуги колективного доступу до Інтернету. Ці вимоги стосуються збереження даних про трафік на протязі періоду від 6 місяців до 3 років і забезпечення належного контролю за користувачами мережі Інтернет, включаючи відвідувачів пунктів колективного доступу.
- наявність можливості у державних інституціях блокувати шкідливий або протиправний контент у випадках, коли це необхідно [11, с. 57].

Слушно додати, що для підвищення ефективності заходів із протидії кіберзлочинності та кібертероризму в Україні повинні запроваджуватися сприятливі умови для правоохоронних органів у проведенні оперативно-розшукових, відповідних технічних заходів та інших видів документування протиправної діяльності. У правоохоронних органів не повинно існувати правових перешкод, пов'язаних з оперативним отриманням матеріалів для документуванням протиправної діяльності правопорушників.

О. Присяжнюк зазначає, що центральною проблемою, яка ускладнює застосування права в сфері регулювання мережі Інтернет, є анонімність користувачів мережі. Суб'єкт може здійснювати свою інформаційну діяльність з будь-якої точки світу, надсилаючи та отримуючи інформацію. Походження повідомлення може бути прихованим або зашифрованим. Споживач мережі може мати псевдонім або електронну ідентифікацію, відмінну від його реальної ідентифікації. Ця можливість користувачів мережі Інтернет використовувати віртуальний простір для створення бастіонів і територій, які дозволяють їм уникати законної юридичної відповідальності без остраху залишити зайвий слід чи бути виявленим компетентними правоохоронними органами.

К. Юртєва, аналізуючи проблематику визначення місця злочинів з використанням комп'ютерних технологій, підсумовує, що існує два основні вектори стосовно розв'язання проблеми подальшого регулювання Інтернету та юридичної відповідальності за злочини міжнародного характеру з використанням комп'ютерних технологій: за першим підходом пропонується пристосувати існуючі традиційні принципи кримінальної юрисдикції до злочинів, що вчиняються за використанням комп'ютерних технологій, в той час як другий підхід пропонує розглядати Інтернет як самостійний віртуальний простір, «кіберпростір», і розробити нові правила застосування кримінальної юрисдикції щодо злочинів, що у ньому вчиняються [12, с. 436]. Представники першого підходу вважають, що виникнення нової Інтернет-технології не автоматично

змінює правову доктрину кримінальної юрисдикції, і її можна застосовувати до злочинів міжнародного характеру, які використовують комп'ютерні технології. Наприклад, цей підхід, на думку вченої, витриманий у рамках Конвенції про кіберзлочинність 2001 року, яка визначила традиційну систему кримінальної юрисдикції для регулювання злочинів і встановила принципи територіальної та національної юрисдикції. На противагу цьому більш відповідним сучасним реаліям вважаємо другий підхід до регулювання правових відносин в мережі Інтернет, котрий представляє альтернативу традиційному підходу, базованому на географічних обмеженнях. Прихильники цього підходу пропонують розглядати місцем вчинення злочинів міжнародного характеру з використанням комп'ютерних технологій не географічну територію країни або інші територіальні межі, а власне сам кіберпростір. Об'єктивно дане твердження вимагає ремарки в тій частині, що обидва підходи мають певні переваги, однак не можуть універсально окреслювати всю сукупність ймовірних ситуацій.

В. Бутузов резюмує, що попри деякі кроки й позитивні зрушення в контексті виокремлення субінституту юридичної відповідальності відносно правопорушень, вчинених в мережі Інтернет, наше законодавство відверто не готове до всебічного забезпечення захисту прав, свобод і законних інтересів при динаміці збільшення кількості активних користувачів мережі Інтернет. Науковець підкреслює, що поширення використання мережі Інтернет на великій шкалі, при відсутності адміністративних обмежень в електронному просторі і майже безконтрольному потоку інформації, сприяє виникненню нових видів злочинів у цій галузі, які важко простежуються. Високотехнологічні злочини стають більш організованими і транснаціональними. Отже, широке впровадження комп'ютеризованих інформаційно-телекомунікаційних систем (автоматизованих комп'ютерних інформаційних систем) на міжнародному рівні створює численні нові проблеми, які потребують наукового дослідження і практичного вирішення.

В. Брижко визначаючи засади й методологію кодифікації інформаційного законодавства України, резюмує, що без об'єднання існуючих наразі в нормах закону положень про правопорушення, які скоюються через мережу Інтернет, отримати якийсь позитивний результат від акумуляції нормативного масиву буде неможливо. Тобто науковиця натякає на провідній ролі кодифікації нормативних актів шляхом консолідації відповідних положень, що обов'язково, але не обмежуючись, уможливить функціональну самостійність значимості особливих суспільних правовідносин, котрі перетікають в мережі Інтернет.

Висновки. Українська правова наука має значний досвід дослідження інформаційного права, проте юридична відповідальність за правопорушення в Інтернеті потребує подальшого розвитку та кодифікації законодавства. Інтернет створює нові міжгалузеві суспільні відносини та загрози, що вимагають спеціалізованого правового регулювання та міжнародного узгодження норм. Основними проблемами залишаються анонімність користувачів, транскордонний характер злочинів і потреба в ефективних механізмах запобігання та документування порушень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Калюжний Р., Гуцалюк М., Цимбалюк В. Питання концепції реформування інформаційного законодавства України. 2000. № 2. С. 17–21. URL: https://surl.li/buqbgj (дата звернення: 08.12.2025).
2. Концепція Національної програми інформатизації: Закон України № 75/98-ВР від 04.02.1998: станом на 01.01.2022. Верховна Рада України. URL: https://surl.li/wbowwm (дата звернення: 08.12.2025).
3. Антипов В.І. Види транснаціональних злочинів за класифікацією ООН та їх поширеність в Україні. *Вісник Харківського національного університету внутрішніх справ*. 2000. № 12 (2). С. 77–87. URL: file:///C:/Users/user/Downloads/VKhnuvs_2000_12(2)__21.pdf (дата звернення: 08.12.2025).
4. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Internet та забезпечення широкого доступу до цієї мережі в Україні: указ Президента України № 928/2000 від 31.07.2000. URL: https://zakon.rada.gov.ua/laws/show/928/2000#Text (дата звернення: 08.12.2025).
5. BSA compliance solutions. Losses from illegal use of software. URL: https://cpl.thalesgroup.com/software-monetization/how-to-prevent-software-piracy (дата звернення: 08.12.2025).

6. Кравчук С.Й. Кравчук О.С. Основні проблеми та напрями протидії злочинності в сфері експлуатації електронно-обчислювальних систем. *Вісник Хмельницького інституту регіонального управління та права*. 2003. № 3-4. С. 300–303. URL: https://elar.khmnu.edu.ua/handle/123456789/2712 (дата звернення: 08.12.2025).
7. Гавловський В., Цимбалюк В., Кашпур В. Державно-правове регулювання соціальних інформаційних відносин. *Українське право*. 1998. № 1. С. 173–176. URL: https://ela.kpi.ua/server/api/core/bitstreams/2aba5e82-6eb1-45af-89bb-94fc0679b253/content (дата звернення: 08.12.2025).
8. Петренко О.С. Інтернет як простір соціальних взаємодій: досвід різних груп користувачів. *Вісник Харківського національного університету імені В.Н. Каразіна.* Серія: Соціологічні дослідження сучасного суспільства: методологія, теорія, методи. 2012. № 993, Вип. 29. С. 126–130. URL: http://nbuv.gov.ua/UJRN/VKhISD_2012_993_29_24 (дата звернення: 08.12.2025).
9. Борисенко І.Л. Особливості самозахисту прав інтелектуальної власності в глобальній мережі Інтернет. *Часопис Київського університету права*. 2010. № 1. С. 197–201. URL: https://nasplib.isofts.kiev.ua/items/5e1b5d5d-5398-4dad-b87c-ae5ab050e141 (дата звернення: 08.12.2025).
10. Про охорону прав на знаки для товарів та послуг: Закон України № 3689-XII від 15.12.1993: станом на 16.05.2008. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3689-12/ed20080516#o176 (дата звернення: 08.12.2025).
11. Гурковський В.І. Правове регулювання розвитку інформаційного суспільства в Україні. *Інвестиції: практика та досвід.* 2010. № 12. С. 56-59. URL: http://www.investplan.com.ua/pdf/12_2010/17.pdf (дата звернення: 08.12.2025).
12. Юртаєва К.В. Визначення місця вчинення злочинів з використанням комп'ютерних технологій. *Форум права.* 2009. № 2. С. 434–451. URL: file:///C:/Users/user/Downloads/FP_index.htm_2009_2_69.pdf (дата звернення: 08.12.2025).