ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД
«УНІВЕРСИТЕТ ЕКОНОМІКИ ТА ПРАВА «КРОК»

Кваліфікаційна наукова праця
на правах рукопису

ХУДОЛЄЙ ЯРОСЛАВ ГРИГОРОВИЧ

УДК 340.131:34.03

ДИСЕРТАЦІЯ

ЮРИДИЧНА ВІДПОВІДАЛЬНІСТЬ ЗА ПРАВОПОРУШЕННЯ В МЕРЕЖІ ІНТЕРНЕТ: ЗАГАЛЬНОТЕОРЕТИЧНИЙ АСПЕКТ

081 «Право»
08 «Право»

Подається на здобуття наукового ступеня доктора філософії в галузі права

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Я. Г. Худолєй

Науковий керівник: кандидат юридичних наук
Загребельна Наталія Анатоліївна

КИЇВ – 2026

АНОТАЦІЯ

Худолєй Я.Г. Юридична відповідальність за правопорушення в мережі Інтернет: загальнотеоретичний аспект. – *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 081 «Право» (Галузь знань: 08 Право). Університет економіки та права «КРОК». Київ. 2026.

У дисертаційному дослідженні здійснено комплексний теоретичний аналіз феномену юридичної відповідальності за правопорушення у мережі Інтернет, узагальнено сучасні наукові підходи та вироблено авторське бачення її загальнотеоретичних засад.

Констатовано, глобалізація та цифрова модернізація суспільства виступають чинниками, що зумовлюють сутнісне переосмислення природи юридичної відповідальності. У сьогоденному правовому дискурсі простежується відхід від її традиційного трактування виключно крізь призму формально-юридичних ознак складу правопорушення. Натомість акцент поступово зміщується на оцінку суспільної результативності відповідальності, яка розглядається як інструмент відновлення порушених прав, превенції майбутніх правопорушень і підтримання довіри до державно-владних інститутів як системної цінності.

Наголошено, системний аналіз міжнародно-правових актів і стратегічних документів провідних міжнародних організацій свідчить про відсутність уніфікованого нормативного визначення поняття «кіберпростір». Водночас у більшості актів простежується його трактування як глобального інформаційно-комунікаційного середовища, у межах якого підлягають застосуванню загальновизнані норми міжнародного права. Артикульовано, міжнародне співтовариство рухається шляхом поступового формування стандартів та правил належної поведінки в кіберпросторі. Остаточне визначення правового статусу кіберпростору потребує комплексного синтезу кількох концептуальних підходів, що полягає у поєднанні визнання

кіберпростору як спільної сфери інтересів усього людства із одночасним збереженням за державами суверенних прав на національні інформаційні ресурси та здійсненням юрисдикції щодо злочинної чи ворожої діяльності, яка походить з їхньої території або спрямована проти неї. За таких умов кіберпростір функціонуватиме як відкрите, стійке та мирне середовище, спрямоване на розвиток людства, а не перетворюватиметься на арену анархії або вседозволеності.

Важливою ознакою мережі Інтернет є її модель управління, оскільки вона історично формувалася за багатосторонньою логікою, у межах якої поряд із державами ключову роль відіграють технічні спільноти зі стандартизації, інституції управління ідентифікаторами, оператори мереж, цифрові платформи та інститути громадянського суспільства. Вказана модель спирається на поєднання «твердого» права та «м'якого» регулювання (стандарти, кодекси, політики застосунків, угоди між операторами та реєстрами), що формує специфічний регулятивний режим співуправління. Для правового аналізу зазначене передбачає розщеплення центрів нормотворення, розмиті кордони юрисдикції та необхідність узгодження технічних стандартів із вимогами верховенства права та прав людини.

Доведено, кіберпростір та мережа Інтернет співвідносяться як широка правова категорія та її інфраструктурна основа. Їх поєднують спільні цінності, але відрізняє предмет регулювання, рівень інституціоналізації та специфіка суб'єктного складу управління. Кіберпростір слід розглядати як глобальне соціально-технічне середовище, що поєднує інформаційні потоки та комунікаційні системи, не має фізичних меж, однак генерує реальні правові наслідки. Інтернет у системі кіберпростору виконує роль матеріальної та організаційної інфраструктури, яка забезпечує функціонування кіберпростору, проте водночас формує власний специфічний правовий режим. Його регулятивна природа визначається поєднанням норм національного законодавства, міжнародного права та актів саморегуляторних спільнот.

На основі аналізу міжнародних стандартів у сфері юридичної відповідальності за правопорушення у мережі Інтернет зроблено ряд висновків: 1) міжнародна нормативна база у цій сфері є фрагментованою за географічною та предметною ознакою, проте спостерігається тенденція до її уніфікації; 2) входження до глобальних домовленостей значно ширшого кола держав з різними правовими системами породжує виклик дотримання прав людини; як показав аналіз фінального тексту конвенції ООН, відсутність жорстких гарантій може бути використана авторитарними режимами для переслідування інакодумців під приводом боротьби з кіберзлочинами; 3) найбільше розвинені стандарти стосуються саме кримінальної відповідальності, що історично обумовлено першочерговим фокусом на кіберзлочинності; натомість міжнародні механізми цивільно-правової та адміністративної відповідальності розвинені значно менше та носять характер радше рекомендацій, ніж обов'язкових норм; встановлено, у перспективі варто очікувати розвитку саме таких «горизонтальних» стандартів, зокрема, у сфері відповідальності постачальників цифрових послуг; 4) ефективність міжнародних стандартів корелюється із належною імплементацією на національному рівні; навіть після приєднання до міжнародних договорів окремі держави не забезпечують повної гармонізації внутрішнього законодавства; не всі передбачені Конвенцією про кіберзлочинність діяння отримують належну криміналізацію, а процесуальні механізми щодо збирання та вилучення електронних доказів залишаються фрагментарними; у цьому зв'язку пріоритетного значення набувають системний моніторинг виконання міжнародних зобов'язань та надання державам технічної допомоги в процесі їх імплементації. Констатовано, міжнародні стандарти у сфері юридичної відповідальності за правопорушення у мережі Інтернет дедалі більше зміщуються у бік комплексного механізму шляхом поєднання відповідальності з просвітою користувачів, кібергігієною, партнерством з приватним сектором та повагою до відкритості мережі. Нові міжнародні документи та ініціативи мають шанс

закріпити та розвинути зазначені принципи. Сьогодні міжнародні стандарти у сфері юридичної відповідальності за інтернет-правопорушення знаходяться в стадії динамічного розвитку, позаяк від фрагментарних регіональних норм вони еволюціонують до цілісної системи універсальних правил, що враховують як потребу у безпеці, так і необхідність збереження фундаментальних прав і свобод у цифрову епоху.

Визначено ключові характеристики юридичної відповідальності за правопорушення в мережі Інтернет: 1) транснаціональний характер, оскільки переважна більшість правопорушень в мережі Інтернет виходить за межі національних юрисдикцій, що зумовлює складнощі у визначенні компетентного органу та виборі застосовного права; 2) ускладнена ідентифікація суб'єкта, позаяк в умовах анонімності, використання псевдонімів, VPN-технологій, блокчейну та систем шифрування постає об'єктивна проблема встановлення особи правопорушника; 3) комплексний характер складу правопорушення, адже правопорушення в мережі Інтернет поєднують технічні, поведінкові, інтелектуальні та інші елементи, що значно ускладнює правову кваліфікацію; 4) множинність нормативного впливу, яка проявляється у взаємодії норм національного законодавства, міжнародно-правових стандартів, актів м'якого права та корпоративних політик цифрових платформ, що створює багаторівневу модель регулювання.

Репрезентовано класифікацію різновидів юридичної відповідальності за правопорушення в мережі Інтернет: вторинна (умовна), саморегуляторна, колективна, алгоритмічна (автоматизована), множинна (гібридна). Розкрито їх сутність та зміст. Сформульовано ознаки множинної (гібридної) відповідальності за правопорушення у мережі Інтернет: 1) характеризується «подвійною атрибуцією», за якої деліктогенний результат одночасно є наслідком вольових рішень людини та автономних або напівавтономних дій цифрових систем; 2) не зводиться до класичної індивідуалізації суб'єкта, а передбачає розподіл правових наслідків між кількома рівнями, зокрема, особою, яка ініціює чи контролює процес, оператором платформи, а також

технічною інфраструктурою, що генерує правопорушний ефект; 3) становить новий інститут загальної теорії права, що вимагає: а) формування критеріїв оцінки ступеня алгоритмічної автономії та меж людського контролю; б) перегляду традиційних категорій вини та необережності в умовах алгоритмізованого середовища; в) вироблення механізмів юрисдикційної координації для подолання колізій багатоярусного правозастосування.

Узагальнено усталені у правовій доктрині і міжнародній практиці різновидів правопорушень у мережі Інтернет та визначено їх класифікацію за наступними критеріями: 1) за об'єктом посягання; 2) за способом здійснення (залежно від методів і технічних засобів); 3) за принципом юрисдикційної належності (територіальною ознакою); 4) за рівнем суспільної небезпеки. Констатовано, аналіз правопорушень у кіберпросторі потребує врахування особливостей цифрового середовища, що відмежовують їх від класичних деліктів у межах традиційно усталеного розуміння, серед яких виокремлено: 1) відсутність територіальної визначеності; 2) технологічна складність правопорушень у мережі Інтернет; 3) дистанційність та віртуалізація дій; 4) анонімність та псевдоанонімність суб'єкта; 5) масовість та колективний характер впливу правопорушень у мережі Інтернет; 6) розмитість об'єкта правопорушення у цифровому середовищі; 7) варіативність правового регулювання у сфері Інтернет-правопорушень; 8) транзитивність (перехідність); 9) автоматизований характер; 10) високий рівень латентності; 11) міждисциплінарний характер правопорушень.

Визначено вектори розвитку інституту юридичної відповідальності у цифровому середовищі: 1) визначення юрисдикційних меж діяльності у метавсесвіті; 2) криміналізація нових форм суспільно небезпечної поведінки, що виникають у віртуальних середовищах; 3) вдосконалення цивільно-правового (деліктного) регулювання шкоди, завданої у VR-, AR-середовищах та метаверсах; 4) здійснення законодавчого встановлення спеціальних обов'язків провайдерів цифрових платформ; 5) впровадження так званої «структурної відповідальності» провайдерів, яка передбачає їх обов'язок

запобігати правопорушенням через архітектуру платформи та алгоритми модерації; 6) застосування концепції «цифрового делікту» як окремої категорії правопорушення, що вимагає нормативного оформлення; запропоновано наступне визначення досліджуваному поняттю «цифровий делікт – це протиправне винне діяння, що здійснюється у віртуальному середовищі й характеризується нематеріальністю об'єкта посягання, транскордонністю юрисдикції та ускладненою ідентифікацією суб'єкта, внаслідок чого завдається шкода майновим чи немайновим правам особи, а також суспільним інтересам, які підлягають правовій охороні»; 7) нормативне визначення критеріїв відповідальності за автономні рішення, що приймаються із застосуванням систем штучного інтелекту; 8) запровадження системи безперервного навчання суддів та слідчих щодо особливостей роботи з цифровими доказами, методів встановлення причинно-наслідкового зв'язку у випадках алгоритмічних рішень, а також стандартів оцінки надійності програмних продуктів і цифрової інфраструктури; 9) посилення участі України у діючих міжнародних механізмах та ініціювання нових форм співробітництва, спрямованих на забезпечення невідворотності відповідальності незалежно від місця вчинення правопорушення; 10) використання цифрових технологій як інструментів підсилення механізмів притягнення до відповідальності; 11) закріплення принципів цифрової етики у правовій площині з метою їх трансформації у юридично значущі регулятори поведінки, що дозволить узгодити вимоги, які висуває суспільство до етичності функціонування віртуальних спільнот, із нормативними приписами, що забезпечуються державним примусом.

Визначено доктринально обґрунтованою необхідність розробки та ухвалення спеціального закону «Про штучний інтелект». У зазначеному нормативному акті мають бути чітко визначені критерії відповідальності суб'єктів: розробника, якщо шкода спричинена дефектом алгоритму, впроваджувача у разі неналежного впровадження системи у виробничий процес, користувача за умови неправомірного або необережного

застосування технології тощо. Наголошено, принципово важливим є закріплення норми, згідно з якою системи штучного інтелекту не визнаються самостійними носіями прав і обов'язків, а отже, відповідальність завжди покладається на визначених фізичних або юридичних осіб. Встановлено, Проєкт Закону України «Про штучний інтелект» повинен передбачати такі структурні елементи: Розділ I. Загальні положення; Розділ II. Класифікація систем штучного інтелекту за рівнем ризику; Розділ III. Вимоги до створення, впровадження та використання систем штучного інтелекту; Розділ IV. Юридична відповідальність за використання систем штучного інтелекту; Розділ V. Інституційне забезпечення функціонування систем штучного інтелекту; Розділ VI. Прикінцеві та перехідні положення. Репрезентовано ключові положення кожної з структурних частин запропонованого законопроєкту.

Ключові слова: юридична відповідальність, Інтернет, інформаційні технології, діджиталізація, захист персональних даних, права людини, правопорушення, міжнародне право, кіберпростір, правове регулювання, ІТ-право, міжнародне співробітництво, веб-сайт, інтелектуальна власність, провайдер.

ABSTRACT

Khudoliei Ya. H. Legal liability for offenses on the Internet: a general theoretical aspect. – *Qualifying scientific work on the rights of the manuscript.*

Thesis for the degree of Doctor of Philosophy in specialty 081 «Law» (Field of Knowledge 08 Law). «KROK» University. Kyiv. 2026.

The dissertation research carried out a comprehensive theoretical analysis of the phenomenon of legal liability for offenses on the Internet, summarized modern scientific approaches and developed the author's vision of its general theoretical principles.

It was stated that globalization and digital modernization of society are factors that cause a fundamental rethinking of the nature of legal liability. In today's legal discourse, there is a departure from its traditional interpretation exclusively through the prism of formal and legal features of the offense. Instead, the emphasis is gradually shifting to assessing the social effectiveness of liability, which is considered as a tool for restoring violated rights, preventing future offenses and maintaining trust in state and government institutions as a systemic value.

It was emphasized that a systematic analysis of international legal acts and strategic documents of leading international organizations indicates the absence of a unified normative definition of the concept of "cyberspace". At the same time, most acts trace its interpretation as a global information and communication environment, within which generally recognized norms of international law are subject to application. Articulated, the international community is moving towards the gradual formation of standards and rules of proper conduct in cyberspace. The final definition of its legal status will involve the synthesis of several concepts by combining the recognition of cyberspace as a common sphere of interests of humanity with the simultaneous preservation of sovereign rights of states to their information resources, as well as jurisdiction over criminal or hostile activities emanating from or directed against their territory. Under such conditions, cyberspace will function as an open, stable and peaceful environment aimed at the development of humanity, and will not turn into an arena of anarchy or permissiveness.

Emphatically, an important feature of the Internet is its governance model, as it has historically developed according to a multilateral logic, within which, along with states, technical standard-setting communities, identifier institutions, network operators, platforms and civil society play a key role. This model is based on a combination of "hard" law and "soft" regulation (standards, codes, application policies, agreements between operators and registries), which forms a specific regulatory co-governance regime. For legal analysis, this implies a fragmentation

of norm-setting centers, blurred boundaries of jurisdiction and the need to harmonize technical standards with the requirements of the rule of law and human rights.

It is proven that cyberspace and the Internet are related as a broad legal category and its infrastructure basis. They are united by common values, but are distinguished by the subject of regulation, the level of institutionalization and the specifics of the subject composition of management. Cyberspace should be considered as a global socio-technical environment that combines information flows and communication systems, has no physical boundaries, however, generates real legal consequences. The Internet in the cyberspace system plays the role of material and organizational infrastructure that ensures the functioning of cyberspace, but at the same time forms its own specific legal regime. Its regulatory nature is determined by a combination of national legislation, international law and acts of self-regulatory communities.

A number of conclusions have been made regarding international standards in the field of legal liability for Internet offenses: 1) the international regulatory framework in this area is fragmented by geographical and subject matter, but there is a tendency towards its unification; 2) the entry into global agreements of a much wider range of states with different legal systems poses a challenge to human rights compliance; as the analysis of the final text of the UN convention has shown, the lack of strict guarantees can be used by authoritarian regimes to persecute dissenters under the pretext of combating cybercrime; 3) the most developed standards relate specifically to criminal liability, which is historically due to the primary focus on cybercrime; in contrast, international mechanisms of civil and administrative liability are much less developed and are more in the nature of recommendations than mandatory norms; It has been established that in the future we should expect the development of such “horizontal” standards, in particular, in the field of liability of digital service providers; 4) the effectiveness of international standards is correlated with proper implementation at the national level; even after joining international treaties, individual states do not ensure full

harmonization of domestic legislation; not all acts provided for by the Convention on Cybercrime are properly criminalized, and procedural mechanisms for collecting and seizing electronic evidence remain fragmentary; in this regard, systematic monitoring of the implementation of international obligations and providing technical assistance to states in the implementation process are of priority importance. It has been noted that international standards in the field of legal liability for offenses on the Internet are increasingly shifting towards a comprehensive mechanism by combining liability with user education, cyber hygiene, partnership with the private sector and respect for the openness of the network. New international documents and initiatives have a chance to consolidate and develop these principles. Today, international standards in the field of legal liability for Internet offenses are in a stage of dynamic development, as they evolve from fragmented regional norms to a holistic system of universal rules that take into account both the need for security and the need to preserve fundamental rights and freedoms in the digital age.

The key characteristics of legal liability for Internet offenses are identified: 1) transnational nature, since the vast majority of Internet offenses go beyond national jurisdictions, which makes it difficult to determine the competent authority and choose the applicable law; 2) complicated identification of the subject, since in the conditions of anonymity, the use of pseudonyms, VPN technologies, blockchain and encryption systems, an objective problem arises of establishing the identity of the offender; 3) the complex nature of the composition of the offense, since Internet offenses combine technical, behavioral, intellectual and other elements, which significantly complicates legal qualification; 4) the multiplicity of regulatory influence, which is manifested in the interaction of national legislation, international legal standards, soft law acts and corporate policies of digital platforms, which creates a multi-level regulatory model.

The classification of types of legal liability for offenses on the Internet is presented: secondary (conditional), self-regulatory, collective, algorithmic (automated), multiple (hybrid). Their essence and content are revealed. The

features of multiple (hybrid) liability for offenses on the Internet are formulated: 1) it is characterized by "double attribution", in which the tortious result is simultaneously the result of volitional decisions of a person and autonomous or semi-autonomous actions of digital systems; 2) it is not reduced to the classical individualization of the subject, but involves the distribution of legal consequences between several levels, in particular, the person who initiates or controls the process, the platform operator, as well as the technical infrastructure that generates the tortious effect; 3) it constitutes a new institution of the general theory of law, which requires: a) the formation of criteria for assessing the degree of algorithmic autonomy and the limits of human control; b) a revision of the traditional categories of fault and negligence in the conditions of an algorithmic environment; c) development of mechanisms of jurisdictional coordination to overcome conflicts of multi-tiered law enforcement.

The types of Internet offenses established in legal doctrine and international practice are summarized and their classification is determined according to the following criteria: 1) by the object of the offense; 2) by the method of commission (depending on methods and technical means); 3) by the principle of jurisdictional affiliation (territorial feature); 4) by the level of public danger. It is stated that the analysis of offenses in cyberspace requires taking into account the features of the digital environment that distinguish them from classical torts within the framework of traditionally established understanding, among which the following are distinguished: 1) lack of territorial certainty; 2) technological complexity of Internet offenses; 3) remoteness and virtualization of actions; 4) anonymity and pseudo-anonymity of the subject; 5) the mass and collective nature of the impact of offenses on the Internet; 6) the blurring of the object of the offense in the digital environment; 7) the variability of legal regulation in the field of Internet offenses; 8) transitivity (transitivity); 9) automated nature; 10) a high level of latency; 11) the interdisciplinary nature of offenses.

The vectors for the development of the institution of legal liability in the digital environment are determined: 1) determining the jurisdictional boundaries of activity in the metaverse; 2) criminalizing new forms of socially dangerous behavior that arise in virtual environments; 3) improving civil law (tort) regulation of harm caused in VR, AR environments and metaverses; 4) implementing the legislative establishment of special obligations of digital platform providers; 5) introducing the so-called "structural liability" of providers, which provides for their obligation to prevent offenses through the platform architecture and moderation algorithms; 6) applying the concept of "digital tort" as a separate category of offense that requires regulatory registration; The following definition of the concept under study is proposed: "digital tort is an unlawful criminal act committed in a virtual environment and characterized by the intangibility of the object of the infringement, cross-border jurisdiction and complicated identification of the subject, resulting in damage to the property or non-property rights of a person, as well as public interests subject to legal protection"; 7) normative definition of the criteria for liability for autonomous decisions made using artificial intelligence systems; 8) introduction of a system of continuous training of judges and investigators on the features of working with digital evidence, methods for establishing a causal relationship in cases of algorithmic decisions, as well as standards for assessing the reliability of software products and digital infrastructure; 9) strengthening Ukraine's participation in existing international mechanisms and initiating new forms of cooperation aimed at ensuring the inevitability of liability regardless of the place of commission of the offense; 10) use of digital technologies as tools to strengthen mechanisms for bringing to justice; 11) consolidation of the principles of digital ethics in the legal sphere with the aim of transforming them into legally significant regulators of behavior, which will allow harmonizing the requirements that society places on the ethics of the functioning of virtual communities with regulatory requirements provided by state coercion.

The need to develop and adopt a special law “On Artificial Intelligence” has been determined to be doctrinally justified. The specified regulatory act should clearly define the criteria for the liability of subjects: the developer, if the damage is caused by a defect in the algorithm, the implementer in the event of improper implementation of the system into the production process, the user in the event of improper or careless use of technology, etc. It was emphasized that it is fundamentally important to establish a norm according to which artificial intelligence systems are not recognized as independent bearers of rights and obligations, and therefore, responsibility always rests with certain individuals or legal entities. It was established that the Draft Law of Ukraine “On Artificial Intelligence” should provide for the following structural elements: Section I. General Provisions; Section II. Classification of artificial intelligence systems by risk level; Section III. Requirements for the creation, implementation and use of artificial intelligence systems; Section IV. Legal responsibility for the use of artificial intelligence systems; Section V. Institutional support for the functioning of artificial intelligence systems; Section VI. Final and transitional provisions. The key provisions of each of the structural parts of the proposed draft law are presented.

Keywords: legal liability, Internet, information technology, digitalization, personal data protection, human rights, offenses, international law, cyberspace, legal regulation, IT law, international cooperation, website, intellectual property, provider.

Список публікацій здобувача наукового ступеня доктора філософії з галузі знань 08 Право за спеціальністю 081 Право

Наукові праці, в яких відображені основні результати дослідження:

1. Худолєй Я. Напрями вдосконалення законодавчого регулювання в контексті легалізації та цифровізації ІТ-бізнесу в мережі Інтернет. *Аналітично-порівняльне правознавство.* 2023. № 02. С. 38–42. DOI: https://doi.org/10.24144/2788-6018.2023.02.6

2. Худолєй Я., Загребельна Н. Захист персональних даних у період дії в Україні правового режиму воєнного стану: загальнотеоретичні аспекти. *«Legal Bulletin»: зб. наук. праць ВНЗ «Університет економіки та права «КРОК».* 2023. Вип. 2(8). С. 75–82. DOI: https://doi.org/10.31732/2708-339X-2023-08-75-82

3. Худолєй Я.Г. Інтерпретація юридичної відповідальності в умовах глобалізації та цифровізації. *Наукові інновації та передові технології.* 2025. № 4 (44). С. 1829–1835. DOI: https://doi.org/10.52058/2786-5274-2025-4(44)-1829-1835

4. Худолєй Я.Г. Класифікаційно-функціональні характеристики юридичної відповідальності у мережі Інтернет. *Актуальні питання у сучасній науці.* 2025. № 4 (34). С. 909–914. DOI: https://doi.org/10.52058/2786-6300-2025-4(34)-909-914

5. Худолєй Я.Г. Поняття та правовий статус кіберпростору у міжнародному праві. *Наука і техніка сьогодні.* 2025. № 4 (45). С. 283–291. DOI: https://doi.org/10.52058/2786-6025-2025-4(45)-283-291

6. Худолєй Я.Г., Бакуменко А.В. Правосуб'єктність штучного інтелекту між юридичною фікцією та онтологічною реальністю. *Legal Bulletin.* 2025. Вип. 4 (18). С. 10–18. DOI: https://doi.org/10.31732/2708-339X-2026-18-A1

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Худолєй Я.Г. Міжнародна операція «Black Axe» та юридична відповідальність за кіберзлочини. *Реалізація конституційного права на свободу пересування в умовах війни: правові стандарти та практичні можливості: матеріали міжнародної правової школи* (м. Ужгород, 24 лютого 2023 р.). Ужгород. 2023. С. 36–38.

8. Худолєй Я.Г. Чинники, що визначають сутність поняття інституту юридичної відповідальності. *Сімдесят четверті економіко-правові дискусії. Серія: Соціальні та гуманітарні науки: матеріали Міжнародної мультидисциплінарної наукової інтернет-конференції* (м. Львів, 25-26 квітня 2023 р). http://www.spilnota.net.ua/ua/article/id-4329/

9. Худолєй Я.Г. Деякі аспекти юридичної відповідальності за правопорушення в мережі Інтернет. *Діяльність органів публічної влади України в умовах війни: пошуки оптимальних моделей: матеріали міжнародної правової школи (м. Ужгород, 11 травня 2023 р.).* Ужгород. 2023. С. 36–38.

10. Худолєй Я.Г. Міжнародне співробітництво у сфері правопорушень в мережі Інтернет. *Міжнародний фактор перемоги України над московією: правові, інституційні, матеріально-технічні складові матеріали міжнародної правової школи (м. Ужгород, 2 червня 2023 р).* Ужгород. 2023. С. 31–35.

11. Худолєй Я.Г. Мережа Інтернет як простір для здійснення правових відносин. *Global Society in Formation of New Security System and World Order: Proceedings of the 2nd International Scientific and Practical Internet Conference* (м. Дніпро, 27–28 липня 2023 р.). http://www.wayscience.com/wp-content/uploads/2023/08/Conference-Proceedings-July-27-28-2023-1.pdf

12. Худолєй Я.Г. Юридичні особи та їх відповідальність за дії в мережі Інтернет. *Інноваційні дослідження та перспективи розвитку науки і техніки у XXI столітті: Міжнародна науково-практична конференція до 30-річчя*

Приватного вищого навчального закладу «Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука» (м. Рівне, 19 жовтня 2023 р).
https://dspace.megu.edu.ua:8443/jspui/handle/123456789/4419

13. Худолєй Я.Г. Цифрова термінологія у міжнародно-правовій площині. *Правові проблеми мобільності в умовах надзвичайних режимів: конституційні, економічні, соціальні, культурні та духовні аспекти: матеріали міжнародної правової школи, м. Ужгород, 27 лютого 2025 р.* Ужгород: Ужгородський національний університет. 2025. С. 67–73.

14. Худолєй Я.Г. Методологічні орієнтири дослідження юридичної відповідальності в умовах інформаційного суспільства. *Українська жінка в умовах війни: міждисциплінарний дискурс: матеріали міжнародної правової школи. м. Ужгород. 28 березня 2025 р.* Ужгород: Ужгородський національний університет. 2025. С. 84–86.

ЗМІСТ

ВСТУП

Обґрунтування вибору теми дослідження. Сучасне суспільство функціонує в умовах стрімкої цифровізації, що зумовлює появу якісно нових форм соціальних відносин, у тому числі й правових. Мережа Інтернет перетворилася на глобальне середовище комунікації, торгівлі, наукової співпраці та реалізації прав людини, водночас зумовивши появу комплексу нових викликів, пов’язаних із вчиненням правопорушень у віртуальному просторі. Окрім цього, зростання кількості правопорушень у кіберпросторі, їхня латентність та високий рівень суспільної небезпеки потребують доктринального переосмислення природи юридичної відповідальності. Зазначене передбачає необхідність вироблення якісно нового загальнотеоретичного позиціювання сутності та ознак відповідальності за інтернет-правопорушення.

Актуальність теми зумовлюється також тим, що фрагментарність існуючих нормативних стандартів і нерівномірність їх імплементації державами створюють додаткові загрози для прав людини, національної безпеки та довіри до правосуддя, що вимагає формування цілісної доктрини юридичної відповідальності у цифровому середовищі, здатної забезпечити належну кореляцію між ефективністю притягнення до відповідальності та дотриманням фундаментальних прав і свобод.

Теоретичну базу дослідження проблематики юридичної відповідальності за правопорушення у мережі Інтернет становлять праці таких вітчизняних та зарубіжних учених, як: О. М. Балинська, О. О. Бандура, О. М. Биков, М. М. Гуренко, О. М. Джужа, Ю. М. Жорнокуй, Н. А. Загребельна, В. О. Карпічков, М. С. Кельман, О. І. Колич, В. В. Корольова, М. П. Кучерявенко, О. В. Мікічурова, В. В. Неволя, К. Г. Некіт, А. С. Овчаренко, Ю. Ю. Орлов, В. Ю. Полатай, С. В. Прийма, П. М. Рабінович, О. В. Ришкова, В. П. Сабадаш, В. В. Савченко, О. Ф. Скакун, В. Б. Скоморовський, Є. М. Смичок, К. І. Спасова, Н. В. Степаненко,

О. О. Тихомиров, Б. П. Ткачук, О. О. Хорватова, А. В. Чуб, В. А. Ященко, R. Abbot, Y. Afina, L. Aiello, L. Alessandretti, M. Allen, M. Almada, S. Alon-Barkat, J. Annas, G. Arslan, I. Ayres, A. Baronchelli, M. Barratt, G. Borges, M. Buiten, W. Burkert, M. Busuioc, R. Calo, P. Charon, B. El-Darwiche, L. Floridi, M. Foulon, R. Friedrich, S. Ganediwalla, M. Gobble, M. Gradillas, T. Haartsen, J. Hazenberg, D. Hillier, Yu. Hong, E. Karner, R. Katz, D. Kaushik, L. Kello, T. Khinvasara, G. Kirk, I. Koto, R. Kraut, A. Laks, S. Lazarus, S. Lenton, M. Martino, G. Meibauer, A. Michienzi, W. Mincewicz, R. Morrison, J. Palmer, M. Schmitt, S. J. Shackelford, M. Shanthi, L. Strikwerda, K. Sudhakar, C. Taylor, G. Teubner, L. Thomas, N. Wang, S. Wingreen, P. Wong, A. Woods, L. Zhmud, J. Zhou, A. Zwitter та ін.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження виконано в межах науково-дослідної теми кафедри теорії та історії держави і права юридичного факультету Вищого навчального закладу «Університет економіки та права «КРОК»: «Теоретичні та практичні проблеми забезпечення прав людини та дитини в умовах розбудови правової, демократичної, соціально орієнтованої держави з широко розгалуженими інститутами громадянського суспільства» (номер державної реєстрації: 0118U001384). Результати дослідження мають безпосередній зв'язок із навчальною діяльністю юридичного факультету та можуть бути використані при підготовці й оновленні навчальних планів і програм, зокрема в дисципліні теорії держави та права, інформаційне право. Такий підхід забезпечує інтеграцію сучасних практик і положень Національної стратегії у сфері прав людини, затвердженої Указом Президента України від 24 березня 2021 року №119/2021, у навчальний процес, що дозволяє студентам здобувати знання на основі актуальних нормативних документів та реальних практик їх застосування.

Мета і завдання дослідження. Метою дисертаційного дослідження є комплексне загальнотеоретичне обґрунтування юридичної відповідальності за правопорушення у мережі Інтернет.

Для досягнення цієї мети дисертантом було визначено наступні **завдання:**

– проаналізувати еволюцію доктринальних підходів до інституту юридичної відповідальності;

– з'ясувати правову природу кіберпростору та Інтернету як особливого середовища виникнення та реалізації правовідносин;

– дослідити міжнародні стандарти у сфері юридичної відповідальності за правопорушення у мережі Інтернет;

– виявити та систематизувати комплекс загальнотеоретичних характеристик інтернет-правопорушень, надати їм правову кваліфікацію;

– визначити проблемні аспекти реалізації юридичної відповідальності у цифровому середовищі;

– обґрунтувати перспективи модернізації досліджуваного інституту в умовах глобалізації та цифровізації.

Об'єктом дослідження є суспільні відносини у сфері юридичної відповідальності, що виникають у цифровому середовищі, зокрема у мережі Інтернет.

Предметом дослідження є загальнотеоретичні засади юридичної відповідальності за правопорушення в мережі Інтернет, її сутність і ознаки, міжнародні стандарти у цій сфері, особливості правової кваліфікації інтернет-правопорушень, а також перспективи модернізації інституту юридичної відповідальності в умовах цифровізації.

Методи дослідження. Методологічну основу дисертації становить комплекс загальнонаукових, спеціально-юридичних та міждисциплінарних методів, застосування яких забезпечило всебічність і системність аналізу інституту юридичної відповідальності в умовах цифровізації суспільства та поширення інтернет-правопорушень.

Діалектичний метод використано як загальнофілософську основу для пізнання сутності юридичної відповідальності, її динаміки та трансформацій у цифровому середовищі, а також для аналізу взаємозв'язку між

традиційними і новітніми підходами до регулювання правовідносин у кіберпросторі (розділи 1-3). Аксіологічний метод використано для розкриття ціннісного виміру юридичної відповідальності у цифровому середовищі, зокрема її ролі як гарантії захисту прав людини, забезпечення довіри до державних і міжнародних інституцій та розвитку цифрової етики (підрозділи 2.1; 3.2). Формально-юридичний метод застосовано для аналізу норм національного та міжнародного законодавства, що регулюють відповідальність за правопорушення в Інтернеті, а також для виявлення прогалин та колізій у досліджуваній сфері (розділи 2, 3). Порівняльно-правовий метод дозволив проаналізувати міжнародні універсальні та регіональні стандарти у сфері юридичної відповідальності за правопорушення у мережі Інтернет (розділ 2). Кібернетичний метод було використано для дослідження правових процесів у цифровому середовищі з урахуванням принципів інформаційних технологій, алгоритмізації та мережевої організації (розділи 2, 3). Метод правового прогнозування дозволив визначити вектори розвитку юридичної відповідальності в умовах цифровізації, зокрема в контексті метавсесвіту та використання штучного інтелекту (підрозділ 3.2).

Наукова новизна одержаних результатів полягає в тому, що дисертація є одним із перших у вітчизняній юридичній науці комплексним монографічним дослідженням інституту юридичної відповідальності за правопорушення у мережі Інтернет у загальнотеоретичному аспекті. У роботі здійснено системне теоретико-методологічне обґрунтування сутності та ознак юридичної відповідальності у цифровому середовищі, розкрито закономірності її трансформації під впливом глобалізації, міжнародних стандартів і розвитку новітніх технологій, а також сформульовано концептуальні підходи до модернізації інституту відповідальності з урахуванням специфіки кіберпростору та інтернет-правопорушень.

У процесі дослідження автором сформульовано низку науково обгрунтованих положень та висновків, котрі містять наукову новизну:

вперше:

– представлено модель багаторівневої юридичної відповідальності, котра передбачає взаємодію кількох взаємопов'язаних рівнів, що відображають сучасні тенденції розвитку правового регулювання: 1) на державному рівні зберігається класична архітектоніка юридичної відповідальності, яка реалізується через кримінально-правові, адміністративно-правові, цивільно-правові механізми тощо; 2) на міжнародному рівні юридична відповідальність набуває форми юрисдикції міжнародних судових та квазісудових органів, а також виражається у виконанні державами зобов'язань за міжнародними договорами; 3) недержавний рівень відповідальності охоплює механізми саморегулювання, зокрема цифрову етику, корпоративні кодекси поведінки, внутрішні регламенти цифрових платформ; зазначений рівень відображає нові форми юридично значущого впливу, що виникають у межах цифрового середовища та доповнюють класичні державні й міжнародні інструменти;

– репрезентовано авторську класифікацію юридичної відповідальності за правопорушення в мережі Інтернет та виокремлено такі її різновиди: вторинна (умовна), саморегуляторна, колективна, алгоритмічна (автоматизована), множинна (гібридна); розкрито їх сутність та зміст;

– визначено, юридична відповідальність у сфері штучного інтелекту поступово набуває рис об'єктивної (суворої) відповідальності, подібної до моделі відповідальності за шкоду, завдану дефектною продукцією; у контексті цифрових технологій вказана відповідальність стає ефективним інструментом правового реагування на складні, технічно опосередковані випадки спричинення шкоди; акцентовано, концепція відповідальності за ризик як альтернатива традиційному поняттю вини є перспективною парадигмою для оновлення інституту юридичної відповідальності; підкреслено, у сфері штучного інтелекту відповідальність повинна покладатися не на агента, що має волю та намір, а на суб'єкта, який створив або експлуатує джерело технологічного ризику;

– встановлено доктринально обґрунтованою необхідність розробки та прийняття Закону України «Про штучний інтелект», у котрому повинні бути чітко визначені критерії відповідальності суб'єктів: розробника, якщо шкода спричинена дефектом алгоритму, впроваджувача, у разі неналежного впровадження системи у виробничий процес, користувача, за умови неправомірного або необережного застосування технології тощо; наголошено, принципово важливим є закріплення норми, згідно з якою системи штучного інтелекту не визнаються самостійними носіями прав і обов'язків, а отже, відповідальність завжди покладається на визначених фізичних або юридичних осіб; репрезентовано ключові положення кожної з структурних частин запропонованого законопроєкту;

удосконалено:

– понятійно-термінологічний апарат у досліджуваній сфері, уніфіковано та уточнено дефініції, серед яких «правопорушення в Інтернеті», «цифровий делікт», «алгоритмічна відповідальність», «саморегуляторні механізми», «структурна відповідальність провайдерів», що усуває семантичні суперечності між галузями, підвищує якість законодавчої техніки, забезпечує єдність судової практики та гармонізацію з європейськими і глобальними стандартами;

– наукові висновки щодо міжнародних стандартів у сфері юридичної відповідальності за інтернет-правопорушення: 1) міжнародна нормативна база у цій сфері є фрагментованою за географічною та предметною ознакою, проте спостерігається тенденція до її уніфікації; 2) входження до глобальних домовленостей значно ширшого кола держав з різними правовими системами породжує виклик дотримання прав людини; як показав аналіз фінального тексту конвенції ООН, відсутність жорстких гарантій може бути використана авторитарними режимами для переслідування інакодумців під приводом боротьби з кіберзлочинами; 3) найбільше розвинені стандарти стосуються саме кримінальної відповідальності, що історично обумовлено першочерговим фокусом на кіберзлочинності; натомість міжнародні

механізми цивільно-правової та адміністративної відповідальності розвинені значно менше та носять характер радше рекомендацій, ніж обов'язкових норм; встановлено, у перспективі варто очікувати розвитку саме таких *«горизонтальних»* стандартів, зокрема у сфері відповідальності постачальників цифрових послуг; 4) ефективність міжнародних стандартів корелюється із належною імплементацією на національному рівні; навіть після приєднання до міжнародних договорів окремі держави не забезпечують повної гармонізації внутрішнього законодавства; не всі передбачені Конвенцією про кіберзлочинність діяння отримують належну криміналізацію, а процесуальні механізми щодо збирання та вилучення електронних доказів залишаються фрагментарними; у цьому зв'язку пріоритетного значення набувають системний моніторинг виконання міжнародних зобов'язань і надання державам технічної допомоги в процесі їх імплементації;

– наукові позиції щодо розуміння ознак множинної (гібридної) відповідальності за правопорушення у мережі Інтернет: 1) характеризується «подвійною атрибуцією», за якої деліктогенний результат одночасно є наслідком вольових рішень людини та автономних або напівавтономних дій цифрових систем; 2) не зводиться до класичної індивідуалізації суб'єкта, а передбачає розподіл правових наслідків між кількома рівнями, зокрема особою, яка ініціює чи контролює процес, оператором платформи, а також технічною інфраструктурою, що генерує правопорушний ефект; 3) становить новий інститут загальної теорії права, що вимагає: а) формування критеріїв оцінки ступеня алгоритмічної автономії та меж людського контролю; б) перегляду традиційних категорій вини та необережності в умовах алгоритмізованого середовища; в) вироблення механізмів юрисдикційної координації для подолання колізій багатоярусного правозастосування;

– положення щодо систематизації особливостей цифрового середовища, що відмежовують їх від класичних деліктів у межах традиційно усталеного розуміння, серед яких виокремлено наступні: 1) відсутність

територіальної визначеності; 2) технологічна складність правопорушень у мережі Інтернет; 3) дистанційність та віртуалізація дій; 4) анонімність та псевдоанонімність суб'єкта; 5) масовість та колективний характер впливу правопорушень у мережі Інтернет; 6) розмитість об'єкта правопорушення у цифровому середовищі; 7) варіативність правового регулювання у сфері Інтернет-правопорушень; 8) транзитивність (перехідність); 9) автоматизований характер; 10) високий рівень латентності; 11) міждисциплінарний характер правопорушень;

– усталені у правовій доктрині та міжнародній практиці різновиди правопорушень у мережі Інтернет і визначено їх класифікацію за наступними критеріями: 1) за об'єктом посягання; 2) за способом здійснення (залежно від методів і технічних засобів); 3) за принципом юрисдикційної належності (територіальною ознакою); 4) за рівнем суспільної небезпеки;

– наукові погляди, відповідно до яких цифрові активи у вигляді невзаємозамінних токенів, віртуальної нерухомості та інших нематеріальних об'єктів набувають ознак майнової цінності та потребують правового режиму, подібного до інституту нематеріального майна у цивільному праві; підкреслено, що моделі корпоративного (приватного) регулювання, засновані на правилах спільнот, не здатні забезпечити рівнозначний захист прав особи, порівняно з публічно-правовими механізмами, що обґрунтовує потребу державного втручання та встановлення загальнообов'язкових стандартів відповідальності у цифровому середовищі;

набули подальшого розвитку:

– наукові підходи щодо співвідношення у правовому вимірі понять «кіберпростір» та «мережа Інтернет» як широкої за сутністю й змістом категорії та її інфраструктурної основи; встановлено, їх поєднують спільні цінності, але відрізняє предмет регулювання, рівень інституціоналізації та специфіка суб'єктного складу управління; наголошено, кіберпростір слід розглядати як глобальне соціально-технічне середовище, що поєднує

інформаційні потоки та комунікаційні системи, не має фізичних меж, однак генерує реальні правові наслідки; мережа Інтернет у системі кіберпростору виконує роль матеріальної та організаційної інфраструктури, яка забезпечує функціонування кіберпростору, проте водночас формує власний специфічний правовий режим;

– ключові характеристики юридичної відповідальності за правопорушення в мережі Інтернет: 1) *транснаціональний характер*, оскільки переважна більшість правопорушень в мережі Інтернет виходить за межі національних юрисдикцій, що зумовлює складнощі у визначенні компетентного органу та виборі застосовного права; 2) *ускладнена ідентифікація суб'єкта,* позаяк в умовах анонімності, використання псевдонімів, VPN-технологій, блокчейну та систем шифрування постає об'єктивна проблема встановлення особи правопорушника; 3) *комплексний характер складу правопорушення*, адже правопорушення в мережі Інтернет поєднують технічні, поведінкові, інтелектуальні та інші елементи, що значно ускладнює правову кваліфікацію; 4) *множинність нормативного впливу*, яка проявляється у взаємодії норм національного законодавства, міжнародно-правових стандартів, актів м'якого права та корпоративних політик цифрових платформ, що створює багаторівневу модель регулювання;

– положення, згідно яких міжнародні стандарти у сфері юридичної відповідальності за правопорушення у мережі Інтернет дедалі більше зміщуються у бік комплексного механізму шляхом поєднання відповідальності з просвітою користувачів, кібергігієною, партнерством з приватним сектором та повагою до відкритості мережі; нові міжнародні документи та ініціативи мають шанс закріпити й розвинути зазначені принципи; аргументовано, сьогодні міжнародні стандарти у сфері юридичної відповідальності за інтернет-правопорушення знаходяться в стадії динамічного розвитку, позаяк від фрагментарних регіональних норм вони еволюціонують до цілісної системи універсальних правил, що

враховують як потребу у безпеці, так і необхідність збереження фундаментальних прав і свобод у цифрову епоху;

– вектори розвитку інституту юридичної відповідальності у цифровому середовищі: 1) визначення юрисдикційних меж діяльності у метавсесвіті; 2) криміналізація нових форм суспільно небезпечної поведінки, що виникають у віртуальних середовищах; 3) вдосконалення цивільно-правового (деліктного) регулювання шкоди, завданої у VR-, AR-середовищах та метаверсах; 4) здійснення законодавчого встановлення спеціальних обов'язків провайдерів цифрових платформ; 5) впровадження так званої «структурної відповідальності» провайдерів, яка передбачає їх обов'язок запобігати правопорушенням через архітектуру платформи та алгоритми модерації; 6) застосування концепції «цифрового делікту» як окремої категорії правопорушення, що вимагає нормативного оформлення; запропоновано наступне визначення досліджуваному поняттю «цифровий делікт – це протиправне винне діяння, що здійснюється у віртуальному середовищі і характеризується нематеріальністю об'єкта посягання, транскордонністю юрисдикції та ускладненою ідентифікацією суб'єкта, внаслідок чого завдається шкода майновим чи немайновим правам особи, а також суспільним інтересам, які підлягають правовій охороні»; 7) нормативне визначення критеріїв відповідальності за автономні рішення, що приймаються із застосуванням систем штучного інтелекту; 8) запровадження системи безперервного навчання суддів та слідчих щодо особливостей роботи з цифровими доказами, методів встановлення причинно-наслідкового зв'язку у випадках алгоритмічних рішень, а також стандартів оцінки надійності програмних продуктів і цифрової інфраструктури; 9) посилення участі України у діючих міжнародних механізмах та ініціювання нових форм співробітництва, спрямованих на забезпечення невідворотності відповідальності незалежно від місця вчинення правопорушення; 10) використання цифрових технологій як інструментів підсилення механізмів притягнення до відповідальності; 11) закріплення принципів

цифрової етики у правовій площині з метою їх трансформації у юридично значущі регулятори поведінки, що дозволить узгодити вимоги, які висуває суспільство до етичності функціонування віртуальних спільнот, із нормативними приписами, що забезпечуються державним примусом.

Практичне значення отриманих результатів. Викладені у дисертації пропозиції та висновки можуть бути використані у:

– науково-дослідній сфері – для подальшої розробки проблематики юридичної відповідальності в цифровому середовищі; уточнення дефініцій та формування нових підходів до класифікації інтернет-правопорушень і їх правової кваліфікації; розробки міждисциплінарних методик дослідження правопорушень у мережі Інтернет;

– правотворчій діяльності – під час оновлення та гармонізації законодавства України у сферах кібербезпеки, захисту персональних даних; при підготовці проєктів законів та підзаконних актів з урахуванням міжнародних стандартів; для запровадження спеціальних обов'язків платформ і механізмів «структурної» та «вторинної» відповідальності;

– правозастосовній практиці – для підвищення ефективності діяльності судів, правоохоронних органів у справах про інтернет-правопорушення;

– навчальному процесі – для оновлення програм, підготовки навчально-методичних матеріалів, при викладанні курсів «Теорія держави і права», «Інтернет-право/Кіберправо», «Міжнародні стандарти у цифровому середовищі», «Захист персональних даних», «Порівняльне правознавство» тощо.

Апробація результатів дисертації. Результати дослідження було репрезентовано на засіданнях кафедри теорії та історії держави і права юридичного факультету ЗВО «Університет економіки та права «КРОК». Окремі положення, висновки, пропозиції та рекомендації, сформульовані в дисертації, отримали апробацію на міжнародних науково-практичних конференціях, а також у роботі міжнародних правових шкіл: «Діяльність

органів публічної влади України в умовах війни: пошуки оптимальних моделей» (м. Ужгород, 11 травня 2023 р); «Міжнародний фактор перемоги України над московією: правові, інституційні, матеріально-технічні складові» (м. Ужгород, 2 червня 2023 р); «Реалізація конституційного права на свободу пересування в умовах війни: правові стандарти та практичні можливості»
(м. Ужгород, 24 лютого 2023 р); «Правові проблеми мобільності в умовах надзвичайних режимів: конституційні, економічні, соціальні, культурні та духовні аспекти» (м. Ужгород, 27 лютого 2025 р); «Українська жінка в умовах війни: міждисциплінарний дискурс» (м. Ужгород, 28 березня 2025 р); «Modern Problems of Science and Technology» (September 22–24, 2025, Tallinn, Estonia).

Публікації. Основні результати дисертаційного дослідження висвітлені в 14 наукових публікаціях, у тому числі у 6 статтях, опублікованих в Україні у виданнях, визначених фаховими для юридичних наук, і 8 тезах доповідей на наукових та науково-практичних конференціях та міжнародних правових школах.

Структура дисертації. Дисертація складається зі вступу, трьох розділів, що поділяються на шість підрозділів, висновків до розділів, загальних висновків, списку використаних джерел та додатків. Загальний обсяг дисертаційної роботи становить 228 сторінок, з них основного тексту – 175 сторінок. Список використаних джерел становить 227 найменувань.

РОЗДІЛ 1
ТЕОРЕТИКО-ПРАВОВІ ОСНОВИ ДОСЛІДЖЕННЯ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ У ЦИФРОВУ ЕПОХУ

1.1. Юридична відповідальність як правовий інститут: еволюція доктринальних підходів

Посилення ролі інституту юридичної відповідальності зумовлене об'єктивними завданнями побудови правової держави та впровадженням у правозастосовну практику принципу взаємної відповідальності держави та особи. Її значущість набуває особливої актуальності в умовах політико-правових трансформацій, зумовлених триваючою анексією та тимчасовою окупацією частини територій України, що супроводжуються погіршенням соціально-економічних умов, зниженням рівня добробуту населення та системними порушеннями прав і свобод людини й громадянина.

У науковій літературі юридична відповідальність традиційно розглядається як багатовимірне явище, концептуалізація якого спирається на значний теоретичний доробок попередніх епох, що дозволяє простежити еволюцію функціонального призначення цього інституту та закономірності його розвитку. У доктринальному вимірі юридична відповідальність постає як механізм державного примусу та інструмент впорядкування суспільних відносин, що поєднує у собі історично вироблені цінності та сучасні підходи.

Слід підкреслити, що питання юридичної відповідальності не є виключно продуктом правової науки. Його ґенеза має глибокі історико-філософські корені, що сягають періоду античності, доби, яка заклала засадничі основи для формування категоріального апарату філософії, етики та права. Вказане свідчить про давність відповідного концепту та про його фундаментальну значущість у структурі правового мислення.

Первинні уявлення про обов'язок, справедливість і відплату стали вихідною основою для формування правових норм у сфері юридичної

відповідальності, які з часом набули системного характеру. У найдавніших зразках письмової культури та філософської рефлексії античних мислителів виокремлюються перші спроби інтерпретувати феномен відповідальності як етичну норму індивідуальної поведінки. Так, у поемах Гомера наявна ідея неминучої відплати за вчинене, як у вигляді божественного втручання, так і через суспільну реакцію. Гесіод у творі «Робота і дні» вказує на важливість дотримання справедливості та морального обов'язку [5; 19].

У спадщині піфагорійської школи категорія відповідальності постає у тісному зв'язку з онтологічною концепцією гармонії, що вбачалася універсальним принципом організації космосу та людської душі. За вченням Піфагора, гармонія є математичною пропорцією та етичним законом, який визначає належний спосіб життя людини у співвідношенні із загальним порядком буття [127; 168]. Відповідальність у такій системі координат набувала значення внутрішньої дисципліни, моральної чистоти та самовдосконалення, що розглядалися як умова підтримання справедливого суспільного устрою. Важливо, що Піфагор та представники його школи заклали підвалини для пізнішого уявлення про взаємозалежність особистої відповідальності та колективного блага [161, с. 85–124; 226].

У філософії Геракліта поняття відповідальності тісно пов'язується з його вченням про Логос як універсальний закон космосу, що визначає порядок буття та поведінки людини. На думку мислителя, кожна особа наділена свободою вибору, однак реалізація цієї свободи неминуче супроводжується відповідальністю за наслідки вчинених дій [172; 181]. Логос у цьому ключі постає мірилом правомірності поведінки, а відхилення від нього тлумачиться як джерело дисгармонії, що спричиняє покарання чи негативні наслідки. У зазначеному аспекті відповідальність набуває характеру обов'язку діяти відповідно до загального закону буття, а не тільки до суб'єктивних переконань чи локальних норм.

Філософські ідеї Демокріта та Сократа істотно поглиблюють розуміння феномена відповідальності, що виходить за межі його розуміння

виключно як зовнішнього примусу. Демокріт розглядав свободу людини крізь призму атомістичного детермінізму, акцентував на усвідомленості індивідуальних дій, внаслідок чого відповідальність набуває значення внутрішнього обов'язку дотримання моральних цінностей та розумного способу життя [176; 215]. Сократ визначав відповідальність як невіддільну властивість моральної особистості, що ґрунтується на знанні добра та справедливості. Незнання у цьому контексті не усуває обов'язку діяти відповідно до об'єктивних моральних законів, а вказує на необхідність самопізнання та самодисципліни [125, с. 55–69; 195, с. 482].

У зазначених концепціях простежується тенденція до виокремлення етичної та соціальної відповідальності, що мало суттєве значення для подальшої інституціоналізації юридичної відповідальності як санкціонованої державою форми реагування на порушення встановлених норм. З огляду на це, у вченні античних мислителів вбачається зародження фундаментальної ідеї про взаємозалежність внутрішньої моральної автономії особи та зовнішніх механізмів правового впливу, яка становить підґрунтя доктринального розуміння інституту юридичної відповідальності [14; 15, с. 782–784; 20].

У політико-правовій доктрині Платона вперше здійснено цілісне концептуальне осмислення взаємозв'язку між індивідом, державою та правом, в котрому центральне місце посідає ідея блага, яка функціонує як критерій оцінки індивідуальної поведінки та діяльності публічної влади [124, с. 165– 166]. Відповідальність у платонівській традиції виходить за межі суто примусового механізму та набуває характеру ціннісно орієнтованого інституту, покликаного забезпечити гармонію між приватним і публічним началами. Арістотель розвинув зазначені положення та розглядав відповідальність крізь призму причинності, волі та наміру, чим започаткував доктринальне підґрунтя для інституціоналізації категорії вини як системоутворюючого елемента юридичної відповідальності [116; 174]. Вказане бачення дозволило поєднати етичний вимір із правовим та надало

можливість індивідуалізувати відповідальність залежно від внутрішніх і зовнішніх факторів вчинку. Відтак, у концепціях Платона та Арістотеля простежується перехід від морально-філософських уявлень про обов'язок і справедливість до формування засадничих положень правової доктрини відповідальності, які залишаються релевантними і у сучасному юридичному дискурсі [2; 38, с. 3–14; 55; 78, с. 36].

У вченні Епікура категорія відповідальності тісно пов'язується з концепцією свободи волі, яка визнається необхідною передумовою для покладення на особу обов'язку відповідати за власні дії. Відхід мислителя від детерміністичної моделі попередніх шкіл знаходить вираження у положенні про самочинне відхилення атомів, що забезпечує можливість вибору та, відповідно, моральну автономію індивіда [111, с. 5–21]. У цьому контексті Епікур проводить розмежування між природними законами, які діють об'єктивно, та правовими нормами, що виникають унаслідок суспільного договору і мають на меті гарантування спокою та безпеки в суспільстві [192, с. 1–8]. Відповідальність, таким чином, розглядається як похідна від свободи волі та водночас як умова функціонування права, що спрямоване на впорядкування міжособистісних відносин та забезпечення соціальної стабільності [6].

Антична філософська традиція сформувала концептуальні засади, що згодом стали підґрунтям для становлення юридичної відповідальності як багаторівневого явища, яке поєднує моральний, соціальний та правовий виміри. Систематизовані у цей період уявлення про свободу волі, справедливість, обов'язок та причинність визначили вихідні орієнтири для подальшої еволюції доктрини відповідальності. Надалі зазначені підходи отримали розвиток у середньовічній правовій думці, що поєднувала морально-релігійні та юридичні уявлення, і стали теоретичною основою правової науки, у якій юридична відповідальність розглядається як системоутворюючий інститут.

Так як зазначалось вище, юридична відповідальність традиційно розглядається як один з фундаментальних інститутів права, нерозривно пов'язаний із реалізацією санкцій за правопорушення. В якості правового інституту досліджуваний феномен являє собою системну сукупність правових норм та принципів, що регулюють підстави й порядок притягнення до відповідальності, види стягнень та наслідки правопорушень.

Подальше дослідження вимагає звернення до доктринальних інтерпретацій категорії юридичної відповідальності, запропонованих у сучасній науковій літературі, а також аналіз тих дефініцій, які формулюють провідні дослідники у галузі теорії та філософії права.

Юридична відповідальність – це застосування до правопорушника заходів державного примусу, що виражаються у формі позбавлення певних благ або покладання додаткових обов'язків» [69, с. 20]. Подібно визначає цю категорію П. М. Рабінович та підкреслює її карально-обтяжливу сутність: «юридична відповідальність – це закріплений у законодавстві і забезпечуваний державою додатковий юридичний обов'язок правопорушника зазнати позбавлення належних йому певних цінностей» [63, с. 133].

Як соціально-правове явище, юридична відповідальність є різновидом соціальної відповідальності, що врегульована нормами права. Інакше кажучи, це специфічна форма підзвітності особи перед суспільством і державою за свою поведінку. Зокрема, М. С. Кельман та О. Г. Мурашин підкреслюють, що юридична відповідальність становить собою саме соціальну відповідальність, але регламентовану правовими нормами. Її настання завжди пов'язане з порушенням приписів права, і саме наявність правопорушення є необхідною передумовою для виникнення охоронних правовідносин відповідальності. У цих правовідносинах держава в особі уповноважених органів вступає у специфічний зв'язок із правопорушником, змістом якого є обов'язок правопорушника зазнати визначених законом обмежень, а метою – відновлення порушеного правового становища, покарання винного та

запобігання новим правопорушенням [27]. Відтак юридична відповідальність виконує охоронно-каральну функцію, оскільки є засобом державного примусу, що слугує забезпеченню суспільного порядку й справедливості, а водночас виступає формою негативної реакції держави на протиправну поведінку [26].

Разом із тим інститут юридичної відповідальності не можна зводити виключно до примусу чи санкції. У правовій доктрині підкреслюється, що державно-правовий примус є поняттям ширшим, ніж власне юридична відповідальність, позаяк не всякий примусовий захід у праві означає притягнення до відповідальності. Держава застосовує й інші заходи впливу, зокрема, попереджувальні, відновлювальні тощо, які виходять за межі відповідальності. На відміну від таких заходів, юридична відповідальність завжди передбачає елемент осуду винного та покарання, а її реалізація відбувається у визначеній процесуальній формі з додержанням встановлених процедур.

У своїй статті Н. А. Загребельна та А. С. Дубовой підкреслюють, що незважаючи на наявність різних наукових підходів до тлумачення досліджуваного феномена, у сучасній правовій доктрині переважає дуалістичне розуміння юридичної відповідальності як засобу забезпечення стабільності правопорядку та превенції правопорушень. При цьому відповідальність виявляється не лише у формально-правовій площині, але й у ширшому соціальному та морально-етичному контексті, що зумовлює її багатовимірний характер та міждисциплінарну значущість [25, с. 17–23].

Однією з найвідоміших доктринальних дискусій, що відобразила еволюцію поглядів на природу юридичної відповідальності, є питання про позитивну і негативну відповідальність. Традиційно під юридичною відповідальністю розумілося ретроспективне реагування на правопорушення, тобто негативна відповідальність, саме такий зміст закріплений у більшості наведених вище визначень. Водночас у другій половині XX ст. в радянській та подальшій пострадянській теорії права з’явилась і набула поширення ідея

перспективної або позитивної відповідальності, що вказує на добровільне, свідоме виконання юридичних обов'язків і загальну правомірну поведінку суб'єкта як різновид «відповідального» ставлення до вимог закону [167, с. 240–259; 209, с. 779–784].

Загальна суть концепції позитивної юридичної відповідальності полягає в тому, що відповідальність розглядається не лише як покарання за минулі правопорушення, але й як характеристика поведінки особи до вчинення порушення, її готовність належним чином виконувати свої обов'язки. Позитивна відповідальність – це добросовісне, сумлінне ставлення суб'єкта до здійснення покладених на нього правових обов'язків [117, с. 1–11]. Вважається, що така відповідальність існує ще до вчинення правопорушення і полягає радше у внутрішньому усвідомленні обов'язку та психологічній готовності діяти правомірно [178, с. 402–409; 222].

Однак концепція позитивної юридичної відповідальності є дискусійною. Багато теоретиків наголошують, що настільки різні явища як «належна правомірна поведінка» та «покарання за її порушення» некоректно об'єднувати одним терміном «відповідальність». Зокрема О. М. Харитонов та Є. О. Харитонова підкреслюють, що основою негативної юридичної відповідальності є правова оцінка діяння, тоді як основою позитивної відповідальності є оцінка моральна, що властива радше етиці, а не праву. Дослідники вважають вказаний поділ штучним та таким, що не відповідає природі зазначеного явища [86, с. 23–30].

Втім варто підкреслити, що поява та розвиток концепції позитивної відповідальності відображають прагнення доктрини подивитися ширше на досліджуваний феномен та побачити у ньому попри каральний, також превентивно-виховний зміст. У науковому дискурсі набув поширення так званий «двохаспектний» підхід, спрямований на поєднання позитивного та негативного вимірів юридичної відповідальності. Його прихильники обґрунтовують доцільність визнання подвійної природи цього феномена, та виокремлюють, з одного боку, позитивний аспект, що виражається у

добровільному та свідомому додержанні правових приписів, а з іншого – негативний аспект, що виявляється у формі державно-примусового осуду за правопорушення. У межах цієї концепції термін «відповідальність» зберігає значення як характеристики належної поведінки, так і санкціонованого державою покарання, проте здійснюється їхнє чітке змістове розмежування. Водночас навіть у двохаспектній інтерпретації поняття відповідальності зберігає внутрішню неоднорідність, що потенційно знижує його наукову точність та практичну ефективність [43, с. 74–85].

Слід констатувати, що розгляд юридичної відповідальності як правового інституту буде неповним без врахування міждисциплінарних підходів, які висвітлюють додаткові грані цього явища. Право не існує у вакуумі, оскільки взаємодіє з психологією, етикою, соціологією та технологічними науками, а відповідальність у цих дисциплінах розглядається під різними кутами.

З точки зору юридичної психології, відповідальність нерозривно пов’язана з усвідомленням особою своїх вчинків і з відчуттям провини. Психологічний аспект відповідальності базується на можливості вибору, на свідомому прийнятті рішення щодо лінії поведінки та готовності нести за цей вибір наслідки. У праві вказане відображається у понятті вини, а винність визначається як психічне ставлення особи до свого протиправного діяння, і наявність вини є передумовою притягнення до відповідальності. Вказане бачення вплинуло і на доктринальні підходи. Ті концепції, що трактують відповідальність через правосвідомість, деліктоздатність, елементи статусу особи фактично спираються на психологічне підґрунтя. Сучасні дослідження також звертають увагу на роль каяття, мотивів, емоційного стану правопорушника при оцінці його відповідальності, що відображається у пом’якшенні чи обтяженні санкцій. Відтак психологічний вимір додає глибини розумінню відповідальності та показує її зв’язок із свідомістю та волею людини [62].

У теорії права набув поширення і соціологічний погляд на інститут відповідальності, згідно з яким відповідальність розглядається як соціально-функціональний механізм підтримання нормативного порядку. Соціологія права підкреслює, що юридична відповідальність виконує важливу соціальну роль, позаяк реалізує суспільне засудження протиправної поведінки й тим самим утверджує силу правових норм та цінностей. На думку науковця І. А. Безклубого, сьогоденна правова наука все більше схиляється до сприйняття сутності інституту відповідальності саме у соціологічному ключі. Зазначене передбачає акцент на її соціальних наслідках і ефективності, чи досягає покарання мети загального й спеціального попередження, як впливає на правову культуру населення чи відновлює довіру до закону [7, с. 8–10]. У цьому контексті принципи справедливості та дієвості юридичної відповідальності виходять на перший план. Зокрема, справедливість вимагає пропорційності між тяжкістю правопорушення та мірою покарання, а дієвість – реального досягнення цілей, серед яких виправлення правопорушника, захист потерпілих, стримування майбутніх правопорушень тощо [56, с. 66–76]. Зазначене положення стало підґрунтям для подальших доктринальних досліджень, зосереджених на аналізі функцій відповідальності, критеріях її ефективності та ролі громадської думки у забезпеченні результативності застосовуваних санкцій.

Соціологічне трактування відповідальності зосереджується переважно на її легітимності й суспільному сприйнятті. Водночас для комплексного розуміння цього феномена необхідним є звернення і до етичного трактування. Саме етична традиція сформувала базові уявлення про відповідальність як моральну категорію, що пов’язана з оцінкою людських вчинків та внутрішньою здатністю особи діяти відповідно до належних критеріїв. Етика історично заклала основи уявлення про відповідальність через категорії добра і зла, свободи волі та обов’язку.

Філософи права розглядають юридичну відповідальність у тісному зв’язку з моральною відповідальністю, при цьому остання є поняттям

ширшим та базується на внутрішніх переконаннях, тоді як юридична відповідальність інституціоналізована в нормах і забезпечена зовнішнім примусом. Проте межа між моральним і правовим не завжди чітка. Новітні технологічні виклики, зокрема поведінка людини у кіберпросторі, породжують питання кіберетики, яка пропонує принципи відповідального користування цифровими технологіями, що не завжди підкріплені правовими санкціями [185, с. 110–115; 198, с. 45–49].

Слід наголосити, що приватність, достовірність інформації та недопустимість кібербулінгу підтримуються радше етичною відповідальністю онлайн-спільнот. Відповідно, правова доктрина стоїть перед завданням осмислити, як нормативно закріпити етичні засади відповідальності в інтернеті, щоб заповнити прогалини. У цьому контексті спостерігається поступова еволюція від повної свободи онлайн-висловлювань до встановлення юридичних меж, зокрема відповідальності за кіберзлочини, мову ворожнечі та порушення прав інших користувачів [50, с. 118–124].

Становлення інформаційного суспільства супроводжується масштабними трансформаціями у сфері базових соціальних інститутів, серед яких ключове місце належить інституту юридичної відповідальності. Глобальні зрушення, зумовлені швидким розвитком цифрових технологій, розширенням кіберпростору як принципово нового середовища соціальної взаємодії, зміною традиційних комунікаційних моделей під впливом медіареальності та загальною динамікою суспільних процесів спричиняють перегляд усталених парадигм у правових дослідженнях [91, с. 81–83].

Новітні виклики, що постають перед правовою системою, пов’язані з проблемами інформаційної безпеки, захисту цифрових прав людини, а також з ускладненням суспільних відносин у віртуальному просторі. У таких умовах актуалізується завдання формування нових науково-методологічних орієнтирів, здатних належним чином відобразити якісні зміни у природі та призначенні юридичної відповідальності в інформаційну добу.

У методологічному забезпеченні дослідження юридичної відповідальності в умовах інформаційного суспільства ключове значення мають такі вектори:

– діалектика – дозволяє виявити розвиток, суперечливість і взаємну зумовленість суспільних процесів, що безпосередньо впливають на зміст та функціонування юридичної відповідальності [3, с. 260; 30, с. 45–51].

– синергетика, котра розглядає правову систему як відкриту та нелінійну, у якій взаємодія порядку і хаосу зумовлює появу нових закономірностей правового регулювання в умовах цифровізації [4, с. 3–12; 52, с. 75–90];

– еволюційний аналіз, який забезпечує розуміння юридичної відповідальності як динамічної конструкції, що змінюється у процесі історичного розвитку та відповідає на нові суспільні виклики;

– системно-структурний аналіз, так як дозволяє розглядати юридичну відповідальність як багаторівневу систему, що адаптується до умов глобалізованого цифрового середовища [11, с. 68].

Передусім вищенаведене пов’язано з розширенням кола об’єктів правової охорони, до яких нині належать персональні дані, цифрова ідентичність, інформаційні ресурси та інші нематеріальні блага, що набувають зростаючої цінності у цифровому суспільстві. Водночас суттєво змінюється характер правопорушень, позаяк поряд із традиційними деліктами з’являються нові форми протиправної поведінки у віртуальному середовищі. Додаткову складність становить транснаціональний вимір таких діянь, адже їх вчинення та наслідки нерідко виходять за межі однієї національної юрисдикції, що ставить на порядок денний питання узгодженості заходів юридичної відповідальності у глобальному комунікаційному просторі та потребує формування нових доктринальних моделей, здатних враховувати поліцентричність сучасного правового середовища.

Поряд із цим варто зазначити, що процеси цифровізації зумовили виникнення якісно нових викликів для класичної доктрини юридичної відповідальності. Передусім ускладнюється ідентифікація суб'єкта правопорушення у віртуальному середовищі, визначення компетентної юрисдикції, належна фіксація факту правопорушення та забезпечення допустимості доказової бази. Відповідно, сучасна правова доктрина формує низку концептуальних підходів, спрямованих на адаптацію категорії відповідальності до умов цифрової доби:

1) активно розробляється концепція розподіленої відповідальності, яка передбачає можливість одночасного залучення до відповідальності кількох суб'єктів цифрового простору, зокрема власників платформ, розробників алгоритмів та кінцевих користувачів;

2) формується технологічна відповідальність, під якою розуміють юридичну відповідальність за створення, використання чи недосконаліть алгоритмів, систем штучного інтелекту та автоматизованих рішень, які здатні спричиняти юридично значущі наслідки;

3) розвивається концепція деанонімізованої відповідальності, спрямована на пошук кореляції між забезпеченням права особи на приватність у мережі та необхідністю притягнення її до відповідальності у разі вчинення шкідливої чи протиправної поведінки [89, с. 1829–1835].

Слід наголосити, що інтенсивне проникнення цифрових технологій у сферу публічного управління набуло статусу не тимчасового тренду, а визначального чинника зміцнення інституційної спроможності держави та її конкурентоспроможності на міжнародному рівні. Цифровізація управлінських процесів сприяє їх оптимізації, мінімізації бюрократичних процедур, забезпеченню прозорості та підзвітності органів влади, а також орієнтації на потреби громадян. Вказані зміни узгоджуються з сучасними стандартами демократичного врядування та формують основу для поєднання ефективності, відкритості й дотримання прав людини у практиці публічного адміністрування.

Зазначені процеси набувають особливої актуальності у світлі євроінтеграційного курсу України. Однією з ключових вимог, що висуваються до держав-кандидатів на вступ до Європейського Союзу, є приведення системи публічного управління у відповідність до цифрових стандартів ЄС. Йдеться, насамперед, про комплексну цифрову трансформацію адміністративних послуг, запровадження механізмів кіберзахисту, ефективне функціонування інститутів захисту персональних даних, а також інтенсивний розвиток електронного урядування як невід'ємного елементу концепції належного врядування. У цьому контексті цифровізація постає засобом технологічної модернізації управлінських процесів та стратегічним критерієм відповідності політичним, правовим і адміністративним стандартам європейського простору. Поряд із цим, вона трансформується у показник здатності держави забезпечувати верховенство права, прозорість влади та ефективність управління в руслі інтеграції до спільного правового простору ЄС [131].

Цифрові трансформації, що охоплюють як суспільні відносини загалом, так і сферу публічного управління, формують окрему термінологічну систему, яка вирізняється високим рівнем спеціалізації та динамізму. Понятійно-категоріальний апарат цифрового врядування має міждисциплінарний характер, оскільки поєднує технічну термінологію інформаційних технологій із правовими, організаційними та соціологічними категоріями, притаманними науці державного управління та юридичній доктрині. Вказана інтеграція зумовлена необхідністю адекватного відображення нових управлінських реалій, що виникають на стику інформаційно-технологічних інновацій та зростаючого суспільного запиту на ефективне, прозоре й інклюзивне врядування. Внаслідок цього формується унікальний мовний інструментарій, здатний описати феномени цифрової доби у категоріях, придатних як для наукового аналізу, так і для нормативно-правового закріплення, що в перспективі сприяє підвищенню якості правового регулювання та інституційної спроможності публічної влади.

Глобалізація сприяла уніфікації стандартів прав людини, формуванню транснаціонального права та розширенню меж публічно-правової юрисдикції держав, а також актуалізувала потребу у новому визначенні меж, форм і суб'єктного складу юридичної відповідальності. При цьому термінологічний апарат, що використовується для опису цифрових перетворень, залишається недостатньо впорядкованим у науковому та нормативно-правовому вимірі. Поняття «оцифрування», «цифровізація», «цифрова трансформація», «діджиталізація», «digital transformation» та інші вживаються досить часто як взаємозамінні [46, с. 142–144].

Відсутність належної термінологічної унормованості у сфері цифрових процесів становить серйозний виклик як для теорії, так і для практики права, позаяк:

1) ускладнює розроблення цілісної наукової концепції цифровізації правової системи, оскільки різночитання базових понять створюють методологічні розриви між окремими дослідницькими школами та напрямами;

2) семантична невизначеність провокує ризики правового релятивізму, коли одні й ті самі терміни у нормативно-правових актах або судовій практиці тлумачаться неоднаково;

3) відсутність стандартизованих дефініцій ускладнює законотворчий процес: законодавець, використовуючи неконкретизовані терміни, фактично залишає широке поле для суб'єктивного тлумачення, що суперечить принципу юридичної визначеності як засадничій складовій правової держави;

4) для правозастосовної практики це означає підвищену небезпеку колізій, правових прогалин та суперечливих судових рішень [42, с. 5–10].

Аналіз доктринальних джерел дає підстави стверджувати, що категорія «оцифрування» (digitization) здебільшого використовується для позначення процесу переведення аналогової інформації у цифрову форму та має переважно техніко-технологічний зміст [96, с. 67–73]. На відміну від

цього, поняття «цифровізація» (digitalization) охоплює соціально-організаційний процес впровадження цифрових технологій у різні сфери суспільного життя, зокрема у сферу публічного управління та правовідносин [203, с. 121–133]. Водночас термін «цифрова трансформація» (digital transformation) характеризує глибинні структурні зміни, які стосуються переосмислення парадигми функціонування інституцій, у тому числі пов'язаних з правотворчою та правозастосовною діяльністю, а також із переосмисленням доктрини юридичної відповідальності. Окремої уваги потребує тенденція некритичного запозичення англомовних термінів («digitalization», «digital transformation») без їх адаптації до українського правового контексту, що зумовлює семантичну невизначеність і ускладнює ефективність правового регулювання, формування судової практики та систематизацію наукового знання [152, с. 56–59; 154, с. 112–143].

Уніфікація та стандартизація термінології у сфері цифрових процесів має суттєве значення як для розвитку правової науки, так і для практики законотворення та правозастосування:

1) забезпечує методологічну цілісність наукових досліджень, створюючи умови для узгодженості концептуальних підходів у різних галузях права; вказане унеможливлює дублювання понять, знімає семантичні суперечності та сприяє формуванню єдиної доктрини цифрової трансформації права;

2) у практичному вимірі уніфікація термінів підвищує якість законодавчої техніки, адже чітко окреслені дефініції зменшують ризик правових колізій і підвищують передбачуваність норм;

3) сприяє єдності судової практики, оскільки стандартизований термінологічний апарат зменшує можливість неоднозначного тлумачення судами та адміністративними органами;

4) на міжнародному рівні уніфікація дозволяє гармонізувати національне законодавство з європейськими та глобальними правовими

стандартами, що є необхідною умовою інтеграції України у світовий правовий простір.

У сучасному правовому дискурсі доктринальна інтерпретація юридичної відповідальності відображає загальну тенденцію до гуманізації права, впровадження стандартів прав людини у всі сфери правозастосування, а також до пошуку дієвих механізмів реагування на новітні форми правопорушень, зумовлених глобальними трансформаціями [1; 23].

Варто зауважити, що глобалізація та цифрова модернізація суспільства виступають чинниками, що зумовлюють сутнісне переосмислення природи юридичної відповідальності. У сучасному правовому дискурсі простежується відхід від її традиційного трактування виключно крізь призму формально-юридичних ознак складу правопорушення. Натомість акцент поступово зміщується на оцінку суспільної результативності відповідальності, яка розглядається як інструмент відновлення порушених прав, превенції майбутніх правопорушень і підтримання довіри до державно-владних інститутів як системної цінності. У результаті відповідальність набуває ознак багаторівневої конструкції, у якій державні, міжнародні та недержавні інструменти взаємодіють, формуючи нову парадигму правового реагування в умовах глобалізованого та цифровізованого суспільства.

Модель багаторівневої юридичної відповідальності передбачає взаємодію кількох взаємопов’язаних рівнів, що відображають актуальні тенденції розвитку правового регулювання. На державному рівні зберігається класична архітектоніка юридичної відповідальності, яка реалізується через кримінально-правові, адміністративно-правові, цивільно-правові механізми тощо. На міжнародному рівні юридична відповідальність набуває форми юрисдикції міжнародних судових та квазісудових органів, а також виражається у виконанні державами зобов’язань за міжнародними договорами, що посилює інтеграцію національних систем у глобальний правовий простір. Водночас формується недержавний рівень відповідальності, який охоплює механізми саморегулювання, зокрема

цифрову етику, корпоративні кодекси поведінки, внутрішні регламенти цифрових платформ. Зазначений рівень відображає нові форми юридично значущого впливу, що виникають у межах цифрового середовища та доповнюють класичні державні та міжнародні інструменти.

Ключова характеристика цієї моделі полягає у відображенні новітніх тенденцій розвитку доктрини юридичної відповідальності, яка виходить за межі вузько нормативістського тлумачення та охоплює ціннісні орієнтири, пов’язані із гарантуванням прав людини та утвердженням принципу верховенства права. Фундаментальне значення моделі полягає у забезпеченні більшої ефективності реагування на нові форми правопорушень, урахуванні транснаціонального характеру цифрового середовища та створенні підґрунтя для гармонізації національного законодавства з міжнародними стандартами.

Аналіз багаторівневої моделі юридичної відповідальності свідчить про те, що сучасна правова система розвивається у напрямі поліцентричності, де взаємодіють державні, міжнародні та недержавні механізми правового впливу. Збереження ключової ролі держави у реалізації класичних форм відповідальності поєднується із посиленням значення міжнародних судових і квазісудових органів, юрисдикція яких формує нові стандарти правозастосування та сприяє уніфікації праворозуміння на глобальному рівні. Недержавний рівень, що проявляється у механізмах саморегулювання та корпоративної етики, фіксує новий етап еволюції правової реальності, у якій приватні суб’єкти здатні виконувати регулятивні функції, традиційно притаманні державі.

1.2. Правова природа кіберпростору та мережі Інтернет: концептуальні засади та категоріально-правовий аналіз

Правова природа мережі Інтернет не може бути досліджена ізольовано від кіберпростору, у межах якого вона функціонує та набуває своїх основних характеристик. Кіберпростір, на відміну від Інтернету як технологічної

інфраструктури, є більш комплексною категорією, що поєднує технічний, соціальний і правовий виміри. Саме тому аналіз правових засад кіберпростору та його співвідношення з Інтернетом має принципове значення для розкриття концептуальних і категоріально-правових характеристик досліджуваного феномену.

Упродовж останніх десятиліть поняття кіберпростору зазнало суттєвої еволюції, від вузько технічної категорії воно трансформувалося у багатовимірне соціально-правове явище, що охоплює комунікаційні процеси, обіг інформації, економічні операції та різноманітні форми соціальної взаємодії. Його швидкий розвиток, глобальний масштаб і нематеріальний характер спричинили істотні зміни у сфері міжнародного права та поставили перед світовим співтовариством комплекс нових викликів, пов'язаних із юрисдикційними межами, проблемами державного суверенітету, питаннями безпеки та забезпеченням прав людини у цифровому середовищі [149, с. 426–427].

Водночас, попри зростаюче значення кіберпростору для функціонування суспільства, міжнародне право досі не виробило ані уніфікованої дефініції цього феномену, ані загальновизнаного правового режиму його регулювання. Невирішеним залишається також питання визначення його правової природи: зокрема, чи слід вважати кіберпростір об'єктом міжнародного права, специфічною сферою людської діяльності або новим глобальним доменом, подібним до категорії «спільних надбань людства» [190, с. 107–117].

У широкому значенні кіберпростір трактується як віртуальне середовище, що формується завдяки поєднанню інформаційно-телекомунікаційних систем, мереж, даних та їх користувачів. Вказане визначення обґрунтовується тим, що кіберпростір не є виключно технічним феноменом, а відображає комплексну взаємодію технологічних, соціальних і правових чинників [206]. Його інфраструктурний вимір охоплює апаратні та програмні засоби, серверні комплекси, системи обробки даних, а також

протоколи комунікації, які забезпечують функціонування глобальної мережевої архітектури [175, с. 112]. Мережевий рівень кіберпростору утворюють взаємопов'язані сегменти, серед яких доцільно виокремити глобальні (Інтернет), корпоративні та спеціалізовані мережі, що надає кіберпростору транскордонного характеру та породжує складні юрисдикційні проблеми [191].

Особливе місце у структурі кіберпростору займають дані, які виступають водночас і його «матеріалом», і самостійним об'єктом правової охорони. Їх обробка, зберігання та передавання формують основу інформаційного обігу, створюють економічну вартість та визначають ризики для конфіденційності та безпеки [208]. Невід'ємним елементом кіберпростору є також його користувачі. До них належать фізичні та юридичні особи, державні органи, приватні компанії, платформи, а також автоматизовані системи, що виконують роль «агентів» цифрової взаємодії [219]. Саме їхня діяльність надає кіберпростору соціального змісту та актуалізує правове регулювання.

Віртуальність цього середовища полягає не у відсутності матеріального базису, а у специфіці соціальної взаємодії, що здійснюється через логічні адресні простори, протоколи та цифрові ідентичності, а не через фізичну територію. Зазначене пояснює наявність багатолокальності однієї дії та множинності можливих юрисдикцій [205].

Широке визначення кіберпростору дозволяє концептуально поєднати технічні, інформаційні та соціальні елементи цього феномену і забезпечує основу для вироблення адекватних моделей правового регулювання, юрисдикції та відповідальності [151, с. 985]. Відтак кіберпростір можна визначити як сукупність віртуально-мережевих зв'язків, що існують у межах цифрової реальності та на які поширюється правове регулювання з боку держави, міжнародних організацій і недержавних суб'єктів. Таке позиціювання має вирішальне значення для розуміння меж юрисдикції,

принципу суверенітету у цифровому вимірі та для правового оформлення юридичної відповідальності у разі правопорушень у кіберпросторі.

Категорія «кіберпростір» сформувалася наприкінці XX ст. на перетині технологічного прогресу та стрімкого культурно-мистецького розвитку. Етимологічно префікс «кібер» походить від грецького kybernetes, «керманич», «штурман», що згодом дало назву науці «кібернетика», орієнтованій на вивчення процесів управління. Одне з перших уживань терміна «кіберпростір» фіксується у спільному мистецькому проєкті «Atelier Cyberspace» данської художниці Сюзанни Уссінг та архітектора Карстена Хоффа наприкінці 1960- х рр., де він позначав серію інтерактивних інсталяцій, так званих «сенсорних просторів», які реагували на поведінку людини у фізичному середовищі. Широкого поширення поняття набуло в 1980-х рр. завдяки науковій фантастиці. У романі Вільяма Ґібсона «Neuromancer» (1984 р.) кіберпростір був представлений як глобальний цифровий світ, що виступає у формі графічного зображення масивів даних, вилучених із банків комп'ютерної пам'яті. Упродовж 1990-х рр. термін «кіберпростір» поступово закріпився у масовій свідомості як позначення глобальної мережі Інтернет та широкого кола цифрових комунікаційних середовищ, що забезпечують взаємодію людей, інформаційних систем і даних [79, с. 22–25].

Відтак у суспільній культурі 1980–1990-х рр. поняття кіберпростору набуло значення специфічного «віртуального світу», який сприймався як новий простір соціальної взаємодії. Його існування асоціювалося з розвитком онлайн-ігор, чатів, форумів та електронних систем обміну повідомленнями, що формували середовище комунікації, відмінне від фізичної реальності, але водночас наділене соціальним та економічним змістом. Таке розуміння поступово перейшло від культурологічного дискурсу до наукового аналізу та актуалізувало питання правового статусу кіберпростору [142].

З правової точки зору кіберпростір став розглядатися як новий об'єкт регуляції, у межах якого виникають відносини, що потребують юридичного

врегулювання, від забезпечення свободи слова та захисту приватності до визначення юридичної відповідальності за протиправні дії у віртуальному середовищі. Культурне уявлення про кіберпростір як «місце» взаємодії людей у мережі заклало передумови для формування концепції його правової природи. У подальшому зазначене відобразилося у дискусіях щодо юрисдикції в мережі Інтернет, проблеми «електронного громадянства», статусу цифрових ідентичностей та меж реалізації прав людини у віртуальному просторі. З огляду на викладене можна стверджувати, що початкове сприйняття кіберпростору в популярній культурі стало основою для вироблення доктринальних підходів до його правового аналізу [95, с. 283–291].

У рамках нашого дослідження варто звернути увагу на «Декларацію незалежності кіберпростору» Джона Перрі Барлоу 1996 року, котра вважається однією з найвідоміших концептуальних спроб визначити місце цифрового середовища у системі суспільних відносин. Документ репрезентує лібертраріанське бачення кіберпростору як автономного соціального простору, відокремленого від юрисдикції держави та організованого на засадах свободи, саморегулювання й формування глобальної цифрової спільноти. У декларації кіберпростір постає не стільки як технологічна інфраструктура, скільки як «дім Розуму», тобто простір мислення, комунікації та самовираження. Слід підкреслити, що Барлоу заперечує легітимність претензій держав на встановлення суверенітету в цифровому середовищі, аргументуючи це відсутністю фізичних кордонів і матеріальних об’єктів, до яких можуть застосовуватися традиційні засоби контролю та примусу. Натомість у тексті окреслюється перспектива становлення нової форми суспільного договору, що ґрунтується не на примусових механізмах державної влади, а на етичних нормах, раціональних інтересах та спільному благу [122].

Оприлюднення документа відбулося як реакція на ухвалення у США Закону про реформу телекомунікацій 1996 року, зокрема його розділу, що

встановлював обмеження щодо поширюваного в мережі контенту. Барлоу розглядав ці норми як прояв надмірного втручання держави у свободу самовираження, а саму «Декларацію» як протест проти спроб використання традиційних механізмів контролю для регулювання цифрового простору.

У науковій літературі цей документ нерідко оцінюється як утопічний чи надмірно ідеалістичний, особливо з огляду на подальший розвиток правового регулювання Інтернету, посилення ролі держав у сфері кібербезпеки та централізацію контролю над цифровими даними. Водночас у ретроспективному вимірі «Декларація» розглядається як знаковий етап становлення доктрини «кіберсвободи» та концепції цифрового громадянства, оскільки її положення стали ідейною основою для формування рухів на захист цифрових прав, права на приватність та принципу вільного Інтернету.

У філософсько-правовому вимірі «Декларація незалежності кіберпростору» Дж. П. Барлоу містить низку ключових положень:

а) кіберпростір визначається як автономна сфера реалізації прав і свобод, що не підлягає традиційним механізмам юрисдикції;

б) проголошується концепція «цифрового громадянства», у межах якого регулятивне значення мають етичні норми, культурні засади та колективна відповідальність учасників мережевої взаємодії;

в) відкидається застосування державного примусу у середовищі, яке позбавлене матеріальної основи для реалізації таких заходів;

г) висувається ідея «постнаціонального суверенітету», що ґрунтується не на територіальних критеріях, а на належності до цифрової спільноти.

Зі зростанням масштабів поширення мережі Інтернет стало очевидним, що кіберпростір справляє безпосередній вплив на суспільні відносини у фізичному світі, а відтак потребує аналізу і у правовому вимірі [79, с. 22–25]. Одним із ключових орієнтирів для доктринальних дискусій стала позиція Верховного суду США у справі «Reno v. American Civil Liberties Union». У зазначеному рішенні Інтернет охарактеризовано як простір, відомий користувачам як кіберпростір, що не має територіальної

прив’язки, але є доступним кожному незалежно від місця перебування [200]. Така характеристика закріпила уявлення про нетериторіальну природу цифрового середовища та актуалізувала питання меж застосування класичних категорій юрисдикції та суверенітету у сфері віртуальних комунікацій.

У міжнародно-правовому контексті дана позиція сприяла формуванню концепції кіберпростору як глобального середовища, яке не може бути цілковито підпорядковане виключній юрисдикції окремої держави, що стало підґрунтям для подальших дискусій щодо допустимих меж державного контролю над цифровими потоками даних та необхідності вироблення універсальних стандартів регулювання Інтернету.

Слід підкреслити, що у науковій доктрині вищезгадана справа розглядається як відправна точка для глобальної полеміки щодо співвідношення суверенітету держав і автономності кіберпростору. Її значення відображено і в пізніших міжнародних розробках, зокрема «Tallinn manual 2.0 on the international law applicable to cyber operations» (2017 р.) [205], де визнається, що принцип територіального суверенітету застосовується до кіберпростору, але з урахуванням його специфічної нематеріальної природи та транскордонного характеру.

Згідно з дослідженнями А.В. Чуба та В. О. Карпічкова, зарубіжна правова доктрина у сфері дослідження кіберпростору та юридичної відповідальності у мережі Інтернет характеризується глибшим теоретичним підґрунтям і тривалішою історією становлення. Водночас у закордонних джерелах простежується ширший доктринальний плюралізм щодо базових засад регулювання мережі Інтернет [101, с. 56].

На початку XXI століття термін «кіберпростір» почав використовуватися поза межами технічної чи фантастичної площини, а також поступово закріплювався у науковій літературі та міжнародних актах. У Рекомендації Генеральної конференції ЮНЕСКО від 15 жовтня 2003 року він визначався як віртуальний світ цифрової та електронної комунікації,

пов’язаної з глобальною інформаційною інфраструктурою [79, с. 22–25], що стало свідченням переходу від розуміння кіберпростору як технологічного явища до його осмислення як особливого виміру суспільного життя. Відповідні питання неодноразово піднімалися у документах ООН, зокрема у Резолюції Генеральної Асамблеї «Створення глобальної культури кібербезпеки» 2002 року [220] та у звітах Групи урядових експертів ООН з питань розвитку у сфері інформаційної безпеки (2013, 2015 рр.) [201; 202].

У червні 2021 року Велика Британія офіційно оприлюднила свою позицію щодо застосування міжнародного права до діяльності держав у кіберпросторі та зробила важливий внесок у формування глобального нормативного дискурсу в цій галузі. У заяві наголошено, що на кіберпростір повною мірою поширюються положення Статуту ООН, зокрема пункт 4 статті 2, що забороняє загрозу силою або її застосування проти територіальної цілісності чи політичної незалежності держав [74]. Зазначається, що кібероперації, наслідки яких тотожні збройному нападу або здатні завдати еквівалентної шкоди, можуть підпадати під поняття збройного нападу у розумінні міжнародного права, що, у свою чергу, активує право на індивідуальну або колективну самооборону відповідно до статті 51 Статуту ООН. Принципи суверенітету та невтручання залишаються повністю чинними у цифровому середовищі. Незаконним визнається будь-яке втручання з боку однієї держави в політичні, економічні чи інші внутрішні справи іншої держави, якщо таке втручання здійснюється за допомогою кіберзасобів без згоди відповідної держави.

У заяві також роз’яснюється, що держави несуть міжнародну відповідальність за кібероперації, які здійснюються їхніми органами або іншими суб’єктами, що діють за їхніми інструкціями, під їхнім керівництвом чи контролем. Водночас наголошується на важливості належної атрибуції кіберінцидентів, відповідно до якої встановлення джерела атаки повинно базуватися на фактичних доказах та міжнародно визнаних методах розслідування. Допускається можливість вжиття контрзаходів у відповідь на

міжнародно-протиправні дії в кіберпросторі, за умови дотримання принципів пропорційності, тимчасовості та спрямованості на припинення порушення і відновлення правопорядку. В умовах збройного конфлікту до кібероперацій повністю застосовуються норми міжнародного гуманітарного права, у тому числі принципи розрізнення, пропорційності та необхідності, з метою запобігання шкоді цивільному населенню. Права і свободи, гарантовані міжнародним правом прав людини, зокрема свобода вираження поглядів та право на приватність, повинні забезпечуватися і в цифровому середовищі. Обмеження таких прав допускаються лише у випадках, коли вони є законними, необхідними та пропорційними у демократичному суспільстві [142]. Право на доступ до Інтернету стає ключовим у сучасному інформаційному суспільстві. Багато країн закріплюють це право в конституціях і законах, забезпечуючи громадянам стабільний доступ до інформації, тоді як інші держави вводять обмеження з політичних або безпекових причин. Зарубіжний досвід, зокрема Бразилії, Фінляндії та Іспанії, демонструє прогресивні підходи до гарантування доступу, тоді як приклади Китаю та Індії вказують на ризики надмірного контролю. Таким чином, важливим є баланс між забезпеченням інформаційної безпеки та правом на доступ до інформації [99, с. 369]. Відтак кіберпростір не є винятком із-під дії права, а навпаки становить нову площину, у якій мають реалізовуватися засади верховенства права, поваги до суверенітету держави та основоположних прав людини.

Закономірно, що у зв’язку з бурхливим розвитком інформаційних технологій міжнародне співтовариство почало приділяти дедалі більше уваги правовим аспектам кіберпростору. Втім, на міжнародному рівні досі не існує уніфікованого, загальновизнаного визначення цього поняття [114].

Так, у документах ООН частіше вживаються терміни «інформаційний простір» або «ICT environment». Важливим кроком стало визнання, що діяльність у кіберпросторі підпадає під дію чинного міжнародного права. Зокрема, у Доповіді Групи урядових експертів ООН 2013 року було вперше

підтверджено, що на кіберпростір поширюється міжнародне право, зокрема Статут ООН [201]. Цю позицію згодом одноголосно підтримали держави в резолюції 2015 року [202].

Документом, який закріпив концепцію кіберпростору як глобального віртуального простору інформаційної взаємодії, є «Рекомендація щодо сприяння та використання багатомовності та універсального доступу до кіберпростору», ухвалена Генеральною конференцією ЮНЕСКО 15 жовтня 2003 року, де кіберпростір описано як віртуальний світ цифрової та електронної комунікації, пов'язаної з глобальною інформаційною інфраструктурою, що свідчить про його сприйняття як технологічного та соціально-культурного феномена [199].

У документах Європейського Союзу поняття кіберпростору інтерпретується у площині забезпечення прав і свобод у цифровому середовищі. У Стратегії кібербезпеки ЄС 2013 року «An open, safe and secure cyberspace» чітко зазначено, що одним із завдань кіберполітики ЄС є сприяння позиціонуванню кіберпростору як простору свободи та фундаментальних прав. Зокрема підкреслюється, що розширення глобальної підключеності не повинно супроводжуватися цензурою або масовим наглядом, а права людини мають бути захищені онлайн на тому ж рівні, що і в офлайн [144]. ЄС підтримує розробку добровільних норм поведінки та заходів довіри в кіберсфері замість запуску нових міжнародних угод, а також надає перевагу застосуванню існуючих зобов'язань у сфері прав людини та сприянню їхній реалізації в цифровому середовищі. За позиціюванням ЄС кіберпростір виступає як середовище, де мають діяти чинні міжнародно-правові норми, з акцентом на збереженні його відкритості, безпеки та повазі до прав людини [166].

НАТО розглядає кіберпростір насамперед крізь призму військово-стратегічного виміру. На Варшавському саміті 2016 року глави держав та урядів офіційно визнали його п'ятою сферою воєнних дій поряд із сушею, морем, повітрям і космосом. У підсумковому комюніке було наголошено, що

кіберпростір є сферою операцій, у якій Альянс повинен забезпечувати захист так само ефективно, як у традиційних доменах війни [189]. Зазначене рішення закріпило доктринальне бачення, відповідно до якого кібератаки можуть розглядатися як потенційні підстави для застосування механізмів колективної оборони, передбачених статтею 5 Вашингтонського договору [188].

Попри відсутність офіційного визначення поняття «кіберпростір» у правових актах НАТО, у внутрішніх стратегічних документах використовується тлумачення, близьке до американського, згідно з яким кіберпростір визначається як глобальний домен інформаційного середовища, що складається з взаємозалежних мереж інформаційних технологій та даних, та охоплює Інтернет, телекомунікаційні системи, комп'ютерні ресурси та вбудовані процесори [187]. Варто підкреслити, що з метою інституційного забезпечення кібероборони Альянс створив Кооперативний центр кібероборони, який здійснює дослідження, аналітику та навчання у стратегічному, операційному, технічному та правовому вимірах [204]. У такий спосіб НАТО визнає кіберпростір окремим доменом воєнних дій, а також розвиває спеціалізовану доктрину та інституційні механізми, що підтверджує належність кібербезпеки до загальної системи колективної оборони.

Відтак у чинних міжнародно-правових документах відсутнє уніфіковане нормативне визначення поняття «кіберпростір». Водночас у більшості актів простежується його трактування як глобального інформаційно-комунікаційного середовища, у межах якого підлягають застосуванню загальновизнані норми міжнародного права. При цьому акценти розставляються по-різному: у доктринальних матеріалах НАТО домінує безпековий вимір, тоді як у позиціюванні Європейського Союзу пріоритет надається захисту прав і свобод людини. Спільним знаменником зазначених підходів є визнання транснаціонального характеру кіберпростору та необхідності міжнародної координації його регулювання.

У сучасному науковому дискурсі кіберпростір розглядається як комплексний глобальний феномен соціально-технічного характеру, що поєднує матеріальну інфраструктуру (комунікаційні мережі, серверні потужності, апаратні пристрої) з потоками даних та системами комунікації між людьми. Його особливість полягає в одночасному існуванні у фізичному вимірі (кабельні мережі, дата-центри, обладнання) та у віртуальному середовищі (інформаційні ресурси, програмні платформи, цифровий контент). Така подвійна природа значно ускладнює вироблення однозначного визначення категорії «кіберпростір».

Попри це, у доктрині переважає розуміння кіберпростору як середовища діяльності, створеного внаслідок інтеграції комп'ютерних систем, яке охоплює всі форми цифрової взаємодії. Воно не має географічної локалізації, однак дії, що здійснюються у ньому, здатні породжувати матеріальні наслідки в реальному світі. З огляду на зазначене, у юридичних дослідженнях кіберпростір дедалі частіше трактується як об'єкт правового регулювання, що потребує адаптації класичних правових категорій до нових умов цифрової реальності [146].

Питання визначення правового статусу кіберпростору належить до найбільш дискусійних у теорії міжнародного права. Основна проблема полягає в тому, що кіберпростір за своєю природою не може бути повністю віднесений до жодної з традиційних категорій ані до «об'єкта» права, ані до «території» у класичному розумінні, ані до самостійної сфери, подібної до відкритого моря чи космічного простору. Його особливість полягає в нематеріальності та транснаціональному характері, які унеможливлюють застосування до нього усталених просторових концепцій міжнародного права.

Кіберпростір не має географічних кордонів, визначеної площі чи матеріального середовища, яке можна було б закріпити за конкретною державою на основі територіального суверенітету. Водночас його технічні складові розташовані на території держав і підпадають під дію їхньої

національної юрисдикції. Проте інформаційні потоки, що циркулюють у межах глобальної мережі, виходять за рамки національних кордонів і формують єдиний цифровий простір, який не може бути відмежований у класичному територіальному сенсі.

У наукових дебатах усе частіше відзначається, що кіберпростір не слід розглядати як «нову територію», придатну для розподілу чи привласнення державами за аналогією із суходолом, морем чи повітряним простором. Навіть держави, які послідовно відстоюють концепцію «кіберсуверенітету», зазвичай виходять з того, що суверенітет може застосовуватися лише щодо дій у кіберпросторі та контролю над матеріальними елементами його інфраструктури, але не означає юрисдикційного «привласнення» окремих сегментів самого цифрового простору. Вищезазначене вкотре підтверджує тенденцію до сприйняття кіберпростору як особливої глобальної сфери, що потребує вироблення спеціальних механізмів міжнародної координації та регулювання.

Проблемним у міжнародно-правовій доктрині є також питання, чи може кіберпростір розглядатися як об’єкт міжнародного права. У певному аспекті – так, оскільки він становить специфічне середовище людської діяльності, у межах якого виникають транскордонні відносини. Водночас класичні об’єкти міжнародно-правового режиму зазвичай характеризуються матеріальною відчутністю або ж формуються як нематеріальні категорії з чітко визначеним статусом «спільної спадщини людства». Кіберпростір же має іншу природу, позаяк складається з поєднання публічних і приватних компонентів; при цьому значна частина інфраструктури Інтернету належить приватним корпораціям або перебуває під контролем окремих держав, що унеможливлює його кваліфікацію як res communis omnium [141; 170].

У сучасному науковому дискурсі поширеною є концепція, відповідно до якої жодна держава не має права монополізувати або проголошувати своєю власністю окремі сегменти глобальної мережі. Вказане позиціювання виходить із необхідності розглядати кіберпростір як сферу колективного

користування, що потребує багаторівневого та кооперативного управління. Водночас існує й альтернативна позиція, прихильники якої наголошують, що визначення кіберпростору «глобальним надбанням» надмірно спрощує правову картину та нівелює роль держав. На відміну від космічного простору чи відкритого моря, значна частина мережевої інфраструктури перебуває у приватній власності та розташована в межах національних територій, що зумовлює здійснення державами юрисдикційних і суверенних повноважень щодо цих елементів. Відтак, повна аналогія з категорією res communis omnium є некоректною. У доктринальному сенсі кіберпростір дедалі частіше трактується як гібридне утворення, оскільки його технічна інфраструктура розподілена між численними національними юрисдикціями, тоді як інформаційні потоки, що функціонують поверх цієї інфраструктури, формують спільне транснаціональне комунікаційне середовище, яке не піддається повному суверенному контролю окремих держав [134; 163].

У міжнародно-правовій доктрині дедалі більшого поширення набуває підхід, згідно з яким кіберпростір слід розуміти не як статичну територію, а як специфічну сферу діяльності. Відповідно, основна увага зосереджується не на самому просторовому вимірі, а на сукупності процесів, що відбуваються в цифровому середовищі, зокрема комунікації, обміні даними, комерційних транзакціях, кібератаках тощо. У цьому контексті держави мають не лише право, а й обов’язок здійснювати свої кіберможливості відповідно до міжнародного права з дотриманням принципів суверенітету, невтручання, заборони застосування сили та поваги до прав людини. Відтак кіберпростір дедалі частіше ототожнюється з традиційними сферами діяльності, у межах яких діють загальновизнані міжнародно-правові норми [205].

Водночас слід підкреслити, що правовий статус кіберпростору ще не врегульовано спеціальним міжнародним договором чи єдиним кодифікованим актом. Наразі не існує «конституції» кіберпростору або узагальненого міжнародно-правового режиму, що регулював би цю сферу.

Водночас це не означає, що кіберпростір перебуває у стані правового вакууму: держави та міжнародні органи послідовно підтверджують застосовність до нього загальних норм міжнародного права, зокрема положень Статуту ООН, норм міжнародного гуманітарного права та міжнародних стандартів у сфері прав людини.

На наш погляд, кіберпростір доцільно визначати як глобальну сферу діяльності людства, що поступово набуває рис особливого міжнародно-правового режиму. Він не може бути віднесений ані до класичних категорій території, ані до виключно техногенних об'єктів, оскільки за своєю природою постає новим виміром міжнародних відносин. У межах цього виміру вже функціонують основоположні норми міжнародного права, серед яких загальні принципи, імперативні норми, а також окремі галузеві договори. Водночас ці норми потребують подальшого розвитку та конкретизації з урахуванням специфіки цифрового середовища й особливостей правової кваліфікації дій у ньому.

Міжнародне співтовариство рухається шляхом поступового формування стандартів і правил належної поведінки в кіберпросторі. Ймовірно, остаточне визначення його правового статусу передбачатиме синтез кількох концепцій, що полягатиме в поєднанні визнання кіберпростору як спільної сфери інтересів людства з одночасним збереженням за державами суверенних прав на власні інформаційні ресурси, а також юрисдикції щодо злочинної чи ворожої діяльності, яка походить з їхньої території або спрямована проти неї. За таких умов кіберпростір функціонуватиме як відкрите, стійке та мирне середовище, зорієнтоване на розвиток людства, а не перетворюватиметься на арену анархії чи вседозволеності.

На відміну від поняття кіберпростору, мережа Інтернет є насамперед матеріально й логічно організованою «мережею мереж», яка функціонує на основі пакетної комутації та протокольної сумісності. Правова природа Інтернету характеризується гібридністю; унаслідок цього Інтернет не може

бути редукований ані до «території» у класичному міжнародно-правовому сенсі, ані до «речі». Радше йдеться про функціональний режим взаємодії приватних і публічних суб'єктів у межах багаторівневої транскордонної інфраструктури [183, с. 231–248].

Важливою ознакою мережі Інтернет є її модель управління, оскільки вона історично формувалася за багатосторонньою логікою, у межах якої поряд із державами ключову роль відіграють технічні спільноти стандартотворення, інституції управління ідентифікаторами, оператори мереж, цифрові платформи та громадянське суспільство. Зазначена модель ґрунтується на поєднанні «твердого» права та механізмів «м'якого» регулювання (технічних стандартів, кодексів поведінки, політик застосування, угод між операторами та реєстрами), що формує специфічний регулятивний режим співуправління. Водночас Інтернет потребує комплексного й адаптивного правового регулювання, оскільки чинна законодавча база залишається фрагментарною та не охоплює всі аспекти інтернет-відносин. Водночас міжнародний досвід свідчить, що ефективне регулювання можливе шляхом інтеграції міжнародних стандартів, використання інструментів «м'якого права» та залучення різних зацікавлених сторін. Основною метою такого регулювання є захист прав і свобод користувачів, забезпечення безпеки, конфіденційності та стабільного функціонування Інтернету [100, с. 96–102]. З погляду правового аналізу це зумовлює розщеплення центрів нормотворення, розмитість юрисдикційних меж і необхідність узгодження технічних стандартів із вимогами верховенства права та стандартами прав людини.

Співвідношення правового статусу кіберпростору та мережі Інтернет можна розглядати як у площині їхніх точок перетину, так і відмінностей. Спільним для обох категорій є те, що вони безпосередньо пов'язані з гарантуванням прав і свобод людини, захистом суверенітету держав та забезпеченням кібербезпеки. У правовому сенсі як кіберпростір, так і Інтернет виступають платформою реалізації загальновизнаних міжнародних

стандартів, насамперед принципу поваги до прав людини. Інтернет є середовищем здійснення свободи вираження поглядів, доступу до інформації та права на приватність. У контексті кіберпростору зазначені права набувають додаткових вимірів, пов'язаних із безпечністю цифрового середовища [153, с. 1082–1083].

У мережі Інтернет питання суверенітету проявляється, передусім, через здійснення державами контролю над фізичною інфраструктурою, розташованою на їхній території, зокрема над дата-центрами, телекомунікаційними вузлами та провайдерами. Для кіберпростору суверенітет має значно ширший зміст, оскільки охоплює також юрисдикцію держав щодо дій, що спричиняють наслідки для їхньої території або громадян, навіть якщо ці дії походять із-за кордону. Саме тому в актах ООН і доктринальних документах закріплено положення про поширення принципу суверенітету на сферу кібероперацій, хоча його практична реалізація ускладнюється транснаціональною природою цифрових процесів [129, с. 24].

У площині безпеки обидва явища виступають як об'єкти захисту від кіберзагроз. В аспекті мережі Інтернет це передусім забезпечення безперебійного функціонування технічних систем та запобігання атакам на інфраструктуру. У контексті кіберпростору проблема безпеки набуває ширшого значення й охоплює захист інформаційних систем органів влади, критичної інфраструктури, виборчих процесів та інших сфер, що виходять далеко за межі суто технічного виміру. Як зазначалося раніше, визнання НАТО у 2016 році кіберпростору п'ятою сферою воєнних дій підтверджує його стратегічну вагу в глобальній системі безпеки.

Водночас існують суттєві відмінності у правовому статусі кіберпростору та Інтернету. Кіберпростір, як зазначалося вище, у сучасній доктрині розглядається передусім як сфера діяльності, у межах якої діють загальні принципи міжнародного права. Його правовий статус формується поступово через практику правозастосування держав і міжнародних органів і наразі не закріплений у окремому кодифікованому акті. Натомість Інтернет є

матеріально та логічно структурованою інфраструктурою з багаторівневою архітектурою, регулювання якої здійснюється через поєднання національного законодавства, міжнародних угод та технічних стандартів.

У сфері управління також простежуються відмінності: для кіберпростору визначальною є роль держав і міжнародних організацій, тоді як для Інтернету характерною є багатостороння модель, у якій вагому частку відповідальності несуть технічні спільноти, приватні компанії та громадянське суспільство. З огляду на це можна дійти висновку, що кіберпростір та мережа Інтернет співвідносяться як широка правова категорія та її інфраструктурна основа. Їх поєднують спільні цінності, проте вони відрізняються предметом регулювання, рівнем інституціоналізації та специфікою суб'єктного складу управління.

Правова природа мережі Інтернет вирізняється складністю та багаторівневим характером, що зумовлено його технічною архітектурою та соціальною функціональністю. Інтернет постає як технічна інфраструктура глобального зв'язку та соціально-правовий простір, у якому здійснюються комунікаційні, економічні, політичні та культурні процеси, що набувають юридично значущих наслідків.

З позицій загальної теорії права Інтернет не можна кваліфікувати як територію або матеріальний об'єкт, подібний до природних ресурсів чи класичних об'єктів міжнародного права. Його правова природа визначається функціонуванням багаторівневої мережевої системи, яка включає фізичний рівень (кабельні мережі, дата-центри, сервери), логічний рівень (протоколи, адресація, доменні імена) та рівень контенту і застосунків. Кожен із цих рівнів підпадає під правове регулювання – національне, міжнародне або договірно-приватне, що обумовлює гібридний характер правової природи Інтернету. [150, с. 78–94].

Інтернет характеризується поєднанням публічно-правових і приватно-правових начал. Публічний вимір Інтернету проявляється у закріпленні принципів свободи вираження поглядів, права на доступ до інформації,

захисту персональних даних та кібербезпеки, що визнаються міжнародними стандартами прав людини, зокрема Міжнародним пактом про громадянські та політичні права та практикою Європейського суду з прав людини. Приватний вимір проявляється у ключовій ролі саморегуляторних і технічних спільнот, які встановлюють стандарти функціонування мережі та координують управління ресурсами.

З точки зору міжнародного права Інтернет є сферою транскордонної взаємодії, на яку поширюються загальні принципи суверенітету, невтручання, заборони застосування сили та дотримання прав людини. При цьому держави здійснюють юрисдикцію щодо фізичних елементів інфраструктури, розташованих на їхній території, однак транскордонність інформаційних потоків і єдність протокольної системи зумовлюють необхідність міжнародної координації [159, с. 7–25]. У цьому сенсі правова природа Інтернету має дворівневий характер, позаяк він є одночасно критичною інфраструктурою, інформаційним середовищем і простором реалізації прав людини, що формує особливий, змішаний режим правового регулювання.

Правова природа мережі Інтернет безпосередньо зумовлює специфіку юридичної відповідальності у цифровому середовищі. Інтернет виступає інфраструктурною основою кіберпростору, а також простором, де реалізуються юридично значущі дії, від комунікацій і обміну інформацією до укладення електронних правочинів, обробки персональних даних тощо. Саме тому мережа Інтернет перетворюється на ключове середовище, в якому набувають практичного виміру класичні правові інститути відповідальності. Саме це зумовлює потребу в адаптації традиційних механізмів юридичної відповідальності до специфіки цифрового середовища [173, с. 103–110; 179, с. 151–161].

Характерною рисою галузей права нового покоління є також органічне поєднання публічно-правових і приватно-правових інтересів. У юридичній доктрині обґрунтовується позиція, згідно якої ключове

призначення таких галузей полягає у забезпеченні реалізації нових функцій держави або в трансформації та адаптації вже існуючих до умов цифрової реальності [39, с. 77–81].

Особливістю правової відповідальності в Інтернеті є транснаціональний характер відносин. Протиправна дія може бути вчинена на території однієї держави, мати наслідки в іншій і водночас зачіпати права осіб у кількох юрисдикціях, що ускладнює визначення належного суб'єкта відповідальності та меж юрисдикції, водночас підкреслюючи значення міжнародно-правових норм і міждержавної співпраці. Саме тому у сфері Інтернету дедалі більшої актуальності набувають концепції колективної, розподіленої та технологічної відповідальності, які виходять за межі класичного розуміння правової відповідальності [135, с. 31–43].

Відтак аналіз правової природи кіберпростору та мережі Інтернет свідчить про їх багатовимірність і взаємозалежність. Кіберпростір слід розглядати як глобальне соціально-технічне середовище, що поєднує інформаційні потоки та комунікаційні системи; він не має фізичних меж, проте генерує реальні правові наслідки. У системі кіберпростору Інтернет виконує роль матеріальної та організаційної інфраструктури, яка забезпечує функціонування кіберпростору, водночас формуючи власний специфічний правовий режим. Його регулятивна природа визначається поєднанням норм національного законодавства, норм міжнародного права та актів саморегуляторних спільнот.

З позицій інституту юридичної відповідальності ці феномени виступають просторами, у яких класичні доктринальні категорії набувають нового змістового навантаження. Транскордонний характер мережевих комунікацій ускладнює ідентифікацію правопорушника та визначення юрисдикції, що зумовлює необхідність розробки міжнародних стандартів поведінки у цифровому середовищі та активної участі держав в інституційних ініціативах. У цьому контексті саме через призму юридичної відповідальності стає можливим забезпечити належну кореляцію між

захистом прав і свобод людини, суверенітетом держав та потребою у глобальній стабільності й безпеці кіберпростору та мережі Інтернет.

Висновки до розділу 1

У ході проведеного дослідження теоретико-правових основ юридичної відповідальності у цифрову епоху дисертант дійшов низки узагальнень та висновків, що стосуються еволюції доктринальних підходів інституту відповідальності, а також правової природи кіберпростору та мережі Інтернет як нових середовищ її реалізації:

– встановлено, інститут юридичної відповідальності не можна зводити виключно до примусу чи санкції. У правовій доктрині підкреслюється, що державно-правовий примус є поняттям ширшим, ніж власне юридична відповідальність, позаяк не всякий примусовий захід у праві передбачає притягнення до відповідальності. Держава застосовує й інші заходи впливу, зокрема, попереджувальні, відновлювальні тощо, які виходять за межі відповідальності. На відміну від таких заходів, юридична відповідальність завжди передбачає елемент осуду винного та покарання, а її реалізація відбувається у визначеній процесуальній формі з додержанням встановлених процедур;

– наголошено, інститут юридичної відповідальності має міждисциплінарну природу, оскільки його зміст формується на перетині права, психології, соціології та етики. Психологічний вимір визначає внутрішнє ставлення особи до власних вчинків, що у правовій площині трансформується у поняття вини як ключової передумови притягнення до відповідальності. Соціологічний вектор має спрямування на легітимності та соціальній функціональності відповідальності. Етичний компонент закладає фундаментальні уявлення про добро, зло, свободу волі та обов’язок, які віддзеркалюються у сучасному правовому регулюванні в умовах цифрових трансформацій, де виникає потреба у формуванні принципів кіберетики;

– акцентовано, цифровізаційні процеси зумовили виникнення якісно нових викликів для класичної доктрини юридичної відповідальності. Передусім ускладнюється ідентифікація суб'єкта правопорушення у віртуальному середовищі, визначення компетентної юрисдикції, належна фіксація факту правопорушення та забезпечення допустимості доказової бази. У зв'язку з цим сучасна правова доктрина формує низку концептуальних підходів, спрямованих на адаптацію категорії відповідальності до умов цифрової доби: 1) активно розробляється концепція розподіленої відповідальності, яка передбачає можливість одночасного залучення до відповідальності кількох суб'єктів цифрового простору, зокрема власників платформ, розробників алгоритмів та кінцевих користувачів; 2) формується технологічна відповідальність, під якою розуміють юридичну відповідальність за створення, використання чи недосконаліть алгоритмів, систем штучного інтелекту та автоматизованих рішень, які здатні спричиняти юридично значущі наслідки; 3) розвивається концепція деанонімізованої відповідальності, спрямована на пошук кореляції між забезпеченням права особи на приватність у мережі та необхідністю притягнення її до відповідальності у разі вчинення шкідливої чи протиправної поведінки;

– визначено, уніфікація та стандартизація термінології у сфері цифрових процесів має суттєве значення як для розвитку правової науки, так і для практики законотворення та правозастосування: 1) забезпечує методологічну цілісність наукових досліджень, створюючи умови для узгодженості концептуальних підходів у різних галузях права; вказане унеможливлює дублювання понять, знімає семантичні суперечності та сприяє формуванню єдиної доктрини цифрової трансформації права; 2) у практичному вимірі уніфікація термінів підвищує якість законодавчої техніки, адже чітко окреслені дефініції зменшують ризик правових колізій і підвищують передбачуваність норм; 3) сприяє єдності судової практики, оскільки стандартизований термінологічний апарат зменшує можливість

неоднозначного тлумачення судами та адміністративними органами; 4) на міжнародному рівні уніфікація дозволяє гармонізувати національне законодавство з європейськими та глобальними правовими стандартами, що є необхідною умовою інтеграції України у світовий правовий простір;

– констатовано, глобалізація та цифрова модернізація суспільства виступають чинниками, що зумовлюють сутнісне переосмислення природи юридичної відповідальності. У сьогоденному правовому дискурсі простежується відхід від її традиційного трактування виключно крізь призму формально-юридичних ознак складу правопорушення. Натомість акцент поступово зміщується на оцінку суспільної результативності відповідальності, яка розглядається як інструмент відновлення порушених прав, превенції майбутніх правопорушень і підтримання довіри до державно-владних інститутів як системної цінності. У результаті відповідальність набуває ознак багаторівневої конструкції, в якій державні, міжнародні та недержавні інструменти взаємодіють і формують нову парадигму правового реагування в умовах глобалізованого та цифровізованого суспільства;

– репрезентовано, модель багаторівневої юридичної відповідальності передбачає взаємодію кількох взаємопов’язаних рівнів, що відображають сучасні тенденції розвитку правового регулювання. На державному рівні зберігається класична архітектоніка юридичної відповідальності, яка реалізується через кримінально-правові, адміністративно-правові, цивільно-правові механізми тощо. На міжнародному рівні юридична відповідальність набуває форми юрисдикції міжнародних судових та квазісудових органів, а також виражається у виконанні державами зобов’язань за міжнародними договорами, що посилює інтеграцію національних систем у глобальний правовий простір. Водночас формується недержавний рівень відповідальності, який охоплює механізми саморегулювання, зокрема цифрову етику, корпоративні кодекси поведінки, внутрішні регламенти цифрових платформ. Зазначений рівень відображає нові форми юридично

значущого впливу, що виникають у межах цифрового середовища та доповнюють класичні державні й міжнародні інструменти;

– встановлено, аналіз генези та концептуального розвитку категорії «кіберпростір» дає підстави стверджувати, що вона пройшла шлях від культурологічного і технічного терміна до комплексного соціально-правового феномена, який дедалі частіше виступає предметом доктринального і нормативного осмислення. Кіберпростір характеризується дуалістичною природою, позаяк поєднує матеріальну інфраструктуру з нематеріальними інформаційними потоками та соціальною взаємодією користувачів, що ускладнює його правове визначення, але водночас виводить у площину міжнародного та національного регулювання.

Наголошується, що відсутність уніфікованої дефініції цього явища в міжнародному праві, а також дискусійність його правового статусу – зокрема питання, чи слід розглядати кіберпростір як об’єкт права, сферу діяльності чи глобальний домен – підкреслюють актуальність формування системних підходів до його юридичної кваліфікації. Попри це, сучасна наука дедалі більше схиляється до розуміння кіберпростору як середовища суспільних відносин, на які поширюються загальні принципи і норми міжнародного права, що створює основу для розробки спеціальних механізмів юрисдикції, притягнення до юридичної відповідальності та захисту прав людини у цифровій реальності.

Таким чином, правова природа кіберпростору визначається його інтегративним характером і зумовлює переосмислення класичних категорій міжнародного права – території, суверенітету та юрисдикції – з урахуванням специфіки віртуального середовища, яке не має географічних меж, проте породжує реальні правові наслідки; системний аналіз міжнародно-правових актів і стратегічних документів провідних міжнародних організацій свідчить про відсутність уніфікованого нормативного визначення поняття «кіберпростір». Водночас у більшості актів простежується його трактування як глобального інформаційно-комунікаційного середовища, у межах якого

підлягають застосуванню загальновизнані норми міжнародного права. При цьому акценти розставляються по-різному: у доктринальних матеріалах НАТО домінує безпековий вимір, у позиціюванні Європейського Союзу пріоритет надається захисту прав і свобод людини. Спільним знаменником вказаних трактувань є визнання транснаціонального характеру кіберпростору та необхідності міжнародної координації у його регулюванні.

Підкреслено, правовий статус кіберпростору ще не врегульовано спеціальним міжнародним договором чи єдиним кодифікованим актом. Наразі не існує «конституції» кіберпростору чи узагальненого міжнародно-правового режиму. Однак це не означає, що кіберсфера є правовим вакуумом, держави та міжнародні органи послідовно підтверджують застосовність до неї загальних норм міжнародного права, зокрема Статуту ООН, норм гуманітарного права та міжнародних стандартів у сфері прав людини.

Визначено, кіберпростір доцільно визначати як глобальну сферу діяльності людства, що поступово набуває рис особливого міжнародно-правового режиму. Він не може бути віднесений ані до класичних категорій території, ані до виключно техногенних об’єктів, оскільки за своєю природою постає новим виміром міжнародних відносин. У межах цього виміру вже функціонують основоположні норми міжнародного права, серед яких загальні принципи, імперативні норми, а також окремі галузеві договори. Водночас ці норми потребують подальшого розвитку та конкретизації з урахуванням специфіки цифрового середовища та особливостей правової кваліфікації дій у ньому;

– артикульовано, міжнародне співтовариство послідовно рухається шляхом поступового формування стандартів і правил належної поведінки в кіберпросторі. Ймовірно, остаточне визначення його правового статусу передбачатиме синтез кількох концепцій шляхом поєднання визнання кіберпростору як спільної сфери інтересів людства з одночасним збереженням за державами суверенних прав на їхні інформаційні ресурси, а

також юрисдикції щодо злочинної чи ворожої діяльності, яка походить із їхньої території або спрямована проти неї. За таких умов кіберпростір функціонуватиме як відкрите, стійке та мирне середовище, орієнтоване на розвиток людства, а не перетворюватиметься на арену анархії чи вседозволеності;

– акцентовано, що важливою ознакою мережі Інтернет є її модель управління, оскільки вона історично розвивалася за багатосторонньою логікою, у межах якої поряд із державами ключову роль відіграють технічні спільноти стандартотворення, інституції управління ідентифікаторами, оператори мереж, цифрові платформи та громадянське суспільство. Зазначена модель ґрунтується на поєднанні «твердого» права та «м'якого» регулювання (технічні стандарти, кодекси поведінки, політики застосунків, угоди між операторами та реєстрами), що формує специфічний регулятивний режим співуправління. З погляду правового аналізу це передбачає розщеплення центрів нормотворення, розмитість юрисдикційних меж і необхідність узгодження технічних стандартів із вимогами верховенства права та прав людини;

– окреслено суттєві відмінності у правовому статусі кіберпростору та Інтернету. Кіберпростір у сучасній доктрині розглядається передусім як сфера діяльності, у якій діють загальні принципи міжнародного права. Його правовий статус формується поступово, через правозастосування держав та міжнародних органів, і поки що не має окремого кодифікованого акта. Інтернет натомість є матеріально та логічно структурованою інфраструктурою, яка має багаторівневу архітектуру і регулюється поєднанням національного законодавства, міжнародних угод та технічних стандартів. У сфері управління також існує відмінність, позаяк для кіберпростору визначальною є роль держав і міжнародних організацій, тоді як для Інтернету характерною є багатостороння модель, де вагому частку відповідальності несуть технічні спільноти, приватні компанії та громадянське суспільство.

Доведено, кіберпростір та мережа Інтернет співвідносяться як широка правова категорія та її інфраструктурна основа. Їх поєднують спільні цінності, але відрізняє предмет регулювання, рівень інституціоналізації та специфіка суб'єктного складу управління. Кіберпростір слід розглядати як глобальне соціально-технічне середовище, що поєднує інформаційні потоки та комунікаційні системи, не має фізичних меж, однак генерує реальні правові наслідки. Інтернет у системі кіберпростору виконує роль матеріальної та організаційної інфраструктури, яка забезпечує функціонування кіберпростору, проте водночас формує власний специфічний правовий режим. Його регулятивна природа визначається поєднанням норм національного законодавства, міжнародного права та актів саморегуляторних спільнот.

Встановлено, що з позицій інституту юридичної відповідальності ці феномени виступають просторами, у яких класичні доктринальні категорії набувають нового змістового навантаження. Транскордонний характер мережевих комунікацій ускладнює ідентифікацію правопорушника та визначення компетентної юрисдикції, що зумовлює необхідність розробки міжнародних стандартів поведінки у цифровому середовищі та активної участі держав в інституційних ініціативах. У цьому контексті саме через призму юридичної відповідальності стає можливим забезпечити належну кореляцію між захистом прав і свобод людини, суверенітетом держав та потребою у глобальній стабільності й безпеці кіберпростору і мережі Інтернет.

РОЗДІЛ 2
ПРАВОПОРУШЕННЯ В МЕРЕЖІ ІНТЕРНЕТ ЯК ОБ'ЄКТ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ

2.1. Міжнародні стандарти у сфері юридичної відповідальності за правопорушення у мережі Інтернет

Сучасна трансформація глобального інформаційного простору та поширення мережі Інтернет зумовили формування міжнародних стандартів у сфері юридичної відповідальності за правопорушення у цифровому середовищі. Інтернет як глобальна мережа комунікацій та економічної взаємодії не обмежується національними кордонами, а тому його правове регулювання потребує міжнародної координації.

У відповідь на глобальний масштаб цифрових комунікацій держави виробили низку міжнародних стандартів різної юридичної природи як обов'язкових міжнародних договорів, так і актів «м'якого права» (soft law). Їх положення спрямовані на уніфікацію підходів до криміналізації протиправних діянь у кіберпросторі, удосконалення превентивних заходів і механізмів переслідування правопорушників, а також на забезпечення належного захисту прав і свобод людини в умовах цифрового середовища. Завдяки таким стандартам забезпечується гармонізація національних законодавств, спрощується процедура міжнародного співробітництва та створюється правова основа для ефективного притягнення винних осіб до відповідальності. Водночас міжнародні акти у сфері боротьби з кіберзлочинністю є неоднорідними як за юридичною силою, так і за змістовним наповненням, що актуалізує потребу у їх систематизації та критичному переосмисленні з метою підвищення ефективності правозастосування.

Ще на початку 1990-х років міжнародне співтовариство усвідомило необхідність систематизації нових форм протиправної діяльності у сфері

використання інформаційних технологій. У 1991 році була запропонована перша спроба класифікації кіберзлочинів, які отримали умовні позначення у вигляді спеціальних абревіатур, що мало на меті виробити уніфіковану термінологію для наукових і практичних досліджень, а також забезпечити можливість порівняльного аналізу проявів протиправної поведінки у різних державах. У межах цієї класифікації було виділено такі основні групи: QA – несанкціонований доступ до інформаційних систем; QDT – використання програмного забезпечення типу «троянський кінь»; QAT – так звана «крадіжка часу», пов'язана з неправомірним використанням обчислювальних ресурсів; QDV – поширення комп'ютерних вірусів; QD – незаконна модифікація чи знищення комп'ютерних даних; QFC – шахрайські дії з банкоматами; QF – комп'ютерне шахрайство в ширшому розумінні; QZ – інші форми комп'ютерних злочинів; QR – незаконне копіювання програмного забезпечення та інформації; QFT – телефонне шахрайство; QS – комп'ютерний саботаж; QFF – виготовлення або використання комп'ютерних підробок [24].

Розпочати аналіз міжнародних стандартів у досліджуваній сфері ми вбачаємо за доцільне із розгляду окремих регіональних та міждержавних правових інструментів. Зазначена категорія охоплює договори та акти, прийняті в рамках регіональних організацій або міждержавних об'єднань, які встановлюють спільні стандарти відповідальності за кіберзлочини та інші правопорушення в Інтернеті. Найбільш впливовими є наступні європейські стандарти: Конвенція Ради Європи №108 1981 р. про захист персональних даних та Протокол 2018 р., Загальний регламент ЄС про захист даних (Регламент ЄС 2016/679), Конвенція Ради Європи про кіберзлочинність 2001 р. (Будапештська конвенція) та її Додатковий протокол 2003 р., Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства 2007 р. (Лансаротська конвенція), правові акти Європейського Союзу (директиви та регламенти щодо кібербезпеки, боротьби з незаконним контентом, захисту даних тощо) та ін.

Конвенція Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних», відкрита для підписання 28 січня 1981 року у Страсбурзі, стала першим міжнародно-правовим актом, що заклав основи комплексного регулювання сфери захисту персональних даних. Її значення полягає у створенні правової рамки, яка зобов'язує держави-учасниці забезпечувати кореляцію між технічним прогресом у сфері автоматизованої обробки інформації та гарантіями основоположних прав людини, насамперед права на приватність. Конвенція визначала ключові принципи обробки даних, серед яких, зокрема, законність і справедливість збору та використання, пропорційність, цільове призначення, достовірність та обмеженість у часі, а також обов'язок держав встановити належні гарантії захисту даних від несанкціонованого доступу чи зловживань. Особливу увагу приділено транскордонному обігу даних. Так, документ передбачав, що передача персональних даних за кордон може здійснюватися лише за умови забезпечення належного рівня їхнього захисту в державі призначення, що стало прототипом сучасних концепцій «адекватного рівня захисту» у європейському праві [35].

У 2018 році був ухвалений Протокол про модернізацію Конвенції 108, відомий також як «Конвенція 108+». Його метою стало оновлення положень Конвенції з урахуванням технологічних і соціальних змін, зокрема розвитку великих масивів даних, штучного інтелекту, глобальних комунікаційних платформ [98]. Протокол передбачив посилення прав суб'єктів даних, зокрема право на прозорість обробки, право знати логіку автоматизованого прийняття рішень, право на заперечення проти обробки та право на перенесення даних. Водночас були розширені обов'язки контролерів даних, у тому числі щодо впровадження процедур «privacy by design» і «privacy by default». Суттєво посилено вимоги до незалежних наглядових органів, яким надано право контролювати діяльність розпорядників даних, застосовувати санкції та співпрацювати між собою на міжнародному рівні [197].

Варто зауважити, що Конвенція 108 і Протокол 2018 року започаткували європейську традицію правового регулювання персональних даних, яка пізніше лягла в основу Загального регламенту ЄС про захист даних (GDPR). Конвенція, на відміну від регламентів ЄС, має відкритий характер і доступна для приєднання держав поза межами Європи, завдяки чому стала глобальним стандартом у сфері захисту приватності. Її модернізована редакція 2018 року закріпила концепцію, котра дозволяє поєднувати технологічні інновації з належними гарантіями прав людини, а відтак сприяє формуванню інституту «цифрової приватності».

Загальний регламент ЄС про захист даних (Регламент ЄС 2016/679) був ухвалений 27 квітня 2016 року та набрав чинності 25 травня 2018 року. Він замінив Директиву 95/46/ЕС і став правовим актом, що забезпечує уніфіковані стандарти захисту персональних даних у межах усього Європейського Союзу. Регламент має пряму дію щодо держав-членів і поширюється на будь-яких суб'єктів за межами ЄС, якщо вони здійснюють обробку даних резидентів Союзу, що передбачає закріплення принципу екстратериторіальності. Його поява була зумовлена необхідністю відповісти на виклики цифрової доби, що пов'язані з масовим збором, автоматизованою обробкою та глобальною передачею персональних даних.

Основу регламенту становить система принципів, які визначають рамки правомірної обробки даних. До них належать законність, справедливість і прозорість, обмеженість мети, мінімізація обсягу даних, точність і актуальність, обмеженість строків зберігання, а також обов'язок забезпечення цілісності та конфіденційності. Визначальним нововведенням стало закріплення принципу підзвітності, за яким контролер має дотримуватися правил та бути спроможним довести їх виконання.

Регламент ЄС 2016/679 істотно розширив права суб'єктів персональних даних, позаяк вони отримали право доступу до інформації про власні дані, право на виправлення та видалення («право бути забутим»), право на обмеження обробки, право на перенесення даних у структурованій

формі, право на заперечення проти обробки, а також право не підлягати рішенню, ухваленому виключно на основі автоматизованої обробки. Зазначені положення посилюють автономію особи у цифровому середовищі та формують основу для концепції «цифрового громадянства».

Досліджуваний документ одночасно покладає жорсткі обов'язки на контролерів і процесорів, котрі згідно його положень зобов'язані проводити оцінку впливу на захист даних у випадках високих ризиків, призначати уповноваженого із захисту даних у певних сферах діяльності, а також повідомляти наглядові органи про порушення безпеки. Особлива увага приділена забезпеченню прозорості алгоритмічних процесів та встановленню контролю за автоматизованими рішеннями.

Важливою особливістю Регламенту ЄС 2016/679 є встановлення санкційних механізмів, які мають реальну стримувальну силу. За порушення його положень передбачено штрафи до двадцяти мільйонів євро або до чотирьох відсотків світового річного обороту компанії, що забезпечує практичну ефективність регулювання. Функціонування регламенту забезпечується системою незалежних наглядових органів у кожній державі-члені, які мають широкі повноваження щодо перевірки, розслідування та накладення санкцій. Для забезпечення єдності правозастосування створено Європейську раду із захисту даних, яка видає керівні роз'яснення та координує діяльність національних органів [65].

Загальний регламент ЄС про захист даних утвердив нову концепцію правового регулювання персональних даних, перетворив захист приватності на один із фундаментальних елементів цифрового врядування Європейського Союзу та закріпив положення, відповідно до яких приватність позиціонується одночасно як індивідуальне право та суспільна цінність. Його вплив поширився далеко за межі ЄС, адже багато держав світу адаптували своє законодавство відповідно до його стандартів з метою забезпечення адекватного рівня захисту та входження у глобальний інформаційний простір.

Попри всеохопний характер Регламенту ЄС 2016/679 у сфері регулювання обробки персональних даних та гарантування цифрової приватності, його дія обмежується переважно адміністративно-правовими та цивільно-правовими механізмами. Разом із тим розвиток інформаційного суспільства зумовив потребу у створенні міжнародно-правових інструментів, які б закріплювали стандарти криміналізації найбільш небезпечних діянь у кіберпросторі та механізми транскордонної взаємодії правоохоронних органів.

У цьому контексті природним продовженням дослідження є звернення до положень Конвенції про кіберзлочинність 2001 року (Будапештська конвенція Ради Європи про кіберзлочинність), що стала першою універсальною міжнародно-правовою угодою, котра заклала фундаментальні підвалини міжнародної доктрини протидії злочинам у сфері інформаційних технологій. Зазначений документ репрезентує системне позиціювання щодо криміналізації правопорушень у кіберпросторі та водночас формує рамки для міждержавної координації у сфері кримінальної юстиції. Так, Конвенція закріплює низку зобов'язань для держав-учасниць, що охоплюють криміналізацію основних форм кіберзлочинності (несанкціонований доступ, незаконне перехоплення, втручання в дані та системи, зловживання пристроями), а також правопорушень, пов'язаних з використанням комп'ютерних технологій (шахрайство, підробка, порушення авторських прав). Особливістю Конвенції є її процесуальний вимір, котрий передбачає створення механізмів міжнародної співпраці, серед яких, зокрема, швидкий доступ до даних, взаємна правова допомога та екстрадиція. У такий спосіб документ виходить за межі суто кримінально-правового акту і набуває ознак комплексного інструменту глобальної кібербезпеки.

Ратифікація Конвенції Законом України № 2824-IV від 7 вересня 2005 року та набрання нею чинності для України з 1 липня 2006 року стало важливим етапом на шляху європейської інтеграції та гармонізації національного законодавства із міжнародними стандартами. Для вітчизняної

доктрини кримінального права це означало визнання нових форм злочинності об’єктом правового регулювання та потребу доктринального перегляду традиційних категорій, зокрема понять предмета злочину, способу вчинення правопорушення, доказів у цифровій формі [34].

Додатковий протокол 2003 року є логічним продовженням Будапештської конвенції 2001 року і спрямований на криміналізацію діянь, що мають расистський та ксенофобський характер, коли вони здійснюються через комп’ютерні системи. Його ухвалення відображає усвідомлення міжнародним співтовариством того факту, що поширення мови ненависті та дискримінаційних матеріалів через Інтернет може мати не менш руйнівні наслідки, ніж класичні форми злочинності.

Протокол вводить спеціальне поняття «расистський та ксенофобський матеріал», під яким розуміються тексти, зображення чи будь-які інші форми вираження, що пропагують, заохочують або виправдовують ненависть, дискримінацію чи насильство проти особи чи групи на підставі раси, кольору шкіри, етнічного походження, національності чи релігії, якщо остання використовується для виправдання расистських чи ксенофобських поглядів. Вказане визначення має базове значення, оскільки слугує підґрунтям для подальшої криміналізації низки діянь. Зазначений документ зобов’язує держави-учасниці передбачити кримінальну відповідальність за навмисне поширення через комп’ютерні системи расистських і ксенофобських матеріалів. Сюди належить як активне розміщення інформації, так і передача її через будь-які цифрові канали. Важливо, що відповідальність настає за умисне поширення, що дозволяє відмежувати кримінально-карані дії від випадкових чи технічно обумовлених процесів.

Досліджуваний акт встановлює кримінальну відповідальність за погрози, здійснені за допомогою комп’ютерних систем, якщо вони спрямовані проти особи чи групи людей на основі расових чи етнічних характеристик. Крім того, передбачено криміналізацію публічних образ у цифровому середовищі, коли такі образи мають расистський або

ксенофобський підтекст і створюють атмосферу ненависті та приниження гідності. Особливе місце у Протоколі займає стаття, яка зобов'язує держави карати за заперечення, грубе применшення, виправдання або схвалення геноциду та злочинів проти людяності, визнаних міжнародним правом. Це стосується, зокрема, Голокосту та інших злочинів, які підтверджені міжнародними судами. Водночас державам надано можливість обмежити застосування цієї статті лише випадками, коли такі дії вчиняються з метою розпалювання ненависті, дискримінації або насильства [18].

Слід підкреслити, що протокол передбачає відповідальність не тільки за безпосереднє вчинення зазначених злочинів, але і за пособництво, підбурювання чи замах, що розширює коло караних діянь і робить правове регулювання більш ефективним, враховуючи специфіку онлайн-простору, де участь у створенні чи поширенні контенту часто має колективний характер. Поряд із цим, документ поширює на нові склади злочинів процедурні механізми Будапештської конвенції, зокрема міжнародне співробітництво, взаємну правову допомогу, доступ до комп'ютерних даних та обмін електронними доказами, що дає змогу державам більш ефективно взаємодіяти у боротьбі з расистською та ксенофобською пропагандою в Інтернеті.

Варто наголосити, що у рамках ЄС імплементація Будапештської конвенції здійснювалася через ухвалення рамкових рішень і директив, до прикладу, Рамкове рішення 2005/222/ЈНА про атаки на інформаційні системи [8], замінене Директивою 2013/40/ЄС, яка зобов'язує встановити покарання за хакерство [140] тощо. ЄС також гармонізував відповідальність за інші кіберправопорушення. Директива 2011/93/ЄС [17], оновлена 2017 року, про боротьбу із сексуальним насильством щодо дітей зобов'язує криміналізувати онлайн-грумінг і перегляд веб-камера-матеріалів з дитячою порнографією; Директива 2017/541 про боротьбу з тероризмом – публічне підбурювання до тероризму в Інтернеті [138]; Директива 2019/713 про боротьбу з шахрайством у безготівкових платіжних засобах – фішинг та кібер-шахрайство тощо [139].

У сфері відповідальності інтернет-посередників і платформ Європейський Союз ще у 2000 році ухвалив Директиву про електронну комерцію, яка запровадила принцип обмеженої відповідальності провайдерів за контент третіх осіб. Згідно з нею постачальники інтернет-послуг звільняються від відповідальності за незаконний контент користувачів за умови, що вони не знали про його існування та оперативно видаляють його після отримання відповідного повідомлення [16].

Наразі ЄС модернізував зазначені правила у Регламенті 2022/2065 (Digital Services Act), відомий як Акт про цифрові послуги, який зберіг принцип обмеженої відповідальності, але ввів більш жорсткі вимоги до модерації контенту і прозорості алгоритмів для великих онлайн-платформ. Слід підкреслити, що зазначений документ є системоутворювальним елементом нової нормативної архітектури Європейського Союзу у сфері цифрового врядування, поява котрого зумовлена потребою подолати асиметрію між динамікою розвитку цифрових платформ та традиційними правовими механізмами контролю, що виявилися недостатніми для забезпечення належного рівня захисту прав і свобод людини у мережевому середовищі.

Акт про цифрові послуги встановлює комплекс обов’язків для суб’єктів, які виконують функції інтернет-посередників, і водночас запроваджує особливий правовий режим для великих онлайн-платформ та пошукових систем, які завдяки масштабам своєї діяльності набули статусу системно значущих для європейського цифрового простору. Зміст Регламенту відображає формування доктрини «відповідальної платформи», котра передбачає активне виконання позитивних обов’язків у сфері інформаційної безпеки шляхом створення процедур для оперативного видалення незаконного контенту із забезпеченням права користувачів на оскарження, а також про обов’язок запроваджувати механізми прозорості алгоритмічних систем, оцінювати та мінімізувати системні ризики, пов’язані з дезінформацією, маніпуляцією громадською думкою чи загрозами

демократичним процесам. Регламент також передбачає дієві механізми нагляду та санкційного впливу, серед яких можливість накладення значних штрафів на порушників, що свідчить про зростання ролі Європейської комісії як наднаціонального регулятора.

Досліджуваний документ передбачає трансформацію нормативного розуміння цифрового середовища від акценту на свободі обігу інформації до моделі, у якій свобода поєднується з відповідальністю та обмежується в інтересах захисту прав людини, громадської безпеки й демократичного ладу. Зазначена парадигма має безпосереднє значення і для України, адже адаптація національного законодавства до стандартів ЄС у сфері цифрових послуг є невід'ємним елементом євроінтеграційного курсу. Регламент ЄС 2022/2065 фактично закладає основу для формування нового типу юридичної відповідальності у цифровому середовищі, яка виходить за межі класичної моделі індивідуалізованого правопорушника і покладає на онлайн-платформи обов'язок активно забезпечувати дотримання прав і свобод у мережі.

Позитивним є те, що Європейський Союз в «Акті про цифрові послуги» фактично пропонує модель комплексного регулювання діяльності онлайн-платформ та встановлює зобов'язання щодо прозорості алгоритмів, модерації контенту, управління ризиками та санкції за їх невиконання [83]. Потенційно, ці підходи будуть трансформовані у міжнародні рамки.

Також звернемо увагу, що 22 вересня 2024 року світові лідери ухвалили Пакт майбутнього (Резолюцію A/RES/79/1), який охоплює Глобальний цифровий договір та Декларацію для майбутніх поколінь. Пакт є кульмінацією інклюзивного багаторічного процесу адаптації міжнародного співробітництва до викликів сьогодення та майбутнього і водночас наймасштабнішою міжнародною угодою за останні десятиліття, яка охоплює абсолютно нові сфери, а також питання, щодо яких не було досягнуто згоди протягом багатьох років. Він спрямований передусім на те, щоб міжнародні інституції могли ефективно функціонувати у сучасному світі. Як зазначив

Генеральний секретар: «Ми не можемо створити майбутнє, придатне для наших онуків і онучок, за допомогою системи, побудованої нашими бабусями і дідусями». Лідери виклали чітке бачення міжнародної системи, у рамках якої обіцянки будуть виконані і яка краще відображає сучасний світ, спираючись на енергію та досвід провідних держав, громадянського суспільства та інших ключових партнерів [51; 193].

Так, Європейський Союз обрав шлях прийняття спеціалізованих регуляторних актів, спрямованих на комплексне врегулювання питань відповідальності у сфері цифрових технологій. У 2024 р. було ухвалено Регламент про штучний інтелект (AI Act) – перший у світі нормативний акт такого рівня, що має на меті встановлення гармонізованих правил для безпечного використання систем штучного інтелекту та одночасний захист основоположних прав людини [22]. Досліджуваний акт має пряму дію в державах-членах ЄС, що забезпечує уніфікованість та гармонізованість стандартів правового регулювання використання штучного інтелекту в межах усього Союзу. Основними завданнями AI Act є:

– забезпечення безпеки систем штучного інтелекту та їхньої функціональності таким чином, щоб вони не порушували основоположні права людини;

– надання правової визначеності для розробників і постачальників відповідних технологій, що особливо важливо з огляду на високий рівень інноваційності цієї сфери;

– сприяння інноваціям у поєднанні з покладенням на суб’єктів технологічної діяльності конкретних обов’язків, пропорційних рівню ризику, який створює система (так званий risk-based approach).

Ключовим доктринальним елементом акта є принцип пропорційності, який передбачає диференційоване регулювання залежно від рівня ризику. Регуляторні обмеження встановлюються лише тоді, коли діяльність пов’язана зі значними загрозами для суспільних відносин та прав людини, і водночас залишаються мінімальними у сферах, де такі загрози є несуттєвими,

що дозволяє уникнути як надмірного втручання, що могло б стримувати інноваційний розвиток, так і прогалин у правовому регулюванні, здатних поставити під сумнів ефективність гарантій прав. В AI Act наведено класифікацію систем штучного інтелекту залежно від рівня ризику, який вони становлять. Зокрема, регламент виділяє кілька категорій:

– неприйнятний ризик («unacceptable risk») – використання ШІ у випадках, коли технологія порушує фундаментальні права чи створює надмірну небезпеку для суспільної безпеки та етики; до них належать, зокрема, системи соціального скорингу чи маніпулятивні технології, здатні підривати автономію людини;

– високий ризик – системи, що функціонують у критично важливих сферах (охорона здоров'я, транспорт, державне управління, освіта, правосуддя, діяльність правоохоронних органів) та підпадають під суворі вимоги щодо попередньої оцінки впливу, ведення документації, постійного моніторингу й забезпечення прозорості;

– обмежений ризик – застосування, які не створюють значної небезпеки, але вимагають певної прозорості, наприклад, інформування користувачів про взаємодію з системою штучного інтелекту чи позначення синтетичного контенту;

– мінімальний ризик – системи, які практично не несуть загрози правам і безпеці, а відтак регламентовані лише мінімальними вимогами або ж залишені в межах механізмів саморегулювання [218].

У сучасній зарубіжній науковій літературі справедливо підкреслюється, що у відносинах, пов'язаних із використанням систем штучного інтелекту, користувачі найчастіше перебувають у становищі інформаційної асиметрії, позаяк не мають достатніх знань та технічних можливостей для повної оцінки ризиків, які генерує відповідна технологія, а також стикаються зі значними труднощами у доведенні причинного зв'язку між роботою алгоритму та завданою шкодою. Безперечно, зазначене зумовлено складністю архітектури систем ШІ, непрозорістю алгоритмічних

процесів («black box problem»), а також багаторівневим характером ланцюга розробників, постачальників та інтеграторів. З метою подолання зазначених бар'єрів Регламент ЄС про штучний інтелект передбачає спеціальні процесуальні механізми, спрямовані на покращення позиції потерпілих у судових чи адміністративних провадженнях. До таких механізмів належать, зокрема, запровадження презумпцій щодо наявності причинного зв'язку та обов'язок прозорості для постачальників систем високого ризику, що передбачає розкриття документації, даних про навчання алгоритмів та інформації про їхнє функціонування. Наведені положення істотно спрощують доказування для позивачів і водночас стимулюють виробників та провайдерів забезпечувати належний рівень відповідності правовим стандартам. Завдяки цьому формується нова модель процесуальної рівноваги у сфері цифрових правовідносин, котра передбачає, що користувач отримує інструменти для ефективного відстоювання своїх прав, тоді як тягар доказування у значній мірі переноситься на суб'єктів, які контролюють функціонування та дизайн технології. Слід зауважити, що вказане відповідає загальній тенденції розвитку європейського права у сфері захисту споживачів і прав людини, відповідно до якої законодавець компенсує структурну нерівність сторін у високотехнологічних секторах [109, с. 85–120].

Важливим є той факт, що Регламент Європейського Союзу про штучний інтелект закріплює засади правового регулювання цифрових технологій, виходячи з того, що технічний прогрес не може існувати поза рамками права та фундаментальних прав людини. Його положення чітко відображають ідею, що свобода вираження, право на повагу до приватного життя та заборона дискримінації становлять базові орієнтири для визначення меж допустимого застосування штучного інтелекту.

У рамках нашого дослідження не можна оминути увагою і Лансаротську конвенцію, офіційно відому як Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства, котра була відкрита для підписання 25 жовтня 2007 року та набула чинності 1

липня 2010 року. Вона стала першим міжнародним договором, який комплексно врегулював питання криміналізації усіх форм сексуального насильства щодо дітей, у тому числі таких, що здійснюються із використанням інформаційно-комунікаційних технологій. Конвенція передбачає встановлення кримінальної відповідальності за сексуальні зловживання, втягнення дітей у проституцію та порнографію, виробництво, поширення та зберігання дитячої порнографії, сексуальні домагання в Інтернеті, так званий «грумінг» і будь-які форми корумпування дітей. Важливим елементом є не лише кримінально-правовий вимір, але і безперечно комплекс заходів із запобігання та захисту, які покладають на держави обов'язок проводити просвітницькі програми, забезпечувати підготовку фахівців, створювати дружні до дітей механізми правосуддя та розбудовувати систему допомоги жертвам. Конвенція також закріплює обов'язок міжнародної співпраці, у тому числі в сфері екстрадиції, обміну інформацією та координації розслідувань [36].

Подібні регіональні договори прийняті й в інших частинах світу. До прикладу, Конвенція Африканського Союзу з кібербезпеки та захисту даних 2014 року, відома як Конвенція Малабо, стала першим регіональним міжнародно-правовим актом, який у комплексній формі врегулював одразу три ключові сфери цифрових відносин, зокрема боротьбу з кіберзлочинністю, захист персональних даних та розвиток електронної комерції. Її положення визначають основні категорії правопорушень у сфері інформаційних технологій (незаконний доступ, втручання у системи, комп'ютерне шахрайство, поширення шкідливого контенту), закріплюють права суб'єктів персональних даних та обов'язки операторів щодо їх обробки, а також встановлюють правила укладення електронних договорів, використання електронного підпису та функціонування сертифікаційних органів. Важливою особливістю Конвенції є поєднання норм публічно-правового і приватно-правового характеру, що забезпечує її міжгалузевий характер та

створює цілісну модель правового регулювання у сфері цифрових технологій [108].

Зміст Конвенції Малабо передбачає адаптацію до напрацьованих у Європі моделей, зокрема до Будапештської конвенції про кіберзлочинність 2001 року та Конвенції Ради Європи № 108 про захист осіб у зв'язку з автоматизованою обробкою персональних даних. Використання цих зразків дозволило поєднати глобальні стандарти у сфері безпеки та конфіденційності з потребами африканських держав, які стикаються з різним рівнем розвитку цифрової інфраструктури та потребою стимулювати довіру до електронних сервісів. Відтак Конвенція фактично стала інструментом інтеграції Африканського континенту у світовий правовий простір кібербезпеки та захисту даних і створила підґрунтя для формування єдиної регіональної політики у цій сфері [31; 45, с. 80–86].

Також у рамках нашого дослідження звернемо увагу на Арабську конвенцію про боротьбу з правопорушеннями у сфері інформаційних технологій, прийнята Лігою арабських держав у 2010 році, котра є регіональним міжнародно-правовим актом, спрямованим на формування узгоджених підходів до криміналізації діянь у сфері інформаційних технологій та координацію зусиль держав-учасниць у протидії кіберзлочинності. Документ закріплює перелік спільних складів правопорушень, що відображають найпоширеніші загрози цифрового середовища, а саме: незаконний доступ до комп'ютерних систем та даних, несанкціоноване перехоплення інформації, використання шкідливого програмного забезпечення, електронне шахрайство, порушення авторських та суміжних прав у мережі, поширення забороненого контенту. Окремий розділ Конвенції присвячений процедурним механізмам взаємодії. Зокрема, передбачаються норми про обмін інформацією між компетентними органами, надання взаємної правової допомоги, координацію діяльності правоохоронних структур, а також визначаються умови екстрадиції осіб, підозрюваних у вчиненні злочинів у сфері інформаційних технологій [115].

Слід зауважити, що у науково-правовому контексті Конвенція 2010 року позиціонує тенденцію до побудови регіональних механізмів боротьби з кіберзлочинністю, що відрізняються від європейських та африканських за змістовними акцентами. Якщо європейські документи приділяють значну увагу гарантіям прав людини у сфері захисту даних, то досліджуваний документ виразно зорієнтований на забезпечення інформаційної та національної безпеки держав. У цьому аспекті Конвенція про боротьбу з правопорушеннями у сфері інформаційних технологій становить приклад адаптації загальносвітових тенденцій протидії кіберзлочинності до специфічного правового та культурного середовища арабських держав.

Африканська конвенція з кібербезпеки та захисту й Арабська конвенція про боротьбу з правопорушеннями у сфері інформаційних технологій є прикладами формування регіональних моделей реагування на виклики цифрового середовища. Якщо у першому випадку акцент зроблено на комплексному врегулюванні трьох сфер – кіберзлочинності, захисту персональних даних та електронної комерції – із прямим орієнтуванням на європейські стандарти (Будапештська конвенція, Конвенція №108), то у другому – на уніфікації складів злочинів та виробленні процедурної основи для співпраці між правоохоронними органами арабських держав.

На цьому тлі показовою є діяльність Організації американських держав (далі – ОАД), яка, на відміну від Африканського Союзу чи Ліги арабських держав, не пішла шляхом розроблення окремої конвенції. Натомість Організація американських держав (ОАД) зосередилася на розробленні модельних законів та ухваленні резолюцій рекомендаційного характеру, які орієнтують держави-члени на гармонізацію національного законодавства з міжнародними стандартами. У документах ОАД підкреслюється доцільність приєднання держав регіону до Будапештської конвенції або імплементації її положень у національне законодавство. Це свідчить про пріоритет адаптації до універсальних інструментів замість

створення власного автономного нормативного масиву, що забезпечує швидше та більш узгоджене інтегрування держав Американського континенту до глобальної архітектури кібербезпеки [112; 147].

Подібну тенденцію демонструють форуми Азійсько-Тихоокеанського регіону (далі – APEC), діяльність яких спрямована не на розробку обов'язкових міжнародних договорів, а на координацію політик у сфері кібербезпеки та формування принципів взаємного визнання. Показовим прикладом є APEC Privacy Framework 2005 року, що визначає базові стандарти захисту персональних даних, орієнтовані на поєднання вільного обігу інформації з гарантіями приватності. Зазначений документ став своєрідною моделлю «м'якого права», яка не має юридично обов'язкової сили, але використовується як орієнтир для зближення національних концепцій у досліджуваній сфері [113].

Відтак у світовій практиці простежуються різні моделі нормативного реагування на виклики цифрової доби. В окремих регіонах превалює підхід до укладення обов'язкових міжнародно-правових актів, як це засвідчують приклади Африканського союзу та Ліги арабських держав. В інших регіональних об'єднаннях застосовуються інструменти рекомендаційного характеру, що належать до сфери «м'якого права» (Організація американських держав, APEC). Незважаючи на відмінності у правових механізмах, усі ці концепції відображають спільну тенденцію – поступову гармонізацію норм національного права з положеннями Будапештської конвенції та міжнародними стандартами у сфері кібербезпеки і захисту персональних даних.

Регіональні ініціативи у сфері кібербезпеки та захисту даних, попри відмінності у правовій техніці та змістових акцентах, фактично стали складовою процесу глобальної уніфікації напрямків протидії кіберзлочинності та регулювання цифрових відносин. Так, до глобальних (універсальних) міжнародних документів у сфері юридичної відповідальності за правопорушення у мережі Інтернет відносяться багатосторонні угоди,

ухвалені під егідою ООН та інших всесвітніх організацій, які встановлюють серед іншого зобов'язання держав криміналізувати певні діяння в кіберпросторі та співпрацювати у боротьбі з ними. До них належить насамперед Конвенція ООН про кіберзлочинність 2024 р., Конвенція ООН проти транснаціональної організованої злочинності 2000 р [32], тощо. Також до цієї категорії можна віднести універсальні договори, що зобов'язують держави карати окремі види інтернет-злочинів, до прикладу, Факультативний протокол до Конвенції ООН про права дитини 2000 р. щодо торгівлі дітьми і дитячої порнографії [85], Конвенцію про запобігання геноциду та покарання за нього 1948 р. – щодо підбурювання до геноциду [33], Міжнародну конвенцію про ліквідацію расової дискримінації 1965 р. [44] – щодо розпалювання расової ненависті.

Прийняття у грудні 2024 р. Конвенції ООН про кіберзлочинність знаменувало новий етап розвитку міжнародного права у сфері протидії злочинам у кіберпросторі. Документ було схвалено Генеральною Асамблеєю ООН 24 грудня 2024 р. та відкрито для підписання державами. Він покликаний стати універсальним міжнародно-правовим інструментом, який регламентує криміналізацію базових форм кіберзлочинності, встановлює стандарти збирання та обміну електронними доказами, а також визначає механізми міжнародної правової допомоги і екстрадиції.

Предметне регулювання Конвенції охоплює незаконний доступ до інформаційних систем, втручання у дані та мережі, неправомірне перехоплення інформації, злочини сексуального характеру щодо дітей в Інтернеті, а також зобов'язання держав забезпечувати швидкий і безпечний обмін цифровими доказами не тільки у справах про кіберзлочини, але і щодо інших тяжких міжнародних злочинів [84], що розширює сферу дії документа та робить його інструментом протидії класичній комп'ютерній злочинності та сучасним загрозам інформаційній безпеці.

Юридичний статус Конвенції передбачає, що вона набере чинності після ратифікації не менш як сорока державами. Водночас уже на етапі

ухвалення документ отримав суперечливі оцінки, позаяк прихильники вбачають у ньому основу для глобальної уніфікації правил боротьби з кіберзлочинністю та гармонізації процедур збирання доказів [221], тоді як критики акцентують на ризиках для прав людини, зокрема, потенційному використанні неоднозначних положень у державах із низьким рівнем демократичних стандартів.

Так, навколо проєкту Конвенції ООН про кіберзлочинність розгорнулася широка дискусія, у якій зійшлися як держави, що вбачають у ній універсальний правовий інструмент протидії кіберзлочинності, так і правозахисні організації, які звертають увагу на потенційні загрози. Аналітичні матеріали вказують, що ключовим предметом критики стало недостатнє врегулювання гарантій захисту основоположних прав. Зокрема, у документі вбачаються ризики надмірно широкого застосування його положень, які можуть стати підґрунтям для переслідування журналістів, правозахисників чи політичних опонентів під приводом боротьби з кіберзлочинністю. Водночас відзначається нечіткість окремих дефініцій, що може призвести до надмірної криміналізації діянь, які в демократіях традиційно вважаються частиною свободи вираження поглядів або дослідницької діяльності у сфері інформаційної безпеки. Це створює загрозу принципу юридичної визначеності та підвищує ризик неоднакового тлумачення норм у різних державах.

Окремий блок критики стосується юрисдикційних положень, які передбачають можливість застосування так званої пасивної індивідуальної юрисдикції, що розширює межі втручання держав у випадках, коли правопорушення відбуваються поза їх територією, але пов’язані з їхніми громадянами чи інтересами. Вказане здатне спричинити серйозні колізії між національними правовими системами та ускладнити міжнародне співробітництво. Окрім зазначеного, правозахисні організації наголошують на відсутності достатніх механізмів підзвітності та незалежного контролю за застосуванням передбачених у Конвенції процедур. Особливу увагу

звертають на положення щодо збереження та передачі даних, які можуть порушувати право на приватність, презумпцію невинуватості та гарантії справедливого суду [77].

Конвенція ООН про кіберзлочинність 2024 року безперечно становить важливий крок до формування універсальної системи міжнародно-правових стандартів протидії злочинам у кіберпросторі. Вперше на глобальному рівні запропоновано уніфікований підхід до криміналізації основних форм кіберзлочинності, а також закріплено обов'язок держав співпрацювати у сфері збирання, збереження та передачі електронних доказів. У цьому вбачається значний потенціал для підвищення ефективності транскордонного правозастосування, особливо в умовах зростаючої глобалізації інформаційних потоків. З іншого боку, положення документа викликають низку серйозних доктринальних сумнівів, зокрема щодо відсутності достатніх гарантій захисту прав людини, нечіткості окремих правових дефініцій та розширеного тлумачення юрисдикційних підстав.

Зазначені формулювання здатні стати підґрунтям для надмірної криміналізації та для обмеження демократичних свобод, зокрема свободи вираження поглядів і права на приватність. Також вони створюють ризики використання Конвенції у політичних цілях, особливо в державах з недемократичними режимами.

У нашому баченні ефективність цієї Конвенції буде залежати від того, чи зможуть держави-учасниці забезпечити належну кореляцію між безпекою та свободою. Важливим видається доповнення її положень чіткими критеріями пропорційності та юридичної визначеності, а також створення незалежних механізмів моніторингу і контролю за їх імплементацією. Без цього Конвенція може залишитися не стільки інструментом глобальної безпеки, скільки потенційним джерелом правових конфліктів і загроз для основоположних прав людини.

Відтак, на основі проведеного аналізу доцільно висловити власну позицію щодо положень Конвенції та сформулювати низку пропозицій,

спрямованих на підвищення її ефективності як універсального міжнародно-правового інструменту:

– у тексті Конвенції варто забезпечити чітке та недвозначне визначення складів кіберзлочинів. Наявність нечітких формулювань створює загрозу довільного правозастосування, надмірної криміналізації та може призвести до обмеження законної діяльності, зокрема журналістської, дослідницької чи правозахисної;

– встановлені Конвенцією процедури збирання та обміну електронними доказами, а також заходи, що передбачають втручання у приватність, мають здійснюватися виключно на основі принципу пропорційності, котрий передбачає перевірку необхідності, доцільності та співмірності кожного втручання у сферу прав людини;

– для забезпечення належної підзвітності та запобігання можливим зловживанням необхідним є створення міжнародного органу або спеціальної процедури оцінки дотримання державами стандартів Конвенції. Вказаний механізм міг би здійснювати регулярний нагляд, проводити експертні огляди та видавати рекомендації щодо усунення виявлених порушень;

– Конвенція повинна бути гармонізована з уже чинними міжнародно-правовими інструментами у сфері кіберзлочинності, передусім із Будапештською конвенцією Ради Європи 2001 р., що дозволить уникнути дублювання норм, зменшить ризики колізій та сприятиме формуванню цілісної транснаціональної системи кримінальної юстиції у цифровому середовищі.

Поява та стрімкий розвиток інформаційних технологій у другій половині XX – на початку XXI століття спричинили формування нового типу протиправної поведінки, кіберзлочинів, які виходять за межі традиційних правових категорій і вимагають переосмислення механізмів юридичної відповідальності. У відповідь на вказані виклики Генеральна Асамблея ООН ухвалила у 2010 році Резолюцію 65/230, якою було започатковано підготовку всеосяжного дослідження у сфері кіберзлочинності [66]. Результатом стала

праця «Comprehensive Study on Cybercrime», підготовлена у лютому 2013 року Управлінням ООН з наркотиків та злочинності (UNODC) для використання міжурядовою експертною групою з кіберзлочинності [133].

Серед міжнародних доктринальних орієнтирів у сфері регулювання кіберпростору особливе місце займає «Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations» 2017 року, підготовлений групою міжнародних експертів за редакцією Майкла Шмітта під НАТО. Слід зауважити, що зазначений документ не має статусу міжнародного договору та не створює юридично обов'язкових норм у класичному розумінні міжнародного права. Водночас він становить систематизований виклад доктринальних позицій провідних фахівців у галузі міжнародного та кіберправа щодо того, яким чином чинні норми міжнародного права підлягають застосуванню у сфері кібероперацій. У його змісті міститься розгорнутий аналіз низки базових принципів, зокрема: 1) принципу суверенітету, який закріплює повноту юрисдикції держав у кіберпросторі та визначає неправомірним будь-яке іноземне втручання у їхні інформаційні системи чи інфраструктуру; 2) принципу невтручання, що забороняє державам здійснювати кібероперації, спрямовані на вплив на політичні, економічні чи соціальні процеси інших держав; 3) принципу заборони застосування сили, який поширюється на кібердії, наслідки яких прирівнюються до збройних атак у розумінні ст. 2(4) Статуту ООН; 4) принципу міжнародної відповідальності держав, що охоплює як дії їхніх органів, так і приватних осіб, які діяли під ефективним контролем держави; 5) принципу захисту прав людини, який підтверджує чинність міжнародних стандартів у сфері прав людини, зокрема свободи вираження поглядів і права на приватність у цифровому середовищі [205].

Не є новиною той факт, що зростання ролі цифрових технологій та глобальної мережі спричинило істотний приріст правопорушень, учинених із використанням Інтернету. Транскордонний характер кіберпростору дозволяє правопорушникам діяти поза межами окремих юрисдикцій, комбінувати

інфраструктуру, дані та інструменти з різних частин світу. У цих умовах ефективна протидія неможлива без узгоджених міжнародних стандартів і постійної оперативної взаємодії держав. Сучасна архітектура міжнародної реакції на правопорушення у мережі Інтернет у цьому ключі спирається на два взаємодоповнювальні напрями: 1) гармонізація матеріального та процесуального права через міжнародні стандарти; 2) оперативна взаємодія правоохоронних органів [93, с. 32–35].

У межах аналізу міжнародних механізмів увагу слід приділити Інтерполу, що виконує функцію глобального комунікаційного вузла для більш ніж 190 держав, підтримує захищені канали зв'язку, координаційні операції проти транснаціональних кіберугруповань, розвиває спроможності цифрової криміналістики та проводить тренінги [54, с. 16–28]. Поряд з Інтерполом, у європейському регіоні ключову роль у сфері протидії кіберзлочинності відіграє Європол, який координує взаємодію правоохоронних органів держав-членів ЄС та виконує роль аналітичного і координаційного центру, зокрема через Європейський центр боротьби з кіберзлочинністю (EC3) і платформу обміну SIENA забезпечує збір, аналіз і поширення розвідувальної інформації, підтримує спільні слідчі групи, координує операції та готує регулярні оцінки загроз. У сукупності зазначені механізми дають змогу виявляти інфраструктуру правопорушень, синхронізувати процесуальні дії в різних державах і підвищувати доказову спроможність проваджень [47, с. 15–20].

Прикладом ефективності міжнародної кооперації у сфері протидії кіберзлочинності стала операція «Black Axe», ініційована Інтерполом за участі правоохоронних органів кількох континентів. Угруповання «Black Axe», що виникло у Нігерії та з часом трансформувалося у розгалужену транснаціональну кримінальну структуру, спеціалізувалося на шахрайстві в мережі Інтернет, зокрема на схемах «business email compromise», фішингових атаках, підроблених банківських рахунках та фальшивих інвестиційних проєктах [223]. Масштабність діяльності цього угруповання призвела до

значних економічних збитків приватних осіб і бізнесу у різних державах. Завдяки скоординованим діям Інтерполу та Європолу було забезпечено обмін інформацією, проведено спільні оперативно-розшукові заходи та арештовано десятки осіб у Нігерії, США, Італії та ін [177, с. 456–480]. Вказане є наочною демонстрацією, що боротьба з транснаціональними кіберзлочинними мережами можлива тільки через поєднання національних і міжнародних правових механізмів та постійне вдосконалення законодавства. Операція «Black Axe» підтвердила, що міжнародні стандарти юридичної відповідальності у сфері кіберзлочинів мають практичну ефективність лише за умови реального співробітництва правоохоронних органів різних держав [92, с. 36–38; 164].

У цьому контексті протидія кіберзлочинності потребує комплексного підходу, що поєднує впровадження сучасних технічних рішень із постійним удосконаленням правових механізмів. Ключове значення при цьому мають міжнародне співробітництво, підвищення рівня професійної підготовки фахівців у сфері кібербезпеки, а також систематичне оновлення національного законодавства відповідно до динаміки цифрових загроз [76, с. 73–80].

В. Б. Скоморовський та В. В. Корольова акцентують свою увагу на тому, що для України аналіз міжнародної практики відкриває можливості для підвищення ефективності національного цифрового регулювання. Важливо забезпечити чіткі гарантії доступу до Інтернету, активізувати розвиток електронного урядування, удосконалити нормативну базу електронних послуг і сформувати збалансовану систему інформаційної безпеки, яка одночасно захищатиме державні інтереси та права громадян [70, с. 1411–1419].

Взаємозв’язок нормативної та оперативної площин має принципове значення. Гармонізовані склади злочинів і уніфіковані процесуальні інструменти зменшують ризик правових «розривів», через які правопорушники уникають відповідальності. Натомість оперативні мережі

забезпечують практичну реалізацію цих норм у темпах, співмірних з «леткістю» електронних доказів. Поєднання гармонізації норм і постійної оперативної взаємодії формує каркас міжнародних стандартів юридичної відповідальності за правопорушення в Інтернеті, що забезпечує сумісність національних інструментів, швидкість реагування на транскордонні загрози та належний рівень гарантій для людини в цифровому середовищі.

Слід підкреслити, що проведений аналіз міжнародних стандартів у сфері юридичної відповідальності за правопорушення у мережі Інтернет дозволяє зробити ряд висновків:

міжнародна нормативна база у цій сфері є фрагментованою за географічною та предметною ознакою, проте спостерігається тенденція до її уніфікації. Прийняття глобальної конвенції ООН про кіберзлочинність знаменувало перехід від регіонально сконцентрованих зусиль до справді універсального позиціювання, відкрило можливість для встановлення мінімальних світових стандартів криміналізації та співробітництва, а також усунуло правові колізії, якими раніше користувалися кіберзлочинці, переховуючись у державах поза дією Будапештської конвенції;

входження до глобальних домовленостей значно ширшого кола держав з різними правовими системами породжує виклик дотримання прав людини. Як показав аналіз фінального тексту конвенції ООН, відсутність жорстких гарантій може бути використана авторитарними режимами для переслідування інакодумців під приводом боротьби з кіберзлочинами. Позитивним прикладом є включення у кіберконвенцію норм про необхідність поваги до свободи вираження поглядів і переконань, приватності та пропорційності втручань;

найбільше розвинені стандарти стосуються саме кримінальної відповідальності, що історично обумовлено першочерговим фокусом на кіберзлочинності. Натомість міжнародні механізми цивільно-правової та адміністративної відповідальності, до прикладу, відшкодування шкоди від кібератак приватним особам, санкції до інтернет-компаній за порушення

правил безпеки чи конфіденційності тощо, розвинені значно менше та носять характер радше рекомендацій, ніж обов'язкових норм. На нашу думку, у перспективі варто очікувати розвитку саме таких «горизонтальних» стандартів, зокрема у сфері відповідальності постачальників цифрових послуг;

ефективність міжнародних стандартів корелюється із належною імплементацією на національному рівні. Навіть після приєднання до міжнародних договорів окремі держави не забезпечують повної гармонізації внутрішнього законодавства; не всі передбачені Конвенцією про кіберзлочинність діяння отримують належну криміналізацію, а процесуальні механізми щодо збирання та вилучення електронних доказів залишаються фрагментарними. У цьому зв'язку пріоритетного значення набуває системний моніторинг виконання міжнародних зобов'язань та надання технічної допомоги державам у процесі їхньої імплементації. Таку функцію виконують, зокрема, інструменти Ради Європи та діяльність Управління ООН з наркотиків і злочинності, яке реалізує програми технічної допомоги у сфері кіберзлочинності та електронних доказів.

Наостанок слід зазначити, що міжнародне співтовариство визнає: боротьба з правопорушеннями в Інтернеті не може обмежуватися виключно репресивними заходами. Стандарти дедалі більше зміщуються у бік комплексного механізму шляхом поєднання відповідальності з просвітою користувачів, кібергігієною, партнерством з приватним сектором та повагою до відкритості мережі. Нові міжнародні документи та ініціативи мають шанс закріпити й розвинути зазначені принципи. Відтак міжнародні стандарти у сфері юридичної відповідальності за інтернет-правопорушення знаходяться в стадії динамічного розвитку, позаяк від фрагментарних регіональних норм вони еволюціонують до цілісної системи універсальних правил, що враховують як потребу у безпеці, так і необхідність збереження фундаментальних прав і свобод у цифрову епоху.

2.2. Загальнотеоретичні характеристики правопорушень у мережі Інтернет та їх правова кваліфікація

Юридична відповідальність у загальнотеоретичному вимірі постає однією з базових категорій права, що концентрує у собі імперативно-примусовий характер правового регулювання у разі порушення встановлених норм. У класичному доктринальному підході її розмежування здійснювалося передусім за галузевим критерієм (кримінальна, адміністративна, цивільна, дисциплінарна відповідальність). Водночас становлення та інтенсивна експансія цифрового простору, насамперед мережі Інтернет, спричинили істотну трансформацію усталених уявлень про природу та форми реалізації юридичної відповідальності. Віртуальне середовище розширило просторово-функціональні межі правопорушень та ускладнило процедури їх виявлення, кваліфікації та реалізації санкцій.

Серед ключових ознак юридичної відповідальності за правопорушення в мережі Інтернет доцільно виокремити кілька визначальних характеристик:

– транснаціональний характер, оскільки переважна більшість правопорушень в мережі Інтернет виходять за межі національних юрисдикцій, що зумовлює складнощі у визначенні компетентного органу та виборі застосовного права;

– ускладнена ідентифікація суб’єкта, позаяк в умовах анонімності, використання псевдонімів, VPN-технологій, блокчейну та систем шифрування постає об’єктивна проблема встановлення особи правопорушника;

– комплексний характер складу правопорушення, адже правопорушення в мережі Інтернет поєднують технічні, поведінкові, інтелектуальні та інші елементи, що значно ускладнює правову кваліфікацію;

– множинність нормативного впливу, яка проявляється у взаємодії норм національного законодавства, міжнародно-правових стандартів, актів

м’якого права та корпоративних політик цифрових платформ, що створює багаторівневу модель регулювання [90, с. 909–914].

Юридичну відповідальність за правопорушення у мережі Інтернет доцільно розглядати крізь призму модусу каузальності та контролю у взаємодії «користувач – посередник – алгоритм – платформа», тобто залежно від того, який суб’єкт генерує деліктний ризик, яким чином цей ризик поширюється цифровою інфраструктурою, якою мірою він піддається управлінню та як у результаті конфігурується коло суб’єктів юридичної відповідальності. Запропоноване позиціювання дозволяє поєднати техніко-організаційні параметри цифрового середовища з юридичними ознаками вини, належної обачності та розподілу тягаря доказування. У межах цього вектору ми виділяємо п’ять різновидів юридичної відповідальності:

1) Вторинна (умовна) юридична відповідальність, яка поширюється на інтернет-провайдерів та адміністраторів онлайн-платформ. Її характерною ознакою є відсутність безумовного обов’язку контролювати або редагувати інформацію, розміщену користувачами, адже такі суб’єкти виступають технічними посередниками, а не повноцінними авторами контенту. Водночас на них покладається зобов’язання реагувати на виявлення протиправної інформації у разі отримання відповідного повідомлення від компетентних органів чи зацікавлених осіб [225].

2) Саморегуляторна відповідальність, котра ґрунтується на механізмах внутрішнього реагування, запроваджених безпосередньо цифровими платформами або онлайн-спільнотами. Зазначений різновид відповідальності регулюється правилами, стандартами та протоколами поведінки, що не мають формального нормативного закріплення в актах держави, проте виконують функціонально значущу регулятивну роль, а також забезпечують порядок взаємодії користувачів у межах конкретного цифрового простору. У цьому контексті саморегуляція реалізується через стандарти спільноти (community standards), умови користування сервісом (terms of service), алгоритмічні системи модерації та фільтрації контенту, а також процедури

повідомлень і скарг, що формують специфічний рівень «квазізаконодавства» у сфері цифрових комунікацій [132].

Показовим прикладом реалізації саморегуляторної відповідальності у цифровому просторі є практика провідних транснаціональних корпорацій та глобальних технологічних платформ, які виробили розгалужені політики щодо допустимості та модерації контенту. У межах таких політик встановлюються обмеження стосовно поширення мови ворожнечі, дезінформації, матеріалів із ознаками сексуального насильства, терористичної пропаганди та інших небезпечних форм цифрового контенту. Зазначені регулятивні акти зазвичай оформлюються у вигляді відкритих публічних документів, що є доступними для користувачів і періодично переглядаються з огляду на динаміку соціальних процесів та технічні новації. Водночас наукова дискусія щодо ефективності цих механізмів залишається актуальною, оскільки їх застосування нерідко супроводжується питаннями про межі свободи вираження поглядів, прозорість алгоритмічних рішень і відповідність процедур стандартам належного процесу [182].

У науковій літературі обґрунтовано наголошується на низці концептуальних проблем, що супроводжують функціонування режиму саморегуляторної відповідальності цифрових платформ: а) непрозорість алгоритмів – відсутність відкритості у функціонуванні автоматизованих систем модерації та фільтрації контенту, що унеможливлює оцінку їх відповідності принципам правової визначеності, пропорційності та справедливості [123, с. 195–202]; б) недостатність процедур оскарження – обмеженість або формальність механізмів апеляції рішень модераторів, що позбавляє користувачів реальної можливості захистити свої права у випадках необґрунтованого видалення контенту чи блокування акаунтів; в) асиметричність застосування стандартів – нерівномірність у практиці регулювання, коли однакові правила застосовуються по-різному до різних категорій користувачів, що суперечить принципу рівності перед законом і створює простір для дискримінації; г) відсутність зовнішнього контролю –

відсутність незалежних механізмів моніторингу та оцінки правомірності корпоративних рішень платформ щодо управління контентом, що породжує ризики свавільності та ставить під сумнів їхню легітимність з огляду на стандарти прав людини [110, с. 153–169].

Сьогодні можна констатувати колосальні масштаби алгоритмізованого контролю у цифровому середовищі, що свідчить про фактичне перетворення автоматизованих систем на ключових суб'єктів ухвалення рішень у сфері регулювання інформаційних потоків. Водночас лише незначна частка таких рішень підлягає безпосередній людській перевірці, тоді як переважна більшість формується алгоритмами машинного навчання. Це, своєю чергою, зумовлює низку доктринальних і практичних ризиків, серед яких помилкова кваліфікація правомірного контенту як забороненого, непропорційне обмеження свободи вираження поглядів, а також посилення ефекту «цифрової цензури» за відсутності належних процесуальних гарантій [158].

У правовій площині вказана ситуація актуалізує питання про відповідність алгоритмізованої модерації базовим стандартам захисту прав людини, зокрема статті 10 Європейської конвенції з прав людини, яка гарантує свободу вираження поглядів. Проблемним аспектом є також відсутність прозорості алгоритмів, за допомогою яких ухвалюються рішення, що позбавляє користувачів можливості оцінити їх правомірність та оскаржити.

Окремої уваги заслуговує аспект відсутності зовнішнього контролю за правомірністю рішень щодо блокування чи видалення контенту. У результаті право на доступ до інформації та свободу вираження поглядів фактично обмежують приватні корпорації, які діють поза межами класичного правового поля та створюють власні регулятивні системи, але не несуть належної публічно-правової відповідальності.

У сучасних умовах особливої ваги набуває питання необхідності належного державного та наднаціонального регулювання саморегуляторних

практик цифрових платформ. У цьому контексті показовим є Регламент Європейського Союзу «Про цифрові послуги» 2022 року, який установив обов'язкові стандарти прозорості, підзвітності та оцінки системних ризиків [105]. У цьому світлі саморегуляторна відповідальність є вразливою через непрозорість алгоритмів, ризики селективного застосування стандартів та відсутність дієвих процедур зовнішнього контролю. Її ефективність прямо залежить від рівня відкритості платформ до інституційного нагляду, залучення громадськості до процесу формування правил, а також від здатності держави забезпечити належну кореляцію між гарантією свободи вираження поглядів і протидією поширенню шкідливого чи незаконного контенту.

Концепція подвійної легітимації саморегуляторної відповідальності за правопорушення у мережі Інтернет передбачає, що внутрішні правила та політики онлайн-платформ можуть визнаватися ефективними тільки у разі їх відповідності двом взаємопов'язаним вимірам легітимності:

внутрішньому (автономному) – коли спільнота користувачів визнає правила справедливими, прозорими та такими, що забезпечують належний рівень захисту їхніх інтересів. Вказане забезпечується через публічність стандартів спільноти, доступність механізмів оскарження рішень та дотримання принципу недискримінації при їх застосуванні;

зовнішньому (міжнародно-правовому) – коли такі правила узгоджуються з принципами міжнародних документів та практикою міжнародних інституцій, зокрема стандартами ЄСПЛ і ЄС щодо свободи вираження поглядів, захисту персональних даних, запобігання мові ворожнечі тощо. У цьому контексті саморегуляторні механізми отримують додаткову нормативну легітимацію через відповідність правозахисним орієнтирам.

3) Колективна форма юридичної відповідальності у мережі Інтернет постає як реакція на складність атрибуції правопорушень, коли їх вчинення зумовлене взаємодією значної кількості суб'єктів, зокрема користувачів,

адміністраторів платформ, розробників алгоритмів, хостинг-провайдерів тощо. Її сутність полягає в тому, що відповідальність не може бути обмежена окремим індивідом, адже делікт у цифровому середовищі виникає як результат системної взаємодії колективного суб'єкта. У цьому контексті формується доктрина «розподіленої вини», що передбачає покладення юридичних наслідків на сукупність учасників цифрової екосистеми за результат їхньої спільної діяльності [216; 217].

У світовій правовій думці проблема колективної відповідальності розробляється у контексті концепцій «мережевої відповідальності» та «інституційної відповідальності», які підкреслюють, що у високотехнологічному суспільстві шкода рідко зумовлюється діями одного суб'єкта, а є наслідком складних соціально-технічних комбінацій [160]. Подібні підходи простежуються і в межах кіберетики та регулювання штучного інтелекту, де доводиться, що алгоритмічні рішення не можуть бути віднесені до «персоналізованого» суб'єкта, а потребують концептуального оформлення у вигляді колективної відповідальності [148].

4) Алгоритмічна (автоматизована). Зростаюче використання штучного інтелекту та алгоритмічних систем у процесах ухвалення рішень актуалізує питання юридичної відповідальності за наслідки їх функціонування. Автоматизована юридична відповідальність охоплює ситуації, за яких деліктогенний ефект породжується діями або рішеннями, сформованими алгоритмічними системами чи системами штучного інтелекту за відсутності безпосереднього людського контролю або втручання. На відміну від класичної моделі юридичної відповідальності, у межах якої суб'єктом правопорушення виступає фізична або юридична особа, у цьому випадку на перший план виходить проблема проксі-суб'єктності цифрових систем, тобто опосередкованого приписування відповідальності через осіб, які розробляють, впроваджують, контролюють або використовують алгоритмічні механізми [128, с. 513–520]. Автоматизована відповідальність не передбачає буквального наділення алгоритмів статусом правового суб'єкта, однак вона

виражає необхідність запровадження особливого механізму юридичного реагування, який враховує технічну автономію програмних комплексів. Її запровадження відкриває шлях до доктрини «технологічної відповідальності», що вимагає адаптації традиційних категорій вини, умислу, необережності до умов алгоритмічного прийняття рішень [194].

5) Множинна (гібридна) відповідальність. У цифровому просторі поступово утверджується концепт множинної (гібридної) юридичної відповідальності, виникнення якого пов’язане з транснаціональною природою Інтернету та взаємодією людського і алгоритмічного чинників у процесі вчинення правопорушень. Функціонування глобальної мережі створює умови для здійснення діяльності компаніями та індивідами у відносинах з користувачами різних держав, що обумовлює можливість одночасного поширення на них правових режимів кількох юрисдикцій.

Показовою у досліджуваному контексті є справа «Illinois v. Hemi Group LLC» 2010 року, у якій Верховний суд США постановив, що компанія, яка здійснювала продаж сигарет через Інтернет резидентам штату Іллінойс, підлягає юрисдикції його судів, попри відсутність фізичної присутності на території штату [162]. Наведений прецедент засвідчив, що транскордонна природа цифрових правопорушень нівелює класичний критерій територіальності та вимагає нових критеріїв щодо визначення меж правозастосування.

У науковій доктрині множинна відповідальність осмислюється як результат «подвійної атрибуції», ситуації, за якої правопорушення є наслідком взаємодії людської волі та алгоритмічних рішень. У таких випадках правопорушення не може бути віднесене винятково до дій особи чи до функціонування цифрового середовища, адже результат формується шляхом синергії двох компонентів:

1) поведінкового, котрий охоплює людський вибір, умисел, необережність тощо;

2) технічного, що передбачає алгоритмічне опрацювання даних, автономні дії програмних систем та ін. [194].

На наш погляд, множинну (гібридну) юридичну відповідальність у мережі Інтернет варто розглядати як комплексну форму правової реакції, що виникає внаслідок поєднання транскордонної багатоюрисдикційності та взаємодії людського і алгоритмічного факторів у процесі вчинення правопорушення. До її ознак варто віднести наступні:

1) характеризується «подвійною атрибуцією», за якої деліктогенний результат одночасно є наслідком вольових рішень людини та автономних або напівавтономних дій цифрових систем;

2) не зводиться до класичної індивідуалізації суб'єкта, а передбачає розподіл правових наслідків між кількома рівнями, зокрема особою, яка ініціює чи контролює процес, оператором платформи, а також технічною інфраструктурою, що генерує правопорушний ефект;

3) становить новий інститут загальної теорії права, що вимагає:

– формування критеріїв оцінки ступеня алгоритмічної автономії та меж людського контролю;

– перегляду традиційних категорій вини та необережності в умовах алгоритмізованого середовища;

– вироблення механізмів юрисдикційної координації для подолання колізій багатоярусного правозастосування [94, с. 75–77].

Слід акцентувати, що стрімкий розвиток цифрових технологій і зростання ролі мережі Інтернет як ключового середовища суспільної комунікації зумовлюють появу нових форм правопорушень, які характеризуються власними, специфічними ознаками. У віртуальному просторі відбувається трансформація класичних підстав та умов юридичної відповідальності, зокрема у частині суб'єктного складу, причинно-наслідкового зв'язку, форми вини та юрисдикційної прив'язки, що істотно ускладнює їх однозначне тлумачення та практичне застосування. Зазначені обставини актуалізують необхідність систематизації правопорушень, що

вчиняються у мережі Інтернет, із визначенням релевантних класифікаційних критеріїв з урахуванням особливостей цифрового середовища.

До загальновизнаних та усталених у правовій доктрині й міжнародній практиці різновидів правопорушень у мережі Інтернет, зокрема, належать:

І. За об'єктом посягання:

правопорушення у сфері інформаційної безпеки (несанкціонований доступ до даних, злам інформаційних систем, поширення шкідливого програмного забезпечення) [80, с. 38–47];

порушення персональних немайнових прав (кібербулінг, онлайн-образи, поширення недостовірної інформації, втручання у приватне життя) [73];

порушення прав інтелектуальної власності (піратство, нелегальне поширення цифрового контенту, несанкціоноване використання авторських творів) [67, с. 20];

економічні правопорушення у кіберпросторі (шахрайство з використанням електронних платіжних систем, маніпуляції з криптовалютами, створення фінансових пірамід у мережі);

порушення регулятивних вимог цифрових платформ (порушення умов користування сервісами, зловживання алгоритмами, маніпуляція даними користувачів) тощо.

ІІ. За способом здійснення (залежно від методів і технічних засобів):

злом або несанкціонований доступ – правопорушення, котрі передбачають злом акаунтів, доступ до закритих інформаційних систем та злом захищених ресурсів;

розповсюдження шкідливого програмного забезпечення – поширення вірусів, троянських програм та іншого шкідливого програмного забезпечення з метою завдання шкоди інформаційним системам [81, с. 94–95];

соціальна інженерія та фішинг – методи обману, що використовуються для отримання доступу до конфіденційної інформації шляхом маніпулювання довірою користувачів;

шахрайські схеми з банківськими картками, інвестиційне шахрайство, а також різні фінансові незаконні операції в Інтернеті.

III. За принципом юрисдикційної належності (територіальною ознакою):

національні правопорушення, що вчиняються всередині однієї держави;

транскордонні правопорушення, які охоплюють кілька держав [12].

IV. За рівнем суспільної небезпеки:

кіберзлочини – тяжкі злочини, які завдають значної шкоди особам, організаціям та суспільству [28, с. 202–214];

адміністративні правопорушення у мережі Інтернет, що не несуть серйозної суспільної небезпеки, однак за їх вчинення можуть бути накладені адміністративні санкції.

Безперечним є той факт, що правова природа досліджуваної юридичної відповідальності безпосередньо детермінується характеристиками правопорушень, які виникають у мережі Інтернет. Адже лише крізь призму їхнього змісту та структури можливо обґрунтувати межі застосування примусових заходів, визначити належних суб’єктів та забезпечити правову визначеність.

Проведене дослідження В. Б. Скоморовського та В. В. Корольової показує, що теоретико-правові засади формування складу правопорушень в Інтернеті перебувають на етапі активного розвитку та характеризуються відсутністю єдиної доктринальної позиції. Швидкий розвиток цифрових технологій спричиняє виникнення нових видів протиправних діянь, які не завжди вкладаються в межі традиційних правових конструкцій, створюючи розрив між реальною практикою та можливостями законодавства [71, с. 2903–2912].

Тому наступним елементом дослідження є виокремлення та теоретичне осмислення ключових ознак правопорушень у цифровому

середовищі, що зумовлюють необхідність формування оновлених доктринальних підходів до інституту юридичної відповідальності.

Аналіз правопорушень у кіберпросторі потребує врахування особливостей цифрового середовища, що відмежовують їх від класичних деліктів у межах традиційно усталеного розуміння:

1) Відсутність територіальної визначеності є однією з базових характеристик деліктної поведінки у цифровому середовищі, яка істотно трансформує класичні доктринальні уявлення про юрисдикцію та межі дії правових норм. На відміну від традиційних правопорушень, локалізованих у чітких просторових межах, правопорушення у мережі Інтернет здійснюються у віртуальному просторі, що не має фізичних кордонів. Вказане передбачає, що одна і та сама протиправна дія може водночас зачіпати кілька держав та створювати феномен багатошарової юрисдикційності, що передбачає:

а) юрисдикційну конкуренцію, коли декілька держав претендують на застосування власного права до одного і того ж делікту;

б) правову лакунарність, оскільки відсутність єдиних стандартів створює ризик невідповідності національних регулятивних норм;

в) фрагментацію правозастосування, котра передбачає, що різні держави кваліфікують одні і ті самі дії по-різному, що перешкоджає уніфікованому реагуванню на глобальні кіберзагрози.

У доктринальному вимірі досліджувана ознака виявляє кризу територіального принципу юрисдикції як традиційної основи правового регулювання. Правова теорія стикається з необхідністю переосмислення концептуальних засад просторової дії права, зокрема через застосування принципів екстериторіальності, функціональної юрисдикції та універсальності у сфері кіберправопорушень. Відсутність територіальної визначеності у цифровому середовищі ускладнює застосування класичних інструментів правової кваліфікації та актуалізує потребу у міждержавній координації, гармонізації законодавства та виробленні спільних стратегій щодо визначення компетентних органів і застосовного права, що в

перспективі має сформувати підґрунтя для створення глобальної архітектоніки кіберправосуддя.

2) Технологічна складність правопорушень у мережі Інтернет визначається тим, що їх вчинення та подальша ідентифікація ґрунтуються на застосуванні спеціальних знань у сфері програмування, криптографії, блокчейн-технологій, штучного інтелекту та інших високотехнологічних рішень. До прикладу, спосіб вчинення, який у «традиційному праві» має допоміжне значення, у сфері Інтернет-правопорушень стає визначальною характеристикою, адже від технічної складності залежить як кваліфікація діяння, так і можливість притягнення суб'єкта до відповідальності [130].

У правозастосовній площині технологічна складність обумовлює залежність ефективності слідства і судового розгляду від рівня технічної підготовки правоохоронних органів. Без спеціальних знань та технічних інструментів держава фактично втрачає здатність забезпечувати дієвість принципу невідворотності відповідальності.

3) Дистанційність та віртуалізація дій. На відміну від класичних форм протиправної поведінки, що передбачають фізичну присутність правопорушника у місці вчинення шкоди, у цифровому середовищі локалізація діяння втрачає матеріальний вимір. Віртуальний простір створює умови, за яких суб'єкт може завдати шкоди об'єктам правового захисту, перебуваючи на значній відстані, у тому числі в іншій юрисдикції, без необхідності фізичного контакту. Вказаний феномен істотно трансформує класичні підходи до кваліфікації деліктів, адже правопорушення у віртуальному вимірі відбувається не у географічно визначеному просторі, а у цифровому середовищі, що саме по собі є транстериторіальним. Зазначене створює значні виклики для традиційних механізмів правозастосування, від ускладненої ідентифікації locus delicti до потреби міжнародної координації для визначення компетентного органу та застосовного права. Віртуалізація дій у мережі також призводить до нового типу правової взаємодії, де

причинно-наслідковий зв’язок між діями суб’єкта і наслідками може бути опосередкованим технологічними процесами.

4) Анонімність та псевдоанонімність суб’єкта істотно впливає як на процес ідентифікації правопорушника, так і на забезпечення невідворотності юридичної відповідальності. Використання псевдонімів, систем шифрування, VPN-технологій, а також механізмів децентралізованих мереж створює ситуацію, за якої класичні інструменти процесуального доказування виявляються малоефективними. Унаслідок цього суб’єкт правопорушення у мережі Інтернет фактично може залишатися поза межами правової юрисдикції, що у свою чергу відтерміновує притягнення до юридичної відповідальності на невизначений строк [104, с. 313; 169, с. 54–64].

Анонімність у кіберпросторі має подвійний характер, позаяк забезпечує реалізацію права на приватність та свободу вираження поглядів і переконань, але одночасно створює правові прогалини, які активно використовуються правопорушниками для уникнення контролю та правозастосовних заходів [88, с. 36–38]. Псевдоанонімність як проміжна форма маскування особи сприяє появі правової невизначеності щодо суб’єкта притягнення до юридичної відповідальності. Зазначена ознака має три ключові вектори: а) епістемологічний, позаяк ускладнює встановлення фактичних обставин і перешкоджає формуванню доказової бази; б) процесуальний, бо обмежує застосування класичних процедур переслідування, оскільки неможливо ідентифікувати конкретного носія деліктної поведінки; в) правоохоронний, що стимулює зростання кількості кіберделіктів через відчуття безкарності та мінімальні ризики для суб’єкта правопорушення.

У результаті анонімність і псевдоанонімність слід розглядати як системний виклик для сучасної теорії юридичної відповідальності, що вимагає розробки нових міждисциплінарних напрямків, від впровадження спеціальних правових режимів ідентифікації у цифровому середовищі до концептуалізації доктрини «цифрової презумпції доброчесності», яка

дозволяла б збалансувати право на приватність із потребами ефективного правозастосування.

5) Масовість та колективний характер впливу правопорушень у мережі Інтернет становлять одну з ключових їхніх доктринальних особливостей. На відміну від класичних деліктів, де шкода зазвичай має індивідуалізований характер та стосується обмеженого кола потерпілих, у цифровому середовищі навіть поодинокий акт може спричинити одночасне порушення прав та інтересів значної кількості суб'єктів. До прикладу, здійснення правопорушення у вигляді поширення фішингового повідомлення або шкідливого програмного забезпечення здатне вражати тисячі чи навіть мільйони користувачів та формувати ефект «ланцюгової реакції» [68, с. 229].

Зазначена специфіка зумовлює трансформацію об'єкта посягання, позаяк шкода завдається не тільки окремій особі, але і також цілісним соціальним групам чи навіть інституціям, що підсилює суспільну небезпеку кіберделіктів. Відтак виникає потреба у нових механізмах колективного захисту. Також слід звернути увагу, що масовий характер впливу формує додаткові вимоги до пропорційності та адекватності юридичної відповідальності, адже класичні моделі санкцій нерідко виявляються недостатніми для відновлення порушеної правової рівноваги.

6) Розмитість об'єкта правопорушення у цифровому середовищі є однією з фундаментальних ознак, що відрізняє його від традиційної деліктології [157]. У сфері кіберпростору об'єктом посягання виступають переважно нематеріальні категорії – інформаційні ресурси, цифрова репутація, персональні дані, інтелектуальна власність. Вказана трансформація об'єкта правопорушення передбачає відсутність матеріальної субстанційності, котра ускладнює юридичну ідентифікацію шкоди, адже порушення нематеріальних прав не завжди можна виміряти у класичних економічних показниках [224]. Окрім зазначеного, розмитість об'єкта обумовлює високу варіативність правових наслідків, від відновлення

репутаційної шкоди до комплексної компенсації за незаконне використання інтелектуальної власності чи витік персональних даних [137; 170].

Порушення прав інтелектуальної власності в Інтернеті потребує створення багаторівневого та спеціалізованого правового механізму захисту, який враховує особливості віртуального середовища, включаючи труднощі з ідентифікацією порушників, поширенням контенту та відповідальністю власників веб-сайтів і провайдерів [75, с. 72–78].

7) Варіативність правового регулювання у сфері Інтернет-правопорушень є однією з найскладніших доктринальних і практичних проблем. На відміну від класичних деліктів, що зазвичай регулюються нормами єдиного взаємоузгодженого національного законодавства, у цифровому середовищі на одне і те саме правопорушення можуть одночасно поширюватися різнорівневі регулятивні масиви, зокрема:

– норми національного законодавства, які визначають юрисдикційні межі та процесуальні механізми відповідальності [107];

– міжнародно-правові стандарти, що формують універсальні гарантії прав людини та забезпечують транснаціональну координацію;

– інструменти soft law, у тому числі рекомендації міжнародних організацій, які хоч і не мають імперативного характеру, проте створюють стандарти належної поведінки у цифровому просторі;

– корпоративні політики онлайн-платформ, що фактично виконують функцію квазіправових норм та визначають правила поведінки для мільйонів користувачів.

8) Транзитивність (перехідність). На відміну від правопорушень у матеріальній сфері, наслідки яких здебільшого обмежуються конкретним об’єктом посягання, у кіберпросторі будь-який делікт набуває потенціалу багаторівневої міграції. Технічна атака на інформаційну систему здатна викликати економічні втрати у вигляді порушення бізнес-процесів, фінансових операцій тощо; водночас вона може трансформуватися у соціальну кризу через поширення паніки серед населення, підрив довіри до

державних інституцій чи дестабілізацію комунікаційної інфраструктури. У крайніх випадках транзитивний ефект правопорушення в мережі Інтернет може призвести до політичної дестабілізації через потенційні можливості впливу на виборчі процеси, національну безпеку та міжнародні відносини [171].

Зазначена характеристика вимагає від теорії права переосмислення проблематики встановлення каузального зв'язку між діянням та його наслідками, адже у цифровому середовищі цей зв'язок набуває багатовимірного і багатосферного характеру. Водночас транзитивність зумовлює потребу у застосуванні механізмів юридичної відповідальності, які враховують як прямі, так і опосередковані наслідки кіберделіктів, що істотно підсилює міждисциплінарний характер дослідження юридичної відповідальності у сфері Інтернет-правопорушень.

9) Автоматизований характер є однією з визначальних ознак правопорушень у цифровому середовищі, що принципово змінює уявлення про механізми вчинення деліктів. Якщо у класичному праворозумінні протиправна поведінка завжди пов'язувалася з усвідомленою та вольовою дією конкретної особи, то у кіберпросторі дедалі частіше маємо справу з ситуаціями, коли деліктна активність здійснюється автоматизованими системами – алгоритмами, ботами, штучними агентами, які функціонують автономно після їх первинного програмування. Юридична специфіка такої поведінки полягає у розмитості суб'єктного складу. Особа, яка створила або запустила алгоритм, може більше не брати безпосередньої участі у кожному акті правопорушення, проте саме цей алгоритм здатен генерувати тисячі або навіть мільйони деліктних дій [126].

Автоматизований характер правопорушень ставить під сумнів традиційні антропоцентричні концепції вини та каузальності, адже діяння може бути результатом не безпосередньої волі людини, а наслідком дії алгоритму, який працює за заздалегідь визначеними або навіть самонавчальними правилами. Вказане потребує розвитку якісно нового

доктринального осмислення «розподіленої відповідальності», де співвідносяться ролі програміста, замовника, користувача та платформи, що надає технологічну інфраструктуру [207].

Концептуальне осмислення цієї ознаки підводить до висновку, що автоматизація у сфері правопорушень є якісно новим викликом для інституту юридичної відповідальності та вимагає перегляду усталених понять суб'єкта правопорушення, меж вини, а також співвідношення між умислом, необережністю і технологічно зумовленим правопорушенням. Безперечно, вказане питання торкається і дискусій про правосуб'єктність штучного інтелекту, які наразі активно ведуться у доктрині права ЄС та США.

10) Високий рівень латентності – одна із ключових ознак правопорушень у мережі Інтернет, яка істотно впливає на можливість їх правової кваліфікації та подальшого притягнення винних до юридичної відповідальності. На відміну від класичних деліктів, що здебільшого залишають матеріальні сліди та очевидні наслідки у фізичному просторі, кіберделікти характеризуються тим, що значна їх частина залишається невиявленою або виявляється через тривалий проміжок часу.

Правова природа латентності у сфері цифрових правопорушень має багатовимірний характер, позаяк:

– зумовлена технологічними особливостями Інтернету, які дозволяють правопорушникам приховувати сліди своєї діяльності;

– посилюється через інформаційну асиметрію між правопорушником та потенційною жертвою, оскільки потерпілі часто навіть не усвідомлюють факту посягання;

– в умовах швидкої глобалізації цифрових процесів традиційні інститути правозастосування виявляються неготовими до оперативного реагування, що створює часовий лаг між вчиненням правопорушення та його процесуальною фіксацією.

Латентність підриває ефективність класичної моделі юридичної відповідальності, яка ґрунтується на своєчасності виявлення та

документування деліктної поведінки. Високий рівень прихованості порушень у кіберпросторі, у свою чергу, нівелює превентивний та виховний потенціал юридичної відповідальності, адже суспільство не отримує належного сигналу про невідворотність санкцій [165]. Досліджувана характеристика правопорушень в мережі Інтернет ставить завдання щодо розробки концепцій проактивного моніторингу, удосконалення механізмів міжнародного обміну інформацією, створення спеціалізованих інституцій кібербезпеки та адаптацію процесуальних норм до специфіки цифрового середовища.

11) Міждисциплінарний характер правопорушень у мережі Інтернет постає однією з найбільш сутнісних їхніх характеристик, що безпосередньо впливає на формування адекватної доктрини юридичної відповідальності. На відміну від класичних деліктів, які можуть бути кваліфіковані переважно крізь призму юридичного аналізу, кіберправопорушення вимагають комплексного осмислення на перетині кількох галузей знань та передбачають встановлення складу правопорушення, його кваліфікацію та визначення санкцій; необхідність глибокого розуміння алгоритмів, програмного забезпечення, технологій шифрування, блокчейну та інших цифрових інструментів, які використовуються як для вчинення, так і для приховування деліктів; пояснення закономірностей масової поведінки у віртуальному просторі, зокрема поширення кібербулінгу, фейкових новин чи деструктивних онлайн-спільнот; виявлення мотиваційних чинників правопорушників і специфіки сприйняття шкоди жертвами у ситуаціях, де фізичний контакт відсутній, але психологічні наслідки є надзвичайно відчутними.

Насамкінець зазначимо, правопорушення у мережі Інтернет постають як самостійний феномен сучасної деліктології, котрий істотно відрізняється від традиційних форм суспільно небезпечної поведінки. Їх онтологія визначається низкою атрибутивних характеристик, котрі ми розглянули вище, зокрема транснаціональністю, анонімністю та псевдоанонімністю

суб’єктів, відсутністю територіальної визначеності, автоматизованим характером, технологічною складністю та високим рівнем латентності. Додаткової уваги заслуговують ознаки масовості впливу, розмитості об’єкта посягання та варіативності правового регулювання, які формують особливий правовий режим їх кваліфікації. Слід також підкреслити, що традиційні галузеві критерії виявляються недостатніми, оскільки не охоплюють міждисциплінарну природу цифрових правопорушень. Загальнотеоретична характеристика правопорушень у мережі Інтернет дозволила дійти висновку, що їх належне правове осмислення є визначальною передумовою для адаптації інституту юридичної відповідальності до викликів XXI століття, забезпечення ефективного захисту прав і свобод особи та утвердження принципу верховенства права у віртуальному вимірі.

Висновки до розділу 2

На підставі аналізу міжнародних стандартів у сфері юридичної відповідальності за правопорушення у мережі Інтернет і проведення їх загальнотеоретичної правової кваліфікації сформульовано висновки.

Встановлено, що сучасна трансформація глобального інформаційного простору зумовила формування багаторівневої системи міжнародних стандартів юридичної відповідальності у цифровому середовищі. Їх основу становлять як універсальні та регіональні договори (Конвенція Ради Європи №108 і Протокол 2018 р., Будапештська конвенція 2001 р. і Додатковий протокол 2003 р., Лансаротська конвенція 2007 р.), так і правові акти ЄС (директиви, регламенти, зокрема Digital Services Act 2022/2065 та AI Act 2024 р.), що визначають сучасну архітектуру цифрового врядування. Констатовано, що вказані акти закріплюють матеріально-правові та

процесуальні підвалини юридичної відповідальності за правопорушення в мережі Інтернет і формують нові моделі її реалізації, серед яких концепція «цифрової приватності», принцип екстратериторіальності у сфері захисту персональних даних, доктрина «відповідальної платформи» та risk-based підхід до регулювання штучного інтелекту.

Визначено, що міжнародна практика передбачає багатоманітність векторів формування цифрових стандартів від обов'язкових міжнародно-правових актів (Африканська конвенція 2014 р., Арабська конвенція 2010 р.) до актів «м'якого права» (рекомендації ОАД, APEC Privacy Framework тощо). Попри відмінності у правовій природі, констатовано тенденцію до гармонізації національних законодавств із положеннями Будапештської конвенції й європейськими стандартами у сфері кібербезпеки та захисту даних. Підкреслено, що значення цих актів виходить за межі суто правового виміру, позаяк вони задають нову парадигму відповідальності у цифрову добу, де належна кореляція між свободою обігу інформації, інноваційним розвитком і гарантіями прав людини виступає системоутворюючим чинником.

Аргументовано, що глобальний процес формування міжнародних стандартів у сфері кібербезпеки не обмежується лише договірними інструментами, а спирається і на доктринальні орієнтири, котрі деталізують застосування базових принципів міжнародного права, що підвищує рівень юридичної визначеності та формує концептуальне підґрунтя для подальшої кодифікації.

Сформулювано низку пропозицій, спрямованих на підвищення ефективності положень Конвенції ООН про кіберзлочинність 2024 року як універсального міжнародно-правового інструменту: 1) у тексті Конвенції варто забезпечити чітке та однозначне визначення складів кіберзлочинів, позаяк наявність нечітких формулювань створює загрозу довільного правозастосування, надмірної криміналізації та може призвести до обмеження законної діяльності, зокрема журналістської, дослідницької чи правозахисної; 2) встановлені Конвенцією процедури збирання та обміну електронними

доказами, а також заходи, що передбачають втручання у приватність, мають здійснюватися виключно на основі принципу пропорційності, котрий передбачає перевірку необхідності, доцільності та співмірності кожного втручання у сферу прав людини; 3) для забезпечення належної підзвітності та запобігання можливим зловживанням необхідним є створення міжнародного органу або спеціальної процедури оцінки дотримання державами стандартів Конвенції; вказаний механізм міг би здійснювати регулярний нагляд, проводити експертні огляди та видавати рекомендації щодо усунення виявлених порушень; 4) Конвенція повинна бути гармонізована з уже чинними міжнародно-правовими інструментами у сфері кіберзлочинності, передусім із Будапештською конвенцією Ради Європи 2001 р., що дозволить уникнути дублювання норм, зменшить ризики колізій та сприятиме формуванню цілісної транснаціональної системи кримінальної юстиції у цифровому середовищі.

Аргументовано, що ефективна протидія кіберзлочинності неможлива без поєднання двох взаємопов'язаних напрямів: гармонізації матеріальних і процесуальних норм міжнародного права та оперативної взаємодії правоохоронних органів. Встановлено, що транскордонний характер Інтернету створює умови, за яких правопорушники комбінують ресурси й інфраструктуру з різних юрисдикцій, що унеможливлює суто національну реакцію на виклики цифрової злочинності. Саме тому діяльність Інтерполу та Європолу має фундаментальне значення для координації держав у глобальному й регіональному масштабах;

Проведений аналіз міжнародних стандартів у сфері юридичної відповідальності за правопорушення у мережі Інтернет дозволяє зробити ряд висновків: 1) міжнародна нормативна база у цій сфері є фрагментованою за географічною та предметною ознакою, проте спостерігається тенденція до її уніфікації; 2) входження до глобальних домовленостей значно ширшого кола держав з різними правовими системами породжує виклик дотримання прав людини; як показав аналіз фінального тексту конвенції ООН, відсутність

жорстких гарантій може бути використана авторитарними режимами для переслідування інакодумців під приводом боротьби з кіберзлочинами; 3) найбільше розвинені стандарти стосуються саме кримінальної відповідальності, що історично обумовлено першочерговим фокусом на кіберзлочинності; натомість міжнародні механізми цивільно-правової та адміністративної відповідальності розвинені значно менше та носять характер радше рекомендацій, ніж обов'язкових норм; встановлено, у перспективі варто очікувати розвитку саме таких «горизонтальних» стандартів, зокрема у сфері відповідальності постачальників цифрових послуг; 4) ефективність міжнародних стандартів корелюється із належною імплементацією на національному рівні; навіть після приєднання до міжнародних договорів окремі держави не забезпечують повної гармонізації внутрішнього законодавства; не всі передбачені Конвенцією про кіберзлочинність діяння отримують належну криміналізацію, а процесуальні механізми щодо збирання та вилучення електронних доказів залишаються фрагментарними; у зв'язку з цим пріоритетного значення набуває системний моніторинг виконання міжнародних зобов'язань та надання технічної допомоги державам у процесі імплементації.

Констатовано, міжнародні стандарти у сфері юридичної відповідальності за правопорушення у мережі Інтернет дедалі більше зміщуються у бік комплексного механізму шляхом поєднання відповідальності з просвітою користувачів, кібергігієною, партнерством з приватним сектором та повагою до відкритості мережі. Нові міжнародні документи та ініціативи створюють передумови для нормативного закріплення та подальшого розвитку зазначених принципів. Сьогодні міжнародні стандарти у сфері юридичної відповідальності за інтернет-правопорушення знаходяться в стадії динамічного розвитку, позаяк від фрагментарних регіональних норм вони еволюціонують до цілісної системи універсальних правил, що враховують як потребу у безпеці, так і необхідність збереження фундаментальних прав і свобод у цифрову епоху.

Визначено ключові характеристики юридичної відповідальності за правопорушення в мережі Інтернет: 1) транснаціональний характер, оскільки переважна більшість правопорушень в мережі Інтернет виходять за межі національних юрисдикцій, що зумовлює складнощі у визначенні компетентного органу та виборі застосовного права; 2) ускладнена ідентифікація суб'єкта, позаяк в умовах анонімності, використання псевдонімів, VPN-технологій, блокчейну та систем шифрування постає об'єктивна проблема встановлення особи правопорушника; 3) комплексний характер складу правопорушення, адже правопорушення в мережі Інтернет поєднують технічні, поведінкові, інтелектуальні та інші елементи, що значно ускладнює правову кваліфікацію; 4) множинність нормативного впливу, яка проявляється у взаємодії норм національного законодавства, міжнародно-правових стандартів, актів м'якого права та корпоративних політик цифрових платформ, що створює багаторівневу модель регулювання.

Наголошено, що юридичну відповідальність за правопорушення у мережі Інтернет доцільно розглядати крізь призму модусу каузальності та контролю у взаємодії «користувач – посередник – алгоритм – платформа», тобто залежно від того, хто генерує деліктний ризик, яким чином він поширюється цифровою інфраструктурою, якою мірою піддається управлінню та як конфігурується суб'єктний склад відповідальності. Запропоноване позиціювання дозволяє поєднати техніко-організаційні параметри цифрового середовища з юридичними ознаками вини, належної обачності та розподілу тягаря доказування.

Репрезентовано класифікацію різновидів юридичної відповідальності за правопорушення в мережі Інтернет:

1) Вторинна (умовна) відповідальність, яка стосується інтернет-провайдерів та адміністраторів онлайн-платформ та не передбачає безумовного обов'язку контролювати весь користувацький контент, однак зобов'язує реагувати на повідомлення про його протиправність від компетентних органів чи зацікавлених осіб;

2) Саморегуляторна відповідальність, що базується на внутрішніх правилах цифрових платформ і онлайн-спільнот, створює своєрідний рівень «квазізаконодавства» у цифровій сфері та забезпечує взаємодію користувачів, але водночас породжує низку проблем, зокрема непрозорість алгоритмів, недостатність механізмів апеляції, вибірковість застосування стандартів та відсутність зовнішнього контролю.

Акцентовано, концепція подвійної легітимації саморегуляторної відповідальності за правопорушення у мережі Інтернет ґрунтується на визнанні ефективності внутрішніх правил платформ лише за умови їх відповідності двом взаємопов'язаним вимірам: 1) внутрішньому (автономному), котрий передбачає, що спільнота користувачів сприймає правила як справедливі, прозорі та недискримінаційні, що забезпечується публічністю стандартів, доступністю процедур оскарження та гарантіями рівності у їх застосуванні; 2) зовнішньому (міжнародно-правовому), відповідно до якого корпоративні політики узгоджуються з міжнародними стандартами у сфері прав людини, зокрема практикою ЄСПЛ та актами ЄС щодо свободи вираження поглядів, захисту персональних даних і протидії мові ворожнечі.

3) Колективна форма юридичної відповідальності у мережі Інтернет розглядається як реакція на складність атрибуції правопорушень, що виникають унаслідок взаємодії користувачів, адміністраторів платформ, розробників алгоритмів, хостинг-провайдерів тощо. У цьому контексті формується доктрина «розподіленої вини», яка передбачає покладення юридичних наслідків на сукупність учасників цифрової екосистеми.

4) Алгоритмічна (автоматизована) відповідальність пов'язана зі зростанням ролі штучного інтелекту та алгоритмів у процесі прийняття рішень. Її сутність полягає в необхідності вироблення особливих механізмів юридичного реагування на делікти, що виникають внаслідок автономних рішень цифрових систем.

5) Множинна (гібридна) відповідальність, під якою варто розуміти комплексну форму правової реакції, яка виникає внаслідок поєднання транскордонної багатоюрисдикційності та взаємодії людського та алгоритмічного факторів у процесі вчинення правопорушення.

Сформульовано ознаки множинної (гібридної) відповідальності за правопорушення у мережі Інтернет: 1) характеризується «подвійною атрибуцією», за якої деліктогенний результат одночасно є наслідком вольових рішень людини та автономних або напівавтономних дій цифрових систем; 2) не зводиться до класичної індивідуалізації суб'єкта, а передбачає розподіл правових наслідків між кількома рівнями, зокрема особою, яка ініціює чи контролює процес, оператором платформи, а також технічною інфраструктурою, що генерує правопорушний ефект; 3) становить новий інститут загальної теорії права, що вимагає: а) формування критеріїв оцінки ступеня алгоритмічної автономії та меж людського контролю; б) перегляду традиційних категорій вини та необережності в умовах алгоритмізованого середовища; в) вироблення механізмів юрисдикційної координації для подолання колізій багатоярусного правозастосування.

Узагальнено усталені у правовій доктрині та міжнародній практиці різновиди правопорушень у мережі Інтернет:

1) за об'єктом посягання: правопорушення у сфері інформаційної безпеки (несанкціонований доступ до даних, злам інформаційних систем, поширення шкідливого програмного забезпечення); порушення персональних немайнових прав (кібербулінг, онлайн-образи, поширення недостовірної інформації, втручання у приватне життя); порушення прав інтелектуальної власності (піратство, нелегальне поширення цифрового контенту, несанкціоноване використання авторських творів); економічні правопорушення у кіберпросторі (шахрайство з використанням електронних платіжних систем, маніпуляції з криптовалютами, створення фінансових пірамід у мережі); порушення регулятивних вимог цифрових платформ

(порушення умов користування сервісами, зловживання алгоритмами, маніпуляція даними користувачів) тощо;

2) за способом здійснення (залежно від методів і технічних засобів): злом або несанкціонований доступ – правопорушення, котрі передбачають злом акаунтів, доступ до закритих інформаційних систем та злом захищених ресурсів; розповсюдження шкідливого програмного забезпечення – поширення вірусів, троянських програм та іншого шкідливого програмного забезпечення з метою завдання шкоди інформаційним системам; соціальна інженерія та фішинг – методи обману, що використовуються для отримання доступу до конфіденційної інформації шляхом маніпулювання довірою користувачів; шахрайські схеми з банківськими картками, інвестиційне шахрайство, а також різні фінансові незаконні операції в Інтернеті;

3) за принципом юрисдикційної належності (територіальною ознакою): національні правопорушення, що вчиняються всередині однієї держави; транскордонні правопорушення, які охоплюють кілька держав;

4) за рівнем суспільної небезпеки: кіберзлочини – тяжкі злочини, які завдають значної шкоди особам, організаціям та суспільству; адміністративні правопорушення у мережі Інтернет, що не несуть серйозної суспільної небезпеки, однак за їх вчинення можуть бути накладені адміністративні санкції.

Констатовано, аналіз правопорушень у кіберпросторі потребує врахування особливостей цифрового середовища, що відмежовують їх від класичних деліктів у межах традиційно усталеного розуміння:

1) Відсутність територіальної визначеності є однією з базових характеристик деліктної поведінки у цифровому середовищі, яка істотно трансформує класичні доктринальні уявлення про юрисдикцію та межі дії правових норм. На відміну від традиційних правопорушень, локалізованих у чітких просторових межах, правопорушення у мережі Інтернет здійснюються у віртуальному просторі, що не має фізичних кордонів. Вказане передбачає, що одна і та сама протиправна дія може водночас зачіпати кілька держав та

створювати феномен багатошарової юрисдикційності, що передбачає: а) юрисдикційну конкуренцію, коли декілька держав претендують на застосування власного права до одного і того ж делікту; б) правову лакунарність, оскільки відсутність єдиних стандартів створює ризик невідповідності національних регулятивних норм; в) фрагментацію правозастосування, котра передбачає, що різні держави кваліфікують одні і ті ж дії по-різному, що перешкоджає уніфікованому реагуванню на глобальні кіберзагрози.

2) Технологічна складність правопорушень у мережі Інтернет визначається тим, що їх вчинення та подальша ідентифікація ґрунтуються на застосуванні спеціальних знань у сфері програмування, криптографії, блокчейн-технологій, штучного інтелекту та інших високотехнологічних рішень.

3) Дистанційність та віртуалізація дій. На відміну від класичних форм протиправної поведінки, що передбачають фізичну присутність правопорушника у місці вчинення шкоди, у цифровому середовищі локалізація діяння втрачає матеріальний вимір. Віртуальний простір створює умови, за яких суб’єкт може завдати шкоди об’єктам правового захисту, перебуваючи на значній відстані, у тому числі в іншій юрисдикції, без необхідності фізичного контакту.

4) Анонімність та псевдоанонімність суб’єкта істотно впливає як на процес ідентифікації правопорушника, так і на забезпечення невідворотності юридичної відповідальності.

Визначено, анонімність у кіберпросторі має подвійний характер, позаяк забезпечує реалізацію права на приватність та свободу вираження поглядів і переконань, але одночасно створює правові прогалини, які активно використовуються правопорушниками для уникнення контролю та правозастосовних заходів.

Акцентовано, псевдоанонімність як проміжна форма маскування особи сприяє появі правової невизначеності щодо суб’єкта притягнення до

юридичної відповідальності та має три ключові вектори: а) епістемологічний, позаяк ускладнює встановлення фактичних обставин і перешкоджає формуванню доказової бази; б) процесуальний, так як обмежує застосування класичних процедур переслідування, оскільки неможливо ідентифікувати конкретного носія деліктної поведінки; в) правоохоронний, що стимулює зростання кількості кіберделіктів через відчуття безкарності та мінімальні ризики для суб'єкта правопорушення.

5) Масовість та колективний характер впливу правопорушень у мережі Інтернет зумовлює трансформацію об'єкта посягання, позаяк шкода завдається не тільки окремій особі, але і також цілісним соціальним групам чи навіть інституціям, що підсилює суспільну небезпеку кіберделіктів.

6) Розмитість об'єкта правопорушення у цифровому середовищі передбачає, що у сфері кіберпростору об'єктом посягання виступають переважно нематеріальні категорії – інформаційні ресурси, цифрова репутація, персональні дані, інтелектуальна власність. Вказана трансформація об'єкта правопорушення передбачає відсутність матеріальної субстанційності, котра ускладнює юридичну ідентифікацію шкоди, адже порушення нематеріальних прав не завжди можна виміряти у класичних економічних показниках.

7) Варіативність правового регулювання у сфері Інтернет-правопорушень передбачає, що у цифровому середовищі на одне і те саме правопорушення можуть одночасно поширюватися різнорівневі регулятивні масиви, зокрема: а) норми національного законодавства, які визначають юрисдикційні межі та процесуальні механізми відповідальності; б) міжнародно-правові стандарти, що формують універсальні гарантії прав людини та забезпечують транснаціональну координацію; в) інструменти soft law, у тому числі рекомендації міжнародних організацій, які хоч і не мають імперативного характеру, проте створюють стандарти належної поведінки у цифровому просторі; г) корпоративні політики онлайн-платформ, що

фактично виконують функцію квазіправових норм та визначають правила поведінки для мільйонів користувачів.

8) Транзитивність (перехідність). На відміну від правопорушень у матеріальній сфері, наслідки яких здебільшого обмежуються конкретним об'єктом посягання, у кіберпросторі будь-який делікт набуває потенціалу багаторівневої міграції. У крайніх випадках транзитивний ефект правопорушення в мережі Інтернет може призвести до політичної дестабілізації через потенційні можливості впливу на виборчі процеси, національну безпеку та міжнародні відносини.

9) Автоматизований характер. У кіберпросторі дедалі частіше маємо справу з ситуаціями, коли деліктна активність здійснюється автоматизованими системами – алгоритмами, ботами, штучними агентами, які функціонують автономно після їх первинного програмування. Юридична специфіка такої поведінки полягає в розмитості суб'єктного складу. Особа, яка створила або запустила алгоритм, може більше не брати безпосередньої участі у кожному акті правопорушення, проте саме цей алгоритм здатен генерувати тисячі або навіть мільйони деліктних дій. Наголошено, вказане потребує розвитку якісно нового доктринального осмислення «розподіленої відповідальності», де співвідносяться ролі програміста, замовника, користувача та платформи, що надає технологічну інфраструктуру.

10) Високий рівень латентності, правова природа якої у сфері цифрових правопорушень має багатовимірний характер, позаяк: а) зумовлена технологічними особливостями Інтернету, які дозволяють правопорушникам приховувати сліди своєї діяльності; б) посилюється через інформаційну асиметрію між правопорушником та потенційною жертвою, оскільки потерпілі часто навіть не усвідомлюють факту посягання; в) в умовах стрімкої глобалізації цифрових процесів традиційні інститути правозастосування часто виявляються неготовими до оперативного реагування, що зумовлює виникнення часового лагу між вчиненням правопорушення та його процесуальною фіксацією.

11) Міждисциплінарний характер правопорушень у мережі Інтернет передбачає, що останні вимагають комплексного осмислення на перетині кількох галузей знань і передбачають: встановлення складу правопорушення, його кваліфікацію та визначення санкцій; необхідність глибокого розуміння алгоритмів, програмного забезпечення, технологій шифрування, блокчейну та інших цифрових інструментів, які використовуються як для вчинення, так і для приховування деліктів; пояснення закономірностей масової поведінки у віртуальному просторі, зокрема поширення кібербулінгу, фейкових новин чи деструктивних онлайн-спільнот; виявлення мотиваційних чинників правопорушників та специфіки сприйняття шкоди жертвами у ситуаціях, де фізичний контакт відсутній, але психологічні наслідки є надзвичайно відчутними.

Резюмовано, загальнотеоретична характеристика правопорушень у мережі Інтернет дозволила дійти висновку, що їх належне правове осмислення є визначальною передумовою для адаптації інституту юридичної відповідальності до викликів XXI століття, забезпечення ефективного захисту прав і свобод особи та утвердження принципу верховенства права у віртуальному вимірі.

РОЗДІЛ 3
ПЕРСПЕКТИВИ МОДЕРНІЗАЦІЇ ІНСТИТУТУ ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ В УМОВАХ ЦИФРОВІЗАЦІЇ

3.1. Проблемні аспекти реалізації юридичної відповідальності за інтернет-правопорушення

Стрімка цифровізація усіх сфер життя ставить нові виклики перед класичними правовими інститутами, зокрема інститутом юридичної відповідальності. Закони багатьох держав досі спираються на архаїчні норми, котрі розроблялися без врахування цифрової реальності, що породжує правову невизначеність щодо поведінки та правопорушень у кіберпросторі. Відсутність належного регулювання призводить до того, що приватні корпорації самостійно встановлюють правила та відповідальність у цифрових платформах [53]. Відтак постає необхідність переосмислення й розвитку інституту юридичної відповідальності з урахуванням сучасних цифрових технологій.

Цифрові технології докорінно змінюють характер правопорушень і способи їх вчинення, розмивають межі юрисдикцій та створюють нові об’єкти і суб’єкти правовідносин. Цифрова епоха висуває вимогу адаптації традиційного інституту відповідальності, позаяк необхідно уточнювати правові поняття, розробляти нові норми та механізми, щоб жодне правопорушення не лишалося поза увагою правосуддя через технологічні особливості. Важливо підкреслити, що сам по собі розвиток цифрових технологій не «покращує» інститут відповідальності автоматично, навпаки, він виявляє його прогалини. Проте реагування на вказані виклики спонукає законодавця до оновлення правових рамок, що зрештою може удосконалити інститут юридичної відповідальності.

Розвиток викликів для інституту юридичної відповідальності закономірно пов’язаний із технологіями, які докорінно змінюють саму архітектоніку правового регулювання. Серед них особливе місце посідає блокчейн як децентралізована система фіксації та зберігання даних, що забезпечує прозорість, незмінність і автономність транзакцій [49, с. 67]. Його поява започаткувала нові правові феномени, зокрема криптовалюти, смарт-контракти, децентралізовані автономні організації, котрі виходять за межі класичних категорій права та ставлять питання про перерозподіл акцентів у визначенні суб’єктів і меж відповідальності. У таких умовах правопорушення можуть вчинятися без прямого волевиявлення конкретної особи, лише внаслідок роботи алгоритму, тоді як учасники системи залишаються анонімними та територіально розпорошеними [41].

Технологія блокчейн і похідні від неї феномени формують нові напрямки еволюції права, насамперед у площині юридичної відповідальності. Специфіка полягає у тому, що значна частина дій у цьому середовищі здійснюється автоматично шляхом виконання коду. Блокчейн утверджує принципово іншу модель довіри, не до інституцій чи держави, а до математичного алгоритму, однак у випадках його збою чи використання для протиправних цілей виникає необхідність забезпечення постраждалим ефективних механізмів правового захисту та відновлення порушених прав [87, с. 33–34].

Смарт-контракти, що становлять собою алгоритмічні програми, здатні автоматично виконувати умови угоди без додаткового волевиявлення сторін, у сучасному праві набувають дедалі більшої актуальності як специфічний об’єкт доктринального осмислення. Їх функціонування спрямоване на мінімізацію ризику невиконання зобов’язань контрагентом шляхом закладення в код чітких правил поведінки, проте водночас вони породжують складні питання щодо меж і суб’єктів юридичної відповідальності. Особливо зазначене стосується ситуацій, коли результат виконання смарт-контракту не

відповідає очікуванням сторін через помилки у програмному коді, вразливості системи чи непередбачувані зовнішні обставини [13, с. 58–62].

Анонімність та глобальна розподіленість учасників блокчейн-мереж істотно ускладнюють застосування традиційних механізмів юридичної відповідальності. За відсутності можливості ідентифікації особи виникає проблема атрибуції протиправних дій, що унеможливлює ефективне переслідування правопорушників у межах національних юрисдикцій. Вказане свідчить про дефіцит класичного позиціювання суб'єктності у цифровому середовищі та актуалізує потребу міжнародної координації у сфері правового регулювання блокчейн-технологій.

Ще складнішу ситуацію породжують децентралізовані автономні організації (далі – DAO), які функціонують без централізованого керівного органу та ухвалюють рішення колективно або автоматично, на основі алгоритму. У такій системі практично відсутній єдиний суб'єкт, на якого можна покласти відповідальність за правопорушення, що ставить під сумнів застосовність традиційної моделі юридичної відповідальності. Зазначене змушує правову доктрину шукати нові концепції – від ідеї колективної або розподіленої відповідальності до розгляду DAO як суб'єкта права, який потребує спеціального нормативного оформлення [196].

Слід наголосити, що у правовому полі Європейського Союзу питання регулювання блокчейн-технологій поступово виходить за межі криптоактивів та охоплює смарт-контракти як інструмент автоматизації зобов'язань. Поряд із Регламентом MiCA, спрямованим на створення єдиної нормативної основи для ринків криптоактивів, у науково-правових дискусіях зростає увага до проблеми юридичної відповідальності у випадках збоїв або протиправного використання смарт-контрактів. Однією з пропонованих ініціатив є запровадження обов'язку для розробників передбачати можливість зовнішнього аудиту коду та механізму призупинення його дії (так званий «kill switch»), що дозволяло б припиняти виконання алгоритму у разі виявлення критичних помилок чи зловживань [227, с. 87–97].

З одного боку, зазначене створює передумови для формування доктрини відповідальності у сфері автоматизованих правочинів, оскільки усуває ключову проблему, котра полягає в неможливості корекції наслідків дії алгоритму без згоди бенефіціара. З іншого боку, подібні пропозиції викликають критику серед прихильників концепції «code is law», для яких будь-яке зовнішнє втручання підриває засади децентралізації та довіри до блокчейну. Проте з позицій правової науки та міжнародної практики очевидним є те, що абсолютна автономність алгоритмів не може співіснувати з принципами верховенства права, захисту прав людини та потребами боротьби з кіберзлочинністю.

Дискусія щодо допустимих меж автономності алгоритмів у сфері блокчейну та смарт-контрактів демонструє необхідність розробки спеціальних механізмів юридичної відповідальності у випадках, коли дії штучно створених програмних систем призводять до суспільно небезпечних наслідків. Водночас навіть за умов технологічної децентралізації абсолютне виключення державного контролю є неможливим, оскільки принципи верховенства права та захисту основоположних прав людини вимагають відповідних правових інструментів реагування. У цьому контексті національне законодавство стає практичним полем імплементації зазначених ідей.

В Україні нормативна база у сфері протидії правопорушенням, пов’язаним з інформаційними технологіями, закріплена у Кримінальному кодексі. Зокрема, стаття 361 визначає відповідальність за несанкціоноване втручання у функціонування комп’ютерів, автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку. Застосування передбачених санкцій залежить від ступеня тяжкості діяння і може передбачати штрафні санкції, обмеження чи позбавлення волі [40, с. 131]. Поряд із цим, у випадках шахрайських дій, що здійснюються через Інтернет, можуть застосовуватися загальні положення кримінального права, зокрема норми, що передбачають відповідальність за шахрайство та крадіжку. З огляду на це, українська

правова система розвиває модель, у межах якої кіберзлочини розглядаються не як повністю ізольована категорія, а як специфічна форма традиційних правопорушень, що вимагає врахування особливостей цифрового простору при визначенні підстав та меж юридичної відповідальності.

У контексті аналізу механізмів протидії правопорушенням у сфері комп'ютерної безпеки постає необхідність розширення дослідження і на інші напрями регулювання цифрових відносин, адже правова відповідальність у мережі Інтернет не вичерпується лише кримінально-правовим реагуванням на кіберзлочини. Особливого значення у цьому вимірі набуває гарантування належного рівня охорони персональних даних, що є невід'ємною складовою інформаційної безпеки та дотримання прав людини у цифровому середовищі.

Так, у добу інформаційного суспільства обсяг даних, що обробляються державними органами, приватними компаніями та цифровими платформами, набув безпрецедентних масштабів, що зумовлює підвищені ризики неправомірного доступу, використання чи розповсюдження персональної інформації, а відтак потребує створення ефективних правових механізмів захисту.

В Україні інституційним фундаментом у цій сфері є Закон «Про захист персональних даних», який закріплює базові принципи обробки та зберігання інформації про фізичних осіб, визначає права суб'єктів персональних даних і обов'язки володільців та розпорядників. Нормативне регулювання у цьому ключі спрямоване на забезпечення прозорості та правомірності обробки, обмеження доступу до даних, їх точність та актуальність, а також на гарантування можливості особи контролювати використання власної інформації [58, с. 481]. Законодавець передбачає серед іншого також комплекс заходів юридичної відповідальності за порушення цих вимог, від адміністративних стягнень до кримінально-правових санкцій, залежно від характеру та тяжкості правопорушення.

Зазначений нормативно-правовий акт спрямований на реалізацію конституційного права на невтручання в особисте і сімейне життя, але поряд

із цим формує превентивні механізми протидії зловживанням у сфері цифрових технологій. В умовах розвитку електронного урядування, поширення електронної комерції та соціальних мереж значення цього закону суттєво зростає, адже він покликаний врегулювати у досліджуваній сфері інтереси держави, бізнесу та громадян.

Водночас практика його застосування виявляє низку проблем, зокрема нечіткість окремих термінів, а також обмеженість інституційних ресурсів для здійснення ефективного нагляду за дотриманням установлених вимог. У науковій літературі підкреслюється, що розвиток інформаційних технологій зумовлює необхідність оновлення правових рамок у напрямі підвищення рівня відповідальності за зловживання персональними даними та створення дієвих інструментів відновлення порушених прав суб'єктів [9, с. 57–62].

Не є новиною той факт, що одним з найскладніших питань є відповідальність за рішення та дії, що приймаються штучним інтелектом (далі – ШІ) та автоматизованими системами. У класичному праві суб'єктами відповідальності є ті, хто має правосуб'єктність, поряд із цим сучасна правова доктрина і законодавство одностайні в тому, що ШІ не визнається самостійним суб'єктом права [102]. Отже, навіть якщо високорозвинена система штучного інтелекту діє автономно і завдає шкоди, її не можна прямо притягнути до юридичної відповідальності. Якщо системи ШІ не мають правосуб'єктності і діють автономно, вони не несуть самостійну юридичну відповідальність за результати своїх дій [21, с. 118].

Так, традиційно право виходило з аксіоми, що суб'єктом юридичної відповідальності може бути лише фізична або юридична особа, яка діє свідомо та володіє волею. Натомість сучасні системи штучного інтелекту здатні ухвалювати рішення автономно, без безпосереднього людського контролю, що істотно ускладнює застосування класичних підходів до визначення відповідальності. Вже сьогодні стаються інциденти, де важко визначити, хто ж повинен нести юридичну відповідальність, розробник програми, користувач чи сама система. Переважає думка, що штучні агенти

не можуть бути самостійними носіями юридичної відповідальності, адже вони не мають ні свідомості, ні наміру. Як зазначають дослідники І. Айрес та Дж. Балкін, правова відповідальність AI-агентів покладається на людських осіб, що виступають у ролі принципалів, адже AI-агенти позбавлені власних намірів, тож право повинно покладати обов'язок дотримуватися стандартів належної обачності на тих людей і компанії, які впроваджують та використовують ці технології [121].

Натомість відповідальність за наслідки застосування ШІ покладається на конкретних учасників, причетних до створення або експлуатації цих систем. Зокрема, можливими носіями відповідальності є:

а) розробники ШІ, якщо помилка чи шкода спричинені недоліками алгоритму, неправильним навчанням моделі або неналежним тестуванням програмного забезпечення; саме розробник, який заклав алгоритм, може відповідати у разі, коли програма діє хибно через конструктивні прорахунки.

б) виробники обладнання, якщо збій або аварія пов'язані із несправністю технічних компонентів системи; у такому випадку відповідальність настає за правилами про дефектну продукцію;

в) власники чи користувачі ШІ-систем, якщо вони застосували систему неналежним чином, неправильно налаштували або порушили інструкції, що призвело до шкоди;

г) компанії, що впроваджують ШІ, якщо організація впровадила ШІ у свої процеси і не забезпечила належного нагляду чи контролю за його рішеннями; за таких умов підприємство може відповідати перед споживачами або третіми особами за шкоду, заподіяну функціонуванням ШІ на виробництві чи у послугах [102].

Наведений вище розподіл відповідальності вже простежується на практиці. Прикладом є судові справи щодо аварій за участю автомобілів Tesla з увімкненим автопілотом. Розслідування цих інцидентів виявило, що водії часто занадто покладалися на автономне керування та не втручалися вчасно для запобігання аварії, що вказує на їхню частку провини. Водночас

встановлено і відповідальність виробника, оскільки якщо доведено технічні недоліки системи автопілоту, компанія Tesla несе відповідальність за дефект, адже саме вона ввела технологію в обіг. Відтак підхід до відповідальності в еру ШІ є комплексним, позаяк розглядаються дії або бездіяльність людини на кожному етапі «життєвого циклу» ШІ – від розробки до експлуатації.

У зв'язку з цим у доктрині набуває поширення концепція розподіленої (похідної) відповідальності, відповідно до якої деліктні наслідки дій «розумних» машин юридично імпутуються їхнім розробникам, власникам чи операторам. Вказаний напрям є новітнім етапом еволюції інституту відповідальності, який вимагає адаптації існуючих правових норм і принципів. Наразі на міжнародному рівні тривають дискусії щодо доцільності запровадження окремого правового статусу для ШІ у вигляді так званої «електронної особи», що теоретично могло б передбачати і окремий режим відповідальності. Втім більшість науковців і практиків ставляться до такої ідеї вкрай обережно, оскільки її реалізація кардинально змінює усталені уявлення про юридичну суб'єктність і вину. Натомість у доктрині та правотворчій практиці пропонується зосередитися на вдосконаленні законодавства щодо відповідальності фізичних і юридичних осіб за рішення, прийняті із застосуванням штучного інтелекту, а також на запровадженні механізмів обов'язкового страхування відповідальності у сфері високоризикових AI-технологій [121].

Запропонована концепція має важливе значення для розвитку правової доктрини, оскільки пропонує якісно нову модель регулювання діяльності систем штучного інтелекту, що ґрунтується не на традиційній категорії наміру, а на оцінці ризику. Зазначена парадигмальна зміна дозволяє адекватно враховувати специфіку функціонування технологій, які не володіють свідомістю чи інтенціями, але здатні генерувати суттєві соціально-правові наслідки.

У сучасному науковому дискурсі простежується позиціювання концепції розподіленої відповідальності як такої, котра сприяє:

1) розвитку спеціальних режимів відповідальності, подібних до інституту відповідальності за шкоду, завдану дефектними товарами, або режимів суворої (безвинної) відповідальності, що дозволяє мінімізувати прогалини у правозастосуванні у випадках, коли встановлення вини є неможливим чи недоцільним;

2) нормативного закріплення нових стандартів у європейських та національних правових актах, присвячених регулюванню штучного інтелекту, які повинні визначати межі допустимого ризику та стандарти належної поведінки розробників, операторів і користувачів таких систем;

3) перегляду класичних категорій юридичної науки, тобто вини, відповідальності, делікту тощо, з урахуванням нових технологічних реалій, що потребує уточнення їхнього змісту та співвідношення з категоріями об'єктивної обачності, передбачуваності наслідків і розподілу ризиків у цифровому середовищі.

Слід підкреслити, що зарубіжні експерти припускають, що в майбутньому надрозумні системи можуть отримати статус окремих юридичних осіб. Європейський Союз свого часу навіть розглядав ідею запровадження для роботів особливого статусу «електронної особи», яка б мала певні права та відповідальність, проте наразі переважає думка, що це передчасно і недоцільно [21, с. 124].

Як підкреслюють дослідники, сьогодні кращим рішенням є використання існуючих правових конструкцій, тобто слід покладати відповідальність за шкоду, завдану ШІ, на реальних суб'єктів, зокрема користувачів, власників або виробників, а не на штучні системи. Законодавець повинен пробивати вуаль технології та дістатись до реальної особи за нею, що аналогічно доктрині «підняття корпоративної вуалі» у корпоративному праві, коли суди ігнорують фіктивну оболонку (компанію) і притягують до відповідальності реальних винуватців. У випадку ШІ вказане передбачає, що навіть якщо система діє автономно, шукати слід

відповідальних серед людей чи організацій, що стоять за її створенням, впровадженням чи використанням.

Слід зауважити, що на сучасному етапі міжнародного правового розвитку спостерігається поступова інституціоналізація механізмів юридичної відповідальності у сфері застосування штучного інтелекту, спрямована на забезпечення рівності процесуальних можливостей та належного захисту прав людини. Європейський Союз поєднує спеціальне регулювання функціонування ШІ-систем із оновленням традиційних цивільно-правових механізмів відшкодування шкоди. Зокрема, у 2024 році було прийнято Європейський акт про штучний інтелект, який уперше встановив системний режим регулювання алгоритмічних технологій на рівні ЄС [82].

Відповідно до положень цього акта, для високоризикових ШІ-систем запроваджуються жорсткі стандарти, серед яких обов'язок забезпечення прозорості, ведення журналів протоколювання прийнятих рішень, надання користувачам повної та достовірної інформації про алгоритмічне функціонування, а також відповідність вимогам кібербезпеки. Водночас передбачено пряму заборону застосування систем, що створюють «неприйнятний ризик» для прав і свобод людини, зокрема практики тотального соціального рейтингування громадян. Порушення цих норм тягне за собою застосування багатомільйонних штрафів, що істотно підвищує рівень відповідальності як розробників, так і провайдерів технологій [103; 119].

Україна, як і більшість держав, наразі не має спеціального закону про ШІ. Регулювання здійснюється через застосування загальних норм різних галузей права, зокрема положення про захист прав споживачів, норми цивільного права про відшкодування шкоди, а також кримінально-правові норми. Вітчизняна правова доктрина, втім, активно досліджує питання ШІ, проводяться дискусії щодо можливої правосуб'єктності ШІ в теорії, але переважає думка про недоцільність цього в найближчій перспективі.

Натомість науковці та практики обґрунтовують необхідність внесення точкових змін до чинного законодавства України, щоб чітко окреслити юридичну відповідальність у сфері ШІ. Зокрема, пропонується врегулювати на законодавчому рівні обов'язки розробників щодо безпеки алгоритмів, встановити вимоги до прозорості автоматизованих рішень в чутливих сферах, серед яких медицина, фінанси, правосуддя, а також передбачити механізми контролю за використанням ШІ у державному секторі, до прикладу, при ухваленні адміністративних рішень [21, с. 118].

Україна приєдналась у 2023 році до Рамкової конвенції Ради Європи про штучний інтелект, права людини, демократію і верховенство права [64], що підтверджує намір держави забезпечити розвиток ШІ з додержанням прав і свобод та стати частиною загальноєвропейського правового простору в цій галузі. Відтак у сфері ШІ перспективи розвитку інституту юридичної відповідальності полягають у нормативному закріпленні принципу, відповідно до якого штучний інтелект є інструментом, а юридичну відповідальність несе людина. Вказане передбачає вдосконалення законів для чіткого визначення кола відповідальних осіб та умов їх відповідальності за шкоду від ШІ, впровадження обов'язкових стандартів розробки та використання алгоритмів, а також створення процедур розслідування інцидентів, пов'язаних з ШІ тощо.

У межах нашого дослідження варто звернути увагу також на проблематику метавсесвітів та розширеної віртуальної реальності, котрі створюють паралельний цифровий простір, в якому люди можуть взаємодіяти, укладати угоди, створювати та обмінювати цифрові об'єкти. Вказаний феномен кидає виклик традиційним уявленням про територіальну юрисдикцію та матеріальні об'єкти права. Одне з перших питань, котре потребує врегулювання, стосується визначення застосовного права і «відповідального» суду. Адже користувачі метавсесвіту можуть перебувати в різних державах, сервери – в інших, а правочини відбуватися цілодобово у віртуальному просторі. На практиці вже траплялися випадки, коли

правопорушення, вчинені в цифровому просторі, ставали предметом судових процесів у реальній юрисдикції, проте за відсутності прямих норм доводиться екстраполювати існуюче право на нові ситуації, що не завжди однозначно [10, с. 499–506].

Ще одним питанням у досліджуваній сфері є правова кваліфікація віртуальних об'єктів. У метавсесвіті існують цифрові активи, наприклад, об'єкти віртуальної нерухомості, предмети для аватарів, NFT-токени тощо, які мають цінність для користувачів. Для України логічно було б визначити право віртуальної власності як специфічний різновид права власності, об'єктом якого є нематеріальне віртуальне майно. Зазначена новела дозволила б поширити на метавсесвіт традиційні механізми захисту власності, а винна особа могла б притягатися до цивільно-правової або кримінальної відповідальності за крадіжку чи знищення віртуального майна так само, як і реального.

У сучасному правовому дискурсі дедалі більшої актуальності набуває проблема правопорушень у віртуальних світах і метавсесвітах, що породжують нетипові форми деліктної поведінки. Одним із таких феноменів є так званий «електронний кіднепінг», тобто несанкціоноване використання аватара чи цифрового двійника особи, яке за своєю суттю наближається до крадіжки ідентичності або шахрайства, але реалізується виключно у цифровому середовищі [211, с. 1542–1548]. Хоча фізичного впливу у таких випадках немає, шкода потерпілим набуває реального психологічного характеру, що ставить питання про криміналізацію подібних діянь, або через адаптацію існуючих складів, або шляхом створення нових норм, спеціально зорієнтованих на віртуальний простір [210, с. 89–97].

Слід підкреслити, що через наявні прогалини у національному та міжнародному законодавстві ключова частина регулятивного навантаження щодо функціонування віртуальних платформ і метавсесвітів поки що фактично покладена на їхніх приватних провайдерів. Відсутність універсальних правових норм обумовлює появу фрагментарних «локальних»

регуляторних режимів, що реалізуються у вигляді правил користування, корпоративних політик та стандартів спільнот, які запроваджують відповідні компанії. Саме у цих документах закріплюються положення, що визначають межі дозволеної поведінки користувачів, санкції за порушення та процедури оскарження [212, с. 128–132].

У науковій літературі слушно наголошується, що така ситуація не може розглядатися як усталена модель регулювання. Приватні правила мають обмежену дію, позаяк поширюються виключно в межах конкретної платформи і спрямовані передусім на захист комерційних інтересів провайдера, а не на забезпечення загальносуспільних цінностей, серед яких захист прав людини, забезпечення публічної безпеки чи відновлення справедливості. Вказане, своєю чергою, зумовлює ризики фрагментації правового поля, відсутності єдиних стандартів відповідальності та порушення принципу правової визначеності [211, с. 1542–1548].

У такому контексті дедалі очевиднішою постає перспектива державного втручання та формування нормативної основи для функціонування метавсесвітів. Зокрема, доцільним вбачається необхідність встановлення мінімальних стандартів відповідальності за правопорушення у віртуальному середовищі та закріплення базових принципів його функціонування, прозорості, підзвітності, захисту даних, дотримання прав і свобод користувачів. Очевидно, що державна нормотворчість повинна випереджати масове поширення технологій, оскільки відставання у правовому регулюванні створює правовий вакуум, який експлуатується недобросовісними суб’єктами та підриває довіру до цифрових середовищ [223, с. 94–104].

Слід акцентувати, що Україна поступово формує національну нормативну базу, спрямовану на правове визнання та регламентацію цифрових активів. Важливим кроком у цьому напрямі стало ухвалення у 2022 році Закону України «Про віртуальні активи», який має на меті встановити

комплексні правила обігу криптовалют та інших цифрових об’єктів [57, с. 151].

Так, Закон України «Про віртуальні активи» (№ 2074-IX від 2022 р.) становить знаковий етап розвитку національного правового поля у сфері цифрової економіки та є спробою створити системний фундамент для врегулювання відносин, що виникають у зв’язку з обігом криптовалют, токенів та інших віртуальних форм вартості. Його прийняття передбачає відхід від практики фактичного правового вакууму, у якому цифрові активи існували як економічна реальність, але не мали нормативного закріплення, і водночас знаменує формування нової парадигми регуляції, зорієнтованої на відповідність міжнародним стандартам.

Важливим є те, що закон вперше в українському праві вводить категорію «віртуальний актив» як об’єкт цивільного обороту та фактично визнає його носієм економічної цінності і потенційним джерелом прав та обов’язків. Тим самим досліджуваний нормативно-правовий акт руйнує традиційний зв’язок майнових прав із матеріальними носіями та відкриває простір для юридичного оформлення цифрових феноменів. Особливе значення має визначення статусу суб’єктів, що надають послуги у сфері віртуальних активів, і закріплення для них комплексу обов’язків, пов’язаних із прозорістю діяльності, запобіганням легалізації доходів, забезпеченням кібербезпеки та захистом прав користувачів. У такий спосіб формується нова модель юридичної відповідальності, що поєднує приватноправові та публічно-правові елементи.

Разом із тим концепція закону не позбавлена недоліків. Насамперед варто звернути увагу на те, що його норми не набули чинності у зв’язку з відсутністю змін до Податкового кодексу, а статус окремих категорій цифрових активів, зокрема NFT, залишився невизначеним. У сучасній правовій доктрині NFT розглядаються як новий феномен цифрової економіки, виникнення якого стало логічним наслідком розвитку блокчейн-технологій та потреби у створенні унікальних цифрових маркерів, здатних

посвідчувати права на конкретні об’єкти у віртуальному та фізичному світі. На відміну від взаємозамінних токенів, тобто криптовалют, які виконують передусім платіжну функцію, NFT наділені невзаємозамінністю, що надає їм рис «цифрового титулу» власності [214].

Правова природа NFT залишається дискусійною. З одного боку, вони можуть кваліфікуватися як нематеріальні активи, що відображають право власності на цифровий об’єкт. Поряд із цим, NFT слід розглядати як правовий титул sui generis, адже сам по собі токен не є контентом, тобто зображенням, музикою, відео тощо, а тільки цифровим сертифікатом, який засвідчує унікальність та походження відповідного об’єкта. Вказане породжує складність у відмежуванні права на NFT від авторських та суміжних прав на сам об’єкт, до якого він прив’язаний. У більшості випадків придбання NFT не передбачає автоматичного переходу інтелектуальної власності, а закріплює право володіння самим токеном [186].

З позицій цивільного права NFT можна віднести до об’єктів цивільних прав, що мають економічну вартість і перебувають у цивільному обороті. Водночас їхній статус вимагає адаптації існуючих правових категорій, оскільки традиційні форми не повною мірою охоплюють специфіку невзаємозамінних токенів. Доктринально виправданим виглядає концепція, за якою NFT виступає новою категорією цифрових активів, що поєднує риси майнового права у вигляді права володіння та розпорядження, а також права інтелектуальної власності на унікальний цифровий ідентифікатор [155].

Вказане свідчить про те, що чинний закон виконує передусім рамкову, концептуально-програмну функцію, позаяк визначає загальні орієнтири для правового регулювання обігу віртуальних активів. Передусім слід підкреслити, що у правовому полі залишається низка сутнісних прогалин. Насамперед ідеться про відсутність чітко врегульованих механізмів відповідальності за зловживання віртуальними активами, що створює потенційні ризики для появи шахрайських схем та підриву довіри до ринку. Ще однією проблемною площиною є захист прав інвесторів та власників

токенів, адже законодавець поки не розробив ефективних процедур компенсації збитків чи запобігання неправомірним діям посередників і провайдерів цифрових послуг. Не менш складним є завдання збалансування приватних і публічних інтересів у сфері цифрового обігу, оскільки держава зацікавлена у стимулюванні розвитку інновацій та інвестицій, однак, зобов'язана гарантувати прозорість, захист прав споживачів та фінансову стабільність.

Разом з тим, у Верховній Раді України зареєстровано низку законопроєктів, спрямованих на уточнення та деталізацію базових категорій у сфері цифрових активів. Йдеться, зокрема, про пропозиції щодо закріплення правового режиму віртуальних предметів, забезпечення охорони прав інтелектуальної власності на цифровий контент, а також нормативне врегулювання відносин щодо володіння, користування і розпорядження віртуальними активами як між фізичними, так і між юридичними особами.

Варто наголосити, що на наднаціональному рівні Європейський Союз уже сформував цілісну модель правового регулювання крипторинку через прийняття Регламенту MiCA (підрозділ 2.1. дисертаційного дослідження), що встановлює єдині стандарти правового режиму криптоактивів для держав-членів ЄС. У контексті євроінтеграційного курсу Україна має високі шанси на поступову гармонізацію національного законодавства з положеннями MiCA та іншими актами ЄС, що забезпечить синхронізацію правового регулювання, підвищить прозорість ринку цифрових активів та сприятиме утвердженню єдиних стандартів юридичної відповідальності у досліджуваній сфері.

Важливим проблемним аспектом реалізації юридичної відповідальності за інтернет-правопорушення є низький рівень цифрової правової культури користувачів. У більшості випадків особи не усвідомлюють правових наслідків власної поведінки в мережі та помилково вважають Інтернет «позаправовим» простором. Недостатнє знання положень законодавства щодо захисту персональних даних, авторського права, етики

спілкування в соціальних мережах та відповідальності за поширення неправдивої інформації зумовлює високий рівень латентності правопорушень.

Окремою проблемою є поширене ігнорування правил безпечного користування інформаційними ресурсами, що проявляється у легковажному ставленні до захисту паролів, використанні неліцензійного програмного забезпечення, поширенні сумнівного контенту. Наведена поведінка сприяє зростанню кількості правопорушень, ускладнює діяльність правоохоронних органів та створює підґрунтя для масових порушень прав інших користувачів.

Формування цифрової правової культури є комплексним завданням, яке неможливо звести виключно до вдосконалення правового регулювання. Зазначене потребує системних та послідовних заходів у сфері правопросвітництва, що передбачають як інституційну, так і неформальну освіту. Важливим напрямом у цьому ключі виступає здобуття знань про правила користування інформаційними технологіями та правові наслідки їх порушення у рамках навчальних програм різних рівнів освіти, від шкільної до вищої. Не менш значущим є розвиток культури відповідального споживання та поширення цифрового контенту, що передбачає формування у громадян критичного мислення, навичок медіаграмотності та усвідомлення обов’язків у цифровому середовищі.

Разом із тим навіть належним чином деталізовані та уніфіковані законодавчі механізми не можуть забезпечити повноцінну реалізацію юридичної відповідальності у сфері Інтернету без сформованого рівня правової свідомості громадян. Лише синергія між нормативно-правовим регулюванням та підвищенням цифрової правової культури користувачів створює умови для належного функціонування інституту юридичної відповідальності, зменшення латентності правопорушень та забезпечення реальної дієвості правових норм у цифровому просторі.

3.2. Вектори розвитку інституту юридичної відповідальності у цифровому середовищі

Формування нових віртуальних середовищ, передусім метавсесвіту, ставить перед юридичною наукою завдання докорінного переосмислення юридичної відповідальності шляхом створення нових доктринальних та нормативних конструкцій, здатних забезпечити належне функціонування досліджуваного інституту у цифровій реальності. Фундаментальною передумовою у цій сфері є визначення юрисдикційних меж діяльності у метавсесвіті, оскільки простежується проблема відсутності територіальної прив'язки цифрових дій. Можливим шляхом розв'язання цієї прогалини є встановлення юрисдикції за місцем реєстрації оператора платформи або шляхом укладення міжнародної угоди про «електронну юрисдикцію», яка забезпечила б однакові стандарти для різних держав. Вказане створило б основу для правової визначеності та зменшило ризик колізій між національним законодавством держав.

Першочерговим напрямом удосконалення інституту юридичної відповідальності є криміналізація нових форм суспільно небезпечної поведінки, що виникають у віртуальних середовищах. З огляду на динаміку розвитку VR- та AR-технологій, а також функціонування метаверсів і блокчейн-платформ, доцільно передбачити у кримінальному законодавстві спеціальні склади злочинів, які враховуватимуть унікальну природу віртуальних активів і цифрових взаємодій. Вважаємо за доцільне, зокрема:

Доцільним видається запровадження окремої кримінально-правової норми, що встановлювала б відповідальність за шахрайство з віртуальними активами, визнавала їх специфічний правовий статус та враховувала економічну цінність цифрових об'єктів, зокрема криптовалют, NFT і токенів. Водночас, попри те що прийняття Закону України «Про віртуальні активи» стало важливим кроком у напрямі легалізації криптовалютної сфери, його положення досі не отримали повної імплементації у правозастосовну

практику. Крім того, у чинному кримінальному та фінансовому законодавстві залишаються суттєві прогалини, що унеможливлюють адекватне реагування на злочини у сфері криптовалютних відносин [48, с. 53–57]. У зв'язку з цим обґрунтованим видається внесення змін до Кримінального кодексу України та суміжних нормативно-правових актів з метою закріплення спеціальних складів злочинів, пов'язаних із неправомірним використанням криптоактивів. До них варто віднести: а) незаконне заволодіння віртуальними активами (крадіжка, шахрайство чи зловживання довірою у криптовалютному середовищі); б) відмивання коштів через криптовалюту, що становить одну з найбільш поширених практик використання блокчейн-технологій у кримінальних схемах; в) створення та функціонування фінансових пірамід із використанням токенів чи криптовалют, які завдають значної шкоди економічним інтересам громадян і держави.

Як показує сучасна практика та наукові дослідження, відсутність прямих норм про кримінальну відповідальність за криптовалютні злочини призводить до фактичної безкарності правопорушників і створює умови для легалізації протиправних схем у цифровому середовищі. Внесення відповідних змін у законодавство, насамперед криміналізація зазначених діянь, є нагальною практичною рекомендацією, що відповідає міжнародним зобов'язанням України у сфері протидії відмиванню коштів та фінансуванню тероризму. Вдосконалення правового регулювання у сфері віртуальних активів дозволить заповнити наявні прогалини, підвищити рівень правової визначеності та забезпечити реальну невідворотність юридичної відповідальності за правопорушення у сфері блокчейну, що, у свою чергу, сприятиме зміцненню фінансової безпеки держави та розвитку України у глобальному правовому просторі регулювання криптовалютних відносин.

Встановити кримінальну відповідальність за кібербулінг у VR-середовищах та кваліфікувати його як різновид психологічного насильства, що здійснюється у віртуальному просторі із застосуванням аватарів та інтерактивних інструментів.

Врегулювати посягання на віртуальну ідентичність користувача у вигляді створення фальшивих аватарів, викрадення або маніпуляції персоніфікованими даними у як окремий об’єкт кримінально-правової охорони.

Розширити предмет кримінально-правового захисту шляхом включення до нього цифрових благ і нематеріальних об’єктів, що мають цінність у віртуальному середовищі.

Окремого вектору удосконалення інституту юридичної відповідальності потребує цивільно-правове (деліктне) регулювання шкоди, завданої у VR-, AR-середовищах та метаверсах. У сучасних умовах шкода може проявлятися у вигляді порушення немайнових прав, зокрема честі, гідності, ділової репутації чи права на особисту ідентичність у віртуальному просторі. З метою забезпечення ефективності правового захисту пропонуємо наступне:

– визнати віртуальну ідентичність користувача об’єктом цивільно-правової охорони, що дозволить застосовувати деліктні механізми у випадках неправомірного використання або викривлення образу аватара;

– розширити категорію майнової шкоди та включити до неї втрати, пов’язані з неправомірним використанням чи знеціненням віртуальних активів (криптовалюти, NFT, токенізованих цифрових об’єктів), адже їх економічна вартість визнається як предмет цивільного обігу; зазначене, у свою чергу, розширить доктрину особистих немайнових прав та створить передумови для ефективного судового захисту від порушень, які нині здебільшого залишаються у «сірій зоні»;

– запровадити компенсацію моральної шкоди у випадках віртуального булінгу чи переслідування у VR-середовищах, що передбачає визнання, що психологічні наслідки таких дій можуть бути не менш значущими, ніж у традиційних офлайн-взаєминах;

– закріпити спеціальні презумпції причинного зв’язку у деліктних спорах щодо застосування ШІ, що дозволить зменшити тягар доказування

для потерпілих, які стикаються з інформаційною асиметрією у відносинах із розробниками чи провайдерами технологій;

– доцільним є також формування багаторівневої системи юридичної відповідальності, як власне передбачено міжнародними стандартами у досліджуваній сфері: первинна – за розробником і постачальником технології, вторинна – за інтегратором чи провайдером, і додаткова – за користувачем, який зловживає інструментами VR чи метаверсу; наведена модель відповідальності дозволить адекватно враховувати складність цифрових ланцюгів і мінімізувати ризик уникнення деліктної відповідальності через розмитість суб'єктного складу.

Ключову роль у впровадженні сучасних технічних рішень із послідовним удосконаленням правових механізмів юридичної відповідальності відіграють міжнародне співробітництво, підвищення рівня професійної підготовки фахівців у сфері кібербезпеки, а також систематичне оновлення законодавства з урахуванням стрімкої еволюції цифрових технологій [72, с. 138–144].

Варто наголосити, що перспективи розвитку інституту юридичної відповідальності у цифровому середовищі полягають у формуванні комплексної моделі, що поєднує кримінально-правові та цивільно-правові механізми захисту. З одного боку, криміналізація нових форм суспільно небезпечних діянь у віртуальних світах (шахрайство з віртуальними активами, кібербулінг у VR-середовищах, посягання на цифрову ідентичність) повинна забезпечити належний рівень превенції та репресії. Поряд із зазначеним, удосконалення цивільно-правових інструментів, про які ми наголошували вище, створює умови для ефективного відшкодування шкоди та відновлення порушених прав. Наведена двовимірна стратегія дозволяє гармонізувати національне законодавство з європейськими стандартами та сформувати нову парадигму юридичної відповідальності у цифровому суспільстві.

Важливим елементом розвитку інституту юридичної відповідальності у цифровому середовищі є врегулювання діяльності провайдерів цифрових платформ у метавсесвіті. Вказані суб'єкти фактично виконують функції приватних регуляторів, оскільки встановлюють правила поведінки користувачів шляхом прийняття «умов користування». Водночас такі документи, попри їхню поширеність та практичне значення, не можуть розглядатися як еквівалент державного правового регулювання, позаяк мають договірний характер і спрямовані переважно на захист інтересів самих провайдерів, а отже, не здатні забезпечити належний рівень охорони публічних інтересів та основоположних прав користувачів. З огляду на це, виникає необхідність законодавчого встановлення спеціальних обов'язків провайдерів цифрових платформ, що функціонують у метавсесвіті. Серед них:

1. Ідентифікація користувачів із метою запобігання анонімному вчиненню правопорушень та забезпечення належного реагування у випадках шкоди.

Анонімність у мережі виступає важливим елементом реалізації свободи вираження поглядів, однак відсутність належних механізмів верифікації унеможливлює встановлення суб'єкта правопорушення та знижує ефективність реагування з боку правоохоронних органів. З огляду на зазначене, доцільним є встановлення обов'язку провайдерів цифрових платформ впроваджувати процедури ідентифікації користувачів, які б дозволяли забезпечити належне співвідношення між правом на приватність та потребою у запобіганні анонімному вчиненню правопорушень. Слід підкреслити, що законодавче закріплення такого обов'язку повинно супроводжуватися чіткими гарантіями захисту персональних даних, що дозволить уникнути ризиків надмірного втручання у приватне життя та зловживань з боку провайдерів.

2. Захист персональних даних відповідно до сучасних стандартів права ЄС з урахуванням принципів мінімізації, цільового використання та обмеження зберігання.

Сьогодні обробка інформації про фізичних осіб є сферою підвищених ризиків порушення приватності, зловживань з боку комерційних структур та виникнення новітніх форм кіберзлочинності. У цьому контексті науково обґрунтованим видається запровадження на законодавчому рівні імперативних обов'язків провайдерів, спрямованих на дотримання сучасних стандартів права Європейського Союзу. У якості методологічної основи доцільним є звернення до положень Регламенту ЄС 2016/679 [65], який закріпив базові принципи обробки персональних даних. Передусім йдеться про: а) принцип мінімізації, що обмежує обсяг даних, які підлягають збору, тільки тими, що є необхідними для реалізації визначеної мети; б) принцип цільового використання, відповідно до якого дані можуть оброблятися виключно у цілях, для яких вони були зібрані, і будь-яке відхилення від цього правила визнається порушенням; в) принцип обмеження строків зберігання, що вимагає видалення або анонімізації даних після досягнення мети їхньої обробки.

Імплементація зазначених положень у національне законодавство створила б юридичні механізми відповідальності провайдерів у випадках порушення права на приватність і дозволила б забезпечити системний захист неповнолітніх та інших вразливих категорій користувачів у цифровому середовищі. Водночас закріплення таких обов'язків сприятиме гармонізації національного законодавства з acquis Європейського Союзу та відповідатиме євроінтеграційному вектору України.

3. Гарантії безпеки неповнолітніх, що передбачають обмеження доступу до небезпечного контенту, застосування батьківського контролю та превентивні механізми протидії кібербулінгу.

В Україні гарантії безпеки неповнолітніх у цифровому середовищі врегульовані лише фрагментарно. Конституція України у статті 52 закріплює

загальну норму про охорону прав дитини державою, що створює нормативне підґрунтя для спеціальних законодавчих рішень у сфері цифрової безпеки [37, с. 141]. У Законі України «Про охорону дитинства» передбачено обов'язок держави створювати умови для захисту дітей від інформації, здатної зашкодити їхньому фізичному, психічному чи моральному розвитку [61, с. 142]. Аналогічне позиціювання реалізовано у Законі «Про медіа», який містить обмеження щодо поширення програм, шкідливих для дітей, зокрема у формі часових рамок трансляції [59, с. 120]. Однак відповідні норми орієнтовані передусім на традиційні медіа й не охоплюють діяльність цифрових платформ чи VR/метаверсів.

Закон України «Про основні засади забезпечення кібербезпеки України» містить загальні положення щодо захисту прав громадян у кіберпросторі, проте не встановлює спеціальних гарантій для неповнолітніх [60, с. 403]. В окремих випадках застосовуються кримінально-правові та адміністративні засоби, зокрема відповідальність за розповсюдження порнографії, у тому числі дитячої (стаття 301^1 КК України) [40, с. 131], а також за булінг (стаття 173^4 КУпАП) [29]. Разом з тим, склад «кібербулінг» у VR чи соціальних мережах не виокремлений, а діяння кваліфікуються у загальних рамках булінгу в освітньому середовищі.

Відтак, чинне законодавство України не містить обов'язкових вимог до провайдерів цифрових платформ щодо запровадження механізмів батьківського контролю, обмеження доступу до небезпечного контенту чи превентивної протидії кібербулінгу. Наявні норми не формують системного правового режиму захисту неповнолітніх у цифровому середовищі, що свідчить про наявність правового вакууму та зумовлює необхідність розробки спеціального законодавства, яке б закріпило чіткі обов'язки провайдерів цифрових сервісів щодо безпеки дітей у віртуальному просторі.

4. Налагодження співпраці з правоохоронними органами, зокрема щодо обов'язкового інформування про випадки вчинення протиправних дій та забезпечення доступу до цифрових доказів.

Актуальним напрямом удосконалення інституту юридичної відповідальності у цифровому середовищі є налагодження співпраці провайдерів цифрових платформ із правоохоронними органами. У сучасних умовах саме провайдери часто володіють первинними цифровими доказами, без яких розслідування кіберзлочинів стає фактично неможливим. Водночас відсутність чітко визначених обов'язків щодо передачі такої інформації призводить до того, що правоохоронні органи стикаються з суттєвими труднощами у доступі до доказової бази. У цьому контексті доцільним видається законодавче закріплення обов'язку провайдерів інформувати компетентні органи про факти вчинення протиправних дій у віртуальних середовищах та забезпечувати належний доступ до цифрових доказів, що дозволить мінімізувати латентність кіберзлочинів, посилити ефективність кримінального переслідування, а також створити умови для формування превентивного ефекту у сфері функціонування цифрових платформ.

Формування нових віртуальних середовищ, передусім метавсесвіту, ставить перед юридичною наукою завдання докорінного переосмислення інституту юридичної відповідальності. Традиційні конструкції, вироблені для регулювання відносин у матеріальному світі, виявляються недостатніми для адекватного правового охоплення процесів, що відбуваються у цифровій реальності. У зв'язку з цим актуалізується потреба у створенні нових доктринальних моделей та нормативних механізмів, здатних забезпечити ефективне функціонування юридичної відповідальності в умовах цифровізації.

Одним зі стратегічних напрямів у цій сфері є впровадження концепції «структурної відповідальності» провайдерів цифрових платформ. Її сутність полягає у зміщенні акценту з реактивного підходу, відповідно до якого провайдери зобов'язані лише усувати наслідки правопорушень, на превентивний, що передбачає створення такої архітектури платформи та алгоритмів модерації, які мінімізують імовірність вчинення протиправних дій. Відповідальність провайдерів за таких умов набуває організаційно-

превентивного характеру, оскільки вони стають зобов’язаними враховувати потенційні ризики правопорушень уже на етапі проєктування цифрового середовища. Впровадження структурної відповідальності відображає формування нової парадигми правового регулювання, у межах якої провайдери визнаються не лише технічними посередниками, а активними суб’єктами формування цифрового середовища. Саме від якості архітектурних і алгоритмічних рішень залежить рівень безпеки у метавсесвіті, а отже – і реальна ефективність інституту юридичної відповідальності в умовах цифрової трансформації. Слід акцентувати, що розвиток інституту юридичної відповідальності у метавсесвіті передбачає застосування концепції «цифрового делікту» як окремої категорії правопорушення, що вимагає нормативного оформлення, виникає виключно у віртуальному середовищі та має низку специфічних рис, що відрізняють його від класичних правопорушень:

– характеризується нематеріальністю об’єкта посягання; якщо у традиційному деліктному праві предметом захисту є майнові або немайнові блага, що мають чітко визначену матеріальну чи соціальну природу, то у метавсесвіті об’єктом може виступати віртуальна ідентичність, цифровий аватар, віртуальний актив чи репутація у VR-просторі; відтак постає завдання доктринального визнання таких об’єктів як самостійних цінностей, що підлягають юридичній охороні;

– суттєвою ознакою цифрового делікту є його транскордонний характер – діяльність у метавсесвіті апріорі виходить за межі юрисдикції однієї держави, а тому правопорушення у віртуальному середовищі не може бути належним чином врегульоване винятково національним законодавством, що потребує вироблення уніфікованого розуміння на рівні міжнародного права, а також механізмів взаємного визнання юрисдикції та співпраці держав у сфері цифрової відповідальності;

– особливість анонімності суб’єкта – використання технологій шифрування, анонімізаторів, блокчейн-мереж та аватарів у VR-середовищах

значно ускладнює ідентифікацію правопорушників, що вимагає перегляду традиційних доктринальних положень щодо суб’єктного складу правопорушення та запровадження нових механізмів ідентифікації, які водночас не повинні порушувати права на приватність.

З огляду на зазначене, концепція цифрового делікту дозволяє закласти нову методологічну основу для розвитку інституту юридичної відповідальності у метавсесвіті. Її нормативна імплементація повинна передбачати: виокремлення цифрових деліктів у складі цивільно-правових і кримінально-правових порушень; розширення предмета правової охорони за рахунок віртуальних активів, цифрової ідентичності та нематеріальних об’єктів у VR/AR-просторах; створення процедур спрощеного доведення шкоди з огляду на інформаційну асиметрію між потерпілими та провайдерами; міжнародно-правову гармонізацію категорії цифрового делікту через участь України у формуванні європейських і глобальних стандартів регулювання.

Пропонуємо наступне визначення досліджуваному поняттю: цифровий делікт – це протиправне винне діяння, що здійснюється у віртуальному середовищі і характеризується нематеріальністю об’єкта посягання, транскордонністю юрисдикції та ускладненою ідентифікацією суб’єкта, внаслідок чого завдається шкода майновим чи немайновим правам особи, а також суспільним інтересам, які підлягають правовій охороні.

Також у рамках нашого дослідження слід звернути увагу, що питання надання правосуб’єктності децентралізованим автономним організаціям (DAO) є одним із ключових у контексті формування правового поля для функціонування блокчейн-стартапів та Web3-проєктів в Україні. DAO як спільноти, що функціонують на основі смарт-контрактів і не мають централізованого управління, кидають виклик класичним уявленням про юридичну особу, суб’єктність та юридичну відповідальність у національному праві.

Одним із потенційно ефективних шляхів врегулювання зазначеного питання може бути юридичне визнання DAO через спеціальну реєстрацію або адаптацію в межах існуючих організаційно-правових форм, у вигляді товариства з обмеженою відповідальністю, або ж запровадити нову окрему категорію, наприклад, «цифрові юридичні особи», подібно до концепції, запровадженої у деяких юрисдикціях США [184]. Юридичне визнання DAO дозволило б чітко визначити обсяг правоздатності такої організації, порядок набуття нею активів, укладення угод, участі в судових процесах, а головне – розмежувати відповідальність учасників. У разі відсутності спеціального правового статусу децентралізована автономна організація (DAO) в українському правовому контексті потенційно може бути розцінена судами як просте товариство відповідно до ст. 1130 Цивільного кодексу України, що зумовлює солідарну відповідальність усіх її учасників за зобов'язаннями, навіть якщо вони не брали безпосередньої участі в управлінні такою організацією [97, с. 356]. Модель правової суб'єктності DAO має бути максимально орієнтованою на саморегулювання з мінімальним державним втручанням, але чіткими правилами відповідальності. Деякі аналітики пропонують ввести концепцію «DAO legal wrappers», спеціальних рамок, що забезпечують легітимність взаємодії DAO з державними органами та судовою системою без обмеження їхньої внутрішньої автономії [136].

Ще одним напрямом розвитку інституту юридичної відповідальності у цифровому середовищі є нормативне визначення критеріїв відповідальності за автономні рішення, що приймаються із застосуванням систем штучного інтелекту. У сферах медицини, транспорту, фінансів автономні технології дедалі частіше використовуються для ухвалення рішень, однак чинне законодавство не визначає меж відповідальності людини у випадках їх застосування. Доцільним є закріплення правила, відповідно до якого використання автоматизованої системи не звільняє оператора від юридичної відповідальності, якщо тільки не буде доведено виняткових обставин, наприклад, технічного збою чи форс-мажору.

Так, Європейський парламент у дослідженні «Artificial Intelligence and Civil Liability» акцентує, що відповідальність повинен нести суб'єкт, який здійснює найбільший контроль над системою, тоді як розробники можуть залучатися у порядку регресу [118]. Аналогічні висновки містяться у роботах дослідника Philipp Hacker, де підкреслюється потреба у закріпленні презумпції відповідальності користувача із подальшим розподілом ризиків [156]. Формування правових критеріїв відповідальності за автономні рішення є необхідною умовою забезпечення правової визначеності та невідворотності відповідальності у сфері цифрових технологій, а також гарантією захисту прав осіб, яким може бути завдано шкоди внаслідок застосування систем штучного інтелекту [106].

У цьому аспекті доктринально обґрунтованою видається необхідність розробки та ухвалення спеціального закону «Про штучний інтелект». У зазначеному нормативному акті мають бути чітко визначені критерії відповідальності суб'єктів: розробника, якщо шкода спричинена дефектом алгоритму, впроваджувача у разі неналежного впровадження системи у виробничий процес, користувача за умови неправомірного або необережного застосування технології тощо. Принципово важливим є закріплення норми, відповідно до якої системи штучного інтелекту не визнаються самостійними носіями прав і обов'язків, а відповідальність за результати їх функціонування завжди покладається на визначених фізичних або юридичних осіб.

На наш погляд, Проєкт Закону України «Про штучний інтелект» повинен передбачати такі структурні елементи:

Розділ І. Загальні положення.

Розділ ІІ. Класифікація систем штучного інтелекту за рівнем ризику.

Розділ ІІІ. Вимоги до створення, впровадження та використання систем штучного інтелекту.

Розділ ІV. Юридична відповідальність за використання систем штучного інтелекту.

Розділ V. Інституційне забезпечення функціонування систем штучного інтелекту.

Розділ VI. Прикінцеві та перехідні положення.

У розділі «Загальні положення» слід визначити предмет і мету закону, які полягатимуть у встановленні єдиних засад правового регулювання функціонування штучного інтелекту, а також у забезпеченні гармонійного поєднання технологічного прогресу з охороною основоположних прав і свобод людини. У цьому ж розділі повинні бути закріплені базові терміни, зокрема «штучний інтелект», «система високого ризику», «оператор», «розробник», «постачальник», а також основні принципи відповідальності – ризик, сувора відповідальність, стандарти належної обачності. До ключових принципів правового регулювання доцільно віднести пріоритет прав і свобод людини, забезпечення прозорості та пояснюваності алгоритмічних рішень, дотримання принципу пропорційності обмежень, а також покладення відповідальності за ризики, пов’язані із застосуванням цифрових технологій.

У другому розділі доцільно передбачити класифікацію систем штучного інтелекту за рівнем ризику. Зокрема, необхідно розрізняти системи низького, обмеженого, високого та неприпустимого рівнів ризику. Критеріями такого поділу повинні бути сфера застосування (медицина, транспорт, безпека, правосуддя), масштаб потенційної шкоди та рівень вразливості користувачів.

У третьому розділі слід закріпити загальні та спеціальні вимоги до систем ШІ, зокрема прозорість алгоритмів, захист персональних даних і приватності, а також гарантування можливості людського нагляду. Для високоризикових систем відповідно до міжнародних стандартів варто запровадити додаткові вимоги, до яких доцільно віднести обов’язковий аудит, реєстрацію у державному реєстрі, сертифікацію відповідності та впровадження механізмів постійного моніторингу ризиків.

Четвертий розділ має бути присвячений питанням юридичної відповідальності. У ньому слід закріпити положення про те, що

відповідальність у сфері штучного інтелекту ґрунтується на ризику, а не на намірі системи, а суб'єктами відповідальності є розробники, оператори, постачальники та користувачі. Важливим елементом повинен стати інститут суворої відповідальності за шкоду, завдану високоризиковими системами життю, здоров'ю чи майну осіб. У таких випадках власник або оператор повинен нести відповідальність незалежно від вини. Для операторів та користувачів повинні бути встановлені стандарти належної обачності, порушення яких є підставою для відповідальності. У цьому ж розділі доцільно передбачити перелік заборонених систем, що створюють неприпустимий ризик, серед яких маніпуляція свідомістю, тотальне стеження тощо.

П'ятий розділ проєкту повинен визначати систему інституційного забезпечення. Доцільно передбачити створення національного органу з нагляду за штучним інтелектом, до повноважень якого належатиме реєстрація, аудит, контроль, застосування санкцій, а також взаємодія з європейськими та міжнародними структурами. Важливим елементом у цьому ключі стане державний реєстр високоризикових систем, який має бути публічним і забезпечувати доступ громадян до інформації. Доцільним є також запровадження обов'язкового страхування цивільної відповідальності для операторів високоризикових систем.

У прикінцевих та перехідних положеннях слід передбачити поетапне впровадження закону:

а) на першому етапі (протягом року) створення наглядового органу;

б) на другому (протягом двох років) запровадження державного реєстру та процедур сертифікації;

в) на третьому (протягом трьох років) повне набрання чинності положеннями про відповідальність і страхування.

Окрім того, необхідною є гармонізація національного законодавства з європейським правом, зокрема з Регламентом ЄС про штучний інтелект 2024 року, а також внесення змін до Цивільного кодексу, Господарського

кодексу, Кодексу України про адміністративні правопорушення та Кримінального кодексу України.

Не є новиною той факт, що розвиток інституту юридичної відповідальності у цифровому середовищі вимагає підвищення рівня компетентності органів, відповідальних за її реалізацію. У досліджуваному контексті актуальним вбачається запровадження системи безперервного навчання суддів та слідчих щодо особливостей роботи з цифровими доказами, методів встановлення причинно-наслідкового зв’язку у випадках алгоритмічних рішень, а також стандартів оцінки надійності програмних продуктів і цифрової інфраструктури. У правовій доктрині вже наголошується, що без належної технічної підготовки персоналу навіть найсучасніші закони залишатимуться декларативними та не зможуть забезпечити реальну невідворотність відповідальності [143].

Відтак інвестиції у людський капітал правосуддя постають як ключова умова ефективного розвитку інституту юридичної відповідальності в цифрову епоху, позаяк вони сприятимуть зниженню інформаційної асиметрії між технологічними компаніями та органами правосуддя, забезпечуватимуть можливість якісного розслідування новітніх правопорушень і підвищуватимуть довіру суспільства до спроможності держави гарантувати захист прав у цифровому середовищі.

Поряд із зазначеним, Україна повинна посилити участь у діючих міжнародних механізмах та ініціювати нові форми співробітництва, спрямовані на забезпечення невідворотності відповідальності незалежно від місця вчинення правопорушення. У цьому аспекті обґрунтованим видається активне використання положень Будапештської конвенції про кіберзлочинність 2001 року та Другого додаткового протоколу до неї 2022 року, які створюють правову основу для транскордонного доступу до електронних доказів, проведення спільних слідчих дій та оперативного обміну інформацією між державами. Важливим напрямом виступає також участь у роботі спільних слідчих груп Європолу та Інтерполу, що дозволяє

скоординувати зусилля у розслідуванні правопорушень, пов’язаних із використанням штучного інтелекту, блокчейн-технологій та віртуальних середовищ. Розвиток міжнародної співпраці у сфері притягнення до відповідальності за кіберзлочини є необхідною умовою формування дієвого механізму захисту прав у цифрову епоху. Лише за умови поєднання національних і міжнародних інструментів можна досягти належного рівня правової визначеності та забезпечити принцип невідворотності відповідальності за правопорушення у кіберпросторі.

Окремим напрямом розвитку інституту юридичної відповідальності є використання цифрових технологій як інструментів підсилення механізмів притягнення до відповідальності. Сучасні інтелектуальні системи здатні виконувати превентивні та доказові функції, що значно підвищує ефективність правозастосування. Зокрема, алгоритми моніторингу фінансових операцій можуть ідентифікувати ознаки шахрайства або відмивання коштів, а системи відеонагляду з функціями розпізнавання облич – сприяти пошуку осіб, які перебувають у розшуку. Водночас упровадження таких систем потребує належного правового врегулювання, зокрема забезпечення гарантій дотримання прав людини і фундаментальних свобод, а також дотримання принципів пропорційності, необхідності та законності під час застосування алгоритмічних інструментів у діяльності правоохоронних органів і судів [145]. Лише за умови впровадження чітких процедур контролю та незалежного нагляду можливе уникнення ризиків надмірного втручання у приватність чи недопустимого використання даних.

З огляду на зазначене вбачається доцільним на державному рівні реалізовувати пілотні проєкти із застосування штучного інтелекту у сфері судочинства, зокрема для аналізу судової практики, прогнозування ймовірності рецидиву та оцінки ризиків у кримінальних провадженнях. При цьому обов’язковими повинні бути незалежна оцінка результатів і розробка етичних стандартів функціонування таких систем. Практика використання алгоритмічних рішень у судових процедурах уже поширюється в низці

європейських держав, наприклад, у Франції та Нідерландах, і засвідчує потенціал підвищення якості судового аналізу за умови збереження верховенства права та автономії судді [120].

Особливої уваги заслуговує також проблема інституціоналізації принципів цифрової етики у правовому полі. Сьогодні правила поведінки у віртуальних спільнотах нерідко формуються у вигляді неформальних кодексів, стандартів або рекомендацій, що відображають етичні уявлення про допустимість певних практик у сфері цифрової взаємодії. Проте такі норми носять здебільшого декларативний характер і позбавлені юридично зобов'язуючої сили, що обмежує їхній вплив на формування відповідального цифрового середовища.

Слід підкреслити, що у правовій доктрині вже сформувалася низка базових принципів цифрової етики, які можуть бути інституціоналізовані у вигляді юридичних норм. Серед них доцільно виокремити принцип прозорості функціонування алгоритмів, відповідальності за наслідки діяльності штучного інтелекту, принцип недискримінаційності та рівного доступу до цифрових послуг, принцип поваги до приватності та персональних даних. Їхнє законодавче закріплення дозволить надати визначеності у сферах, де сьогодні панує саморегуляція або фрагментарні корпоративні стандарти.

Виходячи з наведеного, вбачаємо доцільним закріплення принципів цифрової етики у правовій площині з метою їх трансформації у юридично значущі регулятори поведінки, що дозволить узгодити вимоги, які висуває суспільство до етичності функціонування віртуальних спільнот, із нормативними приписами, що забезпечуються державним примусом. При цьому важливо підкреслити, що йдеться не про підміну права етикою, а про взаємодію двох систем регуляції, де етичні стандарти виконують роль методологічної основи для створення нових правових норм у сфері цифрових відносин.

Умови цифрових технологій висувають до інституту юридичної відповідальності низку нових вимог, серед яких гнучкість, технологічна нейтральність та міжнародна узгодженість. Перспективи його розвитку полягають не стільки у радикальній зміні сутності, адже базові принципи справедливості та вини залишаються непорушними, скільки у динамічній еволюції форм і методів реалізації відповідальності. Доцільним є впровадження вищенаведених рекомендацій, оскільки це сприятиме удосконаленню інституту юридичної відповідальності в Україні. Він стане більш всеосяжним, охоплюючи нові види правопорушень, більш дієвим завдяки чітким нормам і механізмам притягнення до відповідальності, а також сучасним, адекватно реагуючи на виклики цифрової епохи. Тим самим буде забезпечено невідворотність і справедливість відповідальності незалежно від того, у фізичному чи віртуальному світі вчинено правопорушення.

Безперечно, трансформація правових інститутів у цифрову добу не є одномоментним процесом, а відбувається поступово та у тісному взаємозв'язку з глобальними тенденціями і міжнародними правотворчими ініціативами. Водночас саме на сучасному етапі, коли цифрові технології радикально змінюють структуру суспільних відносин і механізми їх регулювання, закладаються підвалини нової юридичної реальності.

Висновки до розділу 3

У ході визначення перспектив модернізації інституту юридичної відповідальності в умовах цифровізації дисертантом встановлено проблемні аспекти та запропоновано низку практичних рекомендацій, спрямованих на розвиток інституту юридичної відповідальності України в умовах цифровізації, котрі спрямовані на усунення виявлених прогалин у законодавстві та правозастосуванні.

Встановлено, цифрові технології докорінно змінюють характер правопорушень і способи їх вчинення, розмивають межі юрисдикцій та створюють нові об’єкти та суб’єкти правовідносин. Наголошено, сам по собі розвиток цифрових технологій не «покращує» інститут відповідальності автоматично, навпаки, він виявляє його прогалини. Проте реагування на вказані виклики спонукає законодавця до оновлення правових рамок, що зрештою може удосконалити інститут юридичної відповідальності. У цьому ключі підкреслено наступне: цифрові інструменти виявляють і підсилюють прогалини чинного законодавства у сфері відповідальності; виникає нагальна потреба у переосмисленні критеріїв суб’єктності та атрибуції протиправної поведінки в умовах розподілених і анонімних систем; існує гострий дефіцит нормативного регулювання нових правових феноменів, що опосередковано впливають на зміст і форму юридичної відповідальності.

Наголошено, розгляд особливостей функціонування децентралізованих автономних організацій (DAO) та смарт-контрактів засвідчив наявність глибокої концептуальної кризи традиційної моделі юридичної відповідальності у цифровому середовищі. Виявлено, що відсутність централізованого керівного органу в DAO, а також автоматизованість ухвалення рішень, значно ускладнюють можливість визначення суб’єкта відповідальності, а отже і реалізацію юридичної відповідальності як інституту. Саме тому у сучасній доктрині зростає інтерес до концепцій розподіленої, колективної або програмно зумовленої відповідальності, а також до моделі визнання DAO як окремого суб’єкта права.

Проаналізовані підходи у правовому полі Європейського Союзу, зокрема, в межах Регламенту MiCA, демонструють зародження доктрини юридичної відповідальності у сфері автоматизованих правочинів. У результаті проведеного аналізу констатовано: а) доктрина юридичної відповідальності виявляє обмеженість при застосуванні до ситуацій, де немає чіткого людського волевиявлення, а дії є результатом виконання заздалегідь

запрограмованого коду; б) залишається неусталеною позиція щодо правосуб'єктності DAO, що унеможливлює належне юридичне оформлення її відповідальності; в) чинне національне законодавство не враховує автономних характеристик блокчейн-середовища та не пропонує ефективних інструментів юридичного реагування у разі настання шкоди внаслідок дії смарт-контракту.

Встановлено, юридична відповідальність за правопорушення у цифровому середовищі не обмежується виключно боротьбою з кіберзлочинністю. Особливої ваги набуває відповідальність у сфері захисту персональних даних, що прямо пов'язана з гарантіями реалізації інформаційної безпеки, права на приватність та дотримання гідності особи у цифровому вимірі. Наголошено, розвиток електронного урядування, онлайн-платформ та цифрових економічних відносин призводить до суттєвого зростання ризиків зловживання персональними даними. Відповідно, інститут юридичної відповідальності має адаптуватися до цих викликів шляхом: 1) удосконалення процедур контролю за обробкою даних; 2) підвищення рівня санкцій за порушення; 3) запровадження превентивних правових засобів захисту.

Визначено, юридична відповідальність у сфері ШІ поступово набуває рис об'єктивної (суворої) відповідальності, подібної до моделі відповідальності за шкоду, завдану дефектною продукцією. У контексті цифрових технологій вказана відповідальність стає ефективним інструментом правового реагування на складні, технічно опосередковані випадки спричинення шкоди. Акцентовано, концепція відповідальності за ризик як альтернатива традиційному поняттю вини є перспективною парадигмою для оновлення інституту юридичної відповідальності. У сфері ШІ відповідальність повинна покладатися не на агента, що має волю та намір, а на суб'єкта, який створив або експлуатує джерело технологічного ризику.

Констатовано, доктринальна дискусія про статус «електронної особи» для ШІ, попри її теоретичну значущість, наразі не має правової реалізації, що підкреслює необхідність зосередження уваги не на фіктивній суб'єктності машин, а на побудові ефективної системи відповідальності фізичних і юридичних осіб, відповідальних за створення, навчання та функціонування ШІ. Визнання правоздатності за системою, яка не має свідомості чи здатності до автономного морального вибору, створює ризик девальвації понять вини, наміру та справедливого покарання.

Акцентовано, на сучасному етапі в Україні відсутній спеціальний закон, який би комплексно врегульовував питання використання систем штучного інтелекту та відповідальності за їх функціонування. Регулювання здійснюється шляхом застосування загальних норм цивільного, адміністративного та кримінального законодавства, що створює прогалини у визначенні відповідальних суб'єктів і механізмів відшкодування шкоди, заподіяної автономними або напівавтономними технологіями. Вказаний стан правового поля вимагає термінового перегляду національного закріплення інституту відповідальності у сфері ШІ з урахуванням техніко-юридичних викликів. Ключовим напрямом розвитку правового регулювання в Україні має стати нормативна конкретизація: обов'язків розробників і провайдерів щодо безпеки алгоритмів; вимог до технічної і юридичної прозорості прийняття рішень у сферах з підвищеним ступенем ризику (медицина, фінанси, правосуддя); процедур контролю та моніторингу впровадження ШІ в державному управлінні.

Визначено, становлення віртуального середовища як автономного цифрового простору призводить до трансформації уявлень про територіальну та персональну юрисдикцію, що унеможливлює застосування традиційних норм міжнародного приватного права без відповідної адаптації. Аргументовано, цифрові активи у вигляді невзаємозамінних токенів (NFT), віртуальної нерухомості та інших нематеріальних об'єктів набувають ознак майнової цінності та потребують правового режиму, подібного до інституту

нематеріального майна у цивільному праві. Підкреслено, що моделі корпоративного (приватного) регулювання, засновані на правилах спільнот, не здатні забезпечити рівнозначний захист прав особи, порівняно з публічно-правовими механізмами, що обґрунтовує потребу державного втручання та встановлення загальнообов'язкових стандартів відповідальності у цифровому середовищі.

Акцентовано, ефективність застосування юридичної відповідальності у віртуальному просторі значною мірою залежить від рівня цифрової правової культури населення, що, у свою чергу, вимагає впровадження системної правопросвітницької політики та формування етики відповідальної цифрової поведінки.

Визначено вектори розвитку інституту юридичної відповідальності у цифровому середовищі: фундаментальною передумовою є визначення юрисдикційних меж діяльності у метавсесвіті, оскільки простежується проблема відсутності територіальної прив'язки цифрових дій. Можливим шляхом розв'язання цієї прогалини є встановлення юрисдикції за місцем реєстрації оператора платформи або шляхом укладення міжнародної угоди про «електронну юрисдикцію», яка забезпечила б однакові стандарти для різних держав. Вказане створило б основу для правової визначеності та зменшило ризик колізій між національним законодавством держав.

Стратегічним напрямом удосконалення інституту юридичної відповідальності є криміналізація нових форм суспільно небезпечної поведінки, що виникають у віртуальних середовищах. З огляду на динаміку розвитку VR- та AR-технологій, а також функціонування метаверсів і блокчейн-платформ, доцільно передбачити у кримінальному законодавстві спеціальні склади злочинів, які враховуватимуть унікальну природу віртуальних активів і цифрових взаємодій. Встановлено за доцільне, зокрема: 1) запровадити окрему кримінально-правову норму про шахрайство з віртуальними активами, яка б визнавала їх специфічний правовий статус і враховувала економічну цінність цифрових об'єктів (криптовалют, NFT,

токенів); обґрунтовано внесення змін до Кримінального кодексу України та суміжних нормативно-правових актів з метою закріплення спеціальних складів злочинів, пов’язаних із неправомірним використанням криптоактивів, серед яких: а) незаконне заволодіння віртуальними активами (крадіжка, шахрайство чи зловживання довірою у криптовалютному середовищі); б) відмивання коштів через криптовалюту, що становить одну з найбільш поширених практик використання блокчейн-технологій у кримінальних схемах; в) створення та функціонування фінансових пірамід із використанням токенів чи криптовалют, які завдають значної шкоди економічним інтересам громадян і держави; 2) встановити кримінальну відповідальність за кібербулінг у VR-середовищах та кваліфікувати його як різновид психологічного насильства, що здійснюється у віртуальному просторі із застосуванням аватарів та інтерактивних інструментів; 3) врегулювати посягання на віртуальну ідентичність користувача у вигляді створення фальшивих аватарів, викрадення або маніпуляції персоніфікованими даними у як окремий об’єкт кримінально-правової охорони; 4) розширити предмет кримінально-правового захисту шляхом включення до нього цифрових благ і нематеріальних об’єктів, що мають цінність у віртуальному середовищі.

Окремого вектору удосконалення інституту юридичної відповідальності потребує цивільно-правове (деліктне) регулювання шкоди, завданої у VR-, AR-середовищах та метаверсах. У сучасних умовах шкода може проявлятися у вигляді порушення немайнових прав, зокрема честі, гідності, ділової репутації чи права на особисту ідентичність у віртуальному просторі. З метою забезпечення ефективності правового захисту запропоновано наступне: 1) визнати віртуальну ідентичність користувача об’єктом цивільно-правової охорони, що дозволить застосовувати деліктні механізми у випадках неправомірного використання або викривлення образу аватара; 2) розширити категорію майнової шкоди та включити до неї втрати, пов’язані з неправомірним використанням чи знеціненням віртуальних

активів (криптовалюти, NFT, токенізованих цифрових об’єктів), адже їх економічна вартість визнається як предмет цивільного обігу; зазначене, у свою чергу, розширить доктрину особистих немайнових прав та створить передумови для ефективного судового захисту від порушень, які нині здебільшого залишаються у «сірій зоні»; 3) запровадити компенсацію моральної шкоди у випадках віртуального булінгу чи переслідування у VR-середовищах, що передбачає визнання, що психологічні наслідки таких дій можуть бути не менш значущими, ніж у традиційних офлайн-взаєминах; 4) закріпити спеціальні презумпції причинного зв’язку у деліктних спорах щодо застосування ШІ, що дозволить зменшити тягар доказування для потерпілих, які стикаються з інформаційною асиметрією у відносинах із розробниками чи провайдерами технологій; 5) забезпечити формування багаторівневої системи юридичної відповідальності, як власне передбачено міжнародними стандартами у досліджуваній сфері: первинна – за розробником і постачальником технології, вторинна – за інтегратором чи провайдером, і додаткова – за користувачем, який зловживає інструментами VR чи метаверсу; наведена модель відповідальності дозволить адекватно враховувати складність цифрових ланцюгів і мінімізувати ризик уникнення деліктної відповідальності через розмитість суб’єктного складу.

Важливим елементом розвитку інституту юридичної відповідальності у цифровому середовищі є врегулювання діяльності провайдерів цифрових платформ у метавсесвіті. Вказані суб’єкти фактично виконують функції приватних регуляторів, оскільки встановлюють правила поведінки користувачів шляхом прийняття «умов користування». Водночас такі документи, попри їхню поширеність та практичне значення, не можуть розглядатися як еквівалент державного правового регулювання, позаяк мають договірний характер і спрямовані переважно на захист інтересів самих провайдерів, а отже, не здатні забезпечити належний рівень охорони публічних інтересів та основоположних прав користувачів. З огляду на це, виникає необхідність законодавчого встановлення спеціальних обов’язків

провайдерів цифрових платформ, що функціонують у метавсесвіті. Серед них: 1) ідентифікація користувачів із метою запобігання анонімному вчиненню правопорушень та забезпечення належного реагування у випадках шкоди; 2) захист персональних даних відповідно до сучасних стандартів права ЄС з урахуванням принципів мінімізації, цільового використання та обмеження зберігання; 3) гарантії безпеки неповнолітніх, що передбачають обмеження доступу до небезпечного контенту, застосування батьківського контролю та превентивні механізми протидії кібербулінгу; 4) налагодження співпраці з правоохоронними органами, зокрема щодо обов'язкового інформування про випадки вчинення протиправних дій та забезпечення доступу до цифрових доказів.

Визначено за доцільне впровадження так званої «структурної відповідальності» провайдерів, яка передбачає їх обов'язок запобігати правопорушенням через архітектуру платформи та алгоритми модерації. Її сутність полягає у зміщенні акценту з реактивного позиціювання, відповідно до якого провайдери зобов'язані тільки усувати наслідки правопорушень, на превентивний, що передбачає створення такої архітектури платформи та алгоритмів модерації, які мінімізують імовірність вчинення протиправних дій. Відповідальність провайдерів за таких умов набуває організаційно-превентивного характеру, оскільки вони стають зобов'язаними враховувати потенційні ризики правопорушень уже на етапі проєктування цифрового середовища. Впровадження структурної відповідальності відображає нову парадигму правового регулювання, у межах якої провайдери визнаються не просто технічними посередниками, а активними суб'єктами формування цифрового середовища. Саме від якості архітектурних та алгоритмічних рішень залежить рівень безпеки у метавсесвіті, а отже, і реальна ефективність інституту юридичної відповідальності в умовах цифрової трансформації.

Розвиток інституту юридичної відповідальності у метавсесвіті передбачає застосування концепції «цифрового делікту» як окремої категорії правопорушення, що вимагає нормативного оформлення, виникає виключно

у віртуальному середовищі та має низку специфічних рис, що відрізняють його від класичних правопорушень: а) характеризується нематеріальністю об'єкта посягання; якщо у традиційному деліктному праві предметом захисту є майнові або немайнові блага, що мають чітко визначену матеріальну чи соціальну природу, то у метавсесвіті об'єктом може виступати віртуальна ідентичність, цифровий аватар, віртуальний актив чи репутація у VR-просторі; відтак постає завдання доктринального визнання таких об'єктів як самостійних цінностей, що підлягають юридичній охороні; б) суттєвою ознакою цифрового делікту є його транскордонний характер – діяльність у метавсесвіті апріорі виходить за межі юрисдикції однієї держави, а тому правопорушення у віртуальному середовищі не може бути належним чином врегульоване винятково національним законодавством, що потребує вироблення уніфікованого розуміння на рівні міжнародного права, а також механізмів взаємного визнання юрисдикції та співпраці держав у сфері цифрової відповідальності; в) особливість анонімності суб'єкта – використання технологій шифрування, анонімізаторів, блокчейн-мереж та аватарів у VR-середовищах значно ускладнює ідентифікацію правопорушників, що вимагає перегляду традиційних доктринальних положень щодо суб'єктного складу правопорушення та запровадження нових механізмів ідентифікації, які водночас не повинні порушувати права на приватність.

Запропоновано наступне визначення досліджуваному поняттю: цифровий делікт – це протиправне винне діяння, що здійснюється у віртуальному середовищі і характеризується нематеріальністю об'єкта посягання, транскордонністю юрисдикції та ускладненою ідентифікацією суб'єкта, внаслідок чого завдається шкода майновим чи немайновим правам особи, а також суспільним інтересам, які підлягають правовій охороні.

Наголошено, ще одним напрямом розвитку інституту юридичної відповідальності у цифровому середовищі є нормативне визначення критеріїв відповідальності за автономні рішення, що приймаються із застосуванням

систем штучного інтелекту. У сферах медицини, транспорту, фінансів автономні технології дедалі частіше використовуються для ухвалення рішень, однак чинне законодавство не визначає меж відповідальності людини у випадках їх застосування. Доцільним є закріплення правила, відповідно до якого використання автоматизованої системи не звільняє оператора від юридичної відповідальності, якщо тільки не буде доведено виняткових обставин, наприклад, технічного збою чи форс-мажору.

Визначено за доцільне запровадження системи безперервного навчання суддів та слідчих щодо особливостей роботи з цифровими доказами, методів встановлення причинно-наслідкового зв'язку у випадках алгоритмічних рішень, а також стандартів оцінки надійності програмних продуктів і цифрової інфраструктури. Інвестиції у людський капітал правосуддя сьогодні постають як ключова умова ефективного розвитку інституту юридичної відповідальності у цифрову епоху, позаяк сприятимуть зниженню інформаційної асиметрії між технологічними компаніями та органами правосуддя, забезпечать можливість якісного розслідування новітніх правопорушень та підвищать довіру суспільства до спроможності держави гарантувати захист прав у цифровому середовищі.

Наголошено, Україна повинна посилити участь у діючих міжнародних механізмах та ініціювати нові форми співробітництва, спрямовані на забезпечення невідворотності відповідальності незалежно від місця вчинення правопорушення. Розвиток міжнародної співпраці у сфері притягнення до відповідальності за правопорушення у мережі Інтернет є необхідною умовою формування дієвого механізму захисту прав у цифрову епоху. Лише за умови поєднання національних і міжнародних інструментів можна досягти належного рівня правової визначеності та забезпечити принцип невідворотності відповідальності за правопорушення у кіберпросторі.

Окремим напрямом розвитку інституту юридичної відповідальності є використання цифрових технологій як інструментів підсилення механізмів притягнення до відповідальності. Сучасні інтелектуальні системи здатні

виконувати превентивні та доказові функції, що значно підвищує ефективність правозастосування. Водночас впровадження таких систем потребує належного правового врегулювання, зокрема забезпечення гарантій дотримання прав людини та фундаментальних свобод, а також принципів пропорційності, необхідності та законності при застосуванні алгоритмічних інструментів у діяльності правоохоронних органів та судів [135]. Лише за умови впровадження чітких процедур контролю та незалежного нагляду можливе уникнення ризиків надмірного втручання у приватність чи недопустимого використання даних.

Визначено доцільним закріплення принципів цифрової етики у правовій площині з метою їх трансформації у юридично значущі регулятори поведінки, що дозволить узгодити вимоги, які висуває суспільство до етичності функціонування віртуальних спільнот, із нормативними приписами, що забезпечуються державним примусом. Підкреслено, йдеться не про підміну права етикою, а про взаємодію двох систем регуляції, де етичні стандарти виконують роль методологічної основи для створення нових правових норм у сфері цифрових відносин.

Доктринально обґрунтовано необхідність розроблення та ухвалення спеціального Закону України «Про штучний інтелект». У зазначеному нормативно-правовому акті доцільно чітко визначити критерії юридичної відповідальності відповідних суб’єктів, зокрема: розробника – у разі заподіяння шкоди внаслідок дефекту алгоритму; впроваджувача – у випадку неналежного інтегрування системи у виробничий або управлінський процес; користувача – за умови неправомірного або необережного застосування технології тощо. Принципово важливим є нормативне закріплення положення про те, що системи штучного інтелекту не визнаються самостійними носіями прав та обов’язків, а відтак юридична відповідальність у всіх випадках покладається на визначених фізичних або юридичних осіб, пов’язаних із розробленням, впровадженням або використанням відповідної системи.

Встановлено, Проєкт Закону України «Про штучний інтелект» повинен передбачати такі структурні елементи: Розділ I. Загальні положення; Розділ II. Класифікація систем штучного інтелекту за рівнем ризику; Розділ III. Вимоги до створення, впровадження та використання систем штучного інтелекту; Розділ IV. Юридична відповідальність за використання систем штучного інтелекту; Розділ V. Інституційне забезпечення функціонування систем штучного інтелекту; Розділ VI. Прикінцеві та перехідні положення.

У розділі I «Загальні положення» слід: 1) визначити предмет і мету закону, які полягатимуть у встановленні єдиних засад правового регулювання функціонування штучного інтелекту, а також у забезпеченні гармонійного поєднання технологічного прогресу з охороною основоположних прав і свобод людини; 2) закріпити базові терміни, зокрема «штучний інтелект», «система високого ризику», «оператор», «розробник», «постачальник», а також основні принципи відповідальності – ризик, сувора відповідальність, стандарти належної обачності. У розділі II доцільно передбачити класифікацію систем штучного інтелекту за рівнем ризику та розрізняти системи низького, обмеженого, високого та неприпустимого ризику. Критеріями такого поділу повинні стати сфера застосування (медицина, транспорт, безпека, правосуддя), масштаб потенційної шкоди та рівень вразливості користувачів. У розділі III слід закріпити загальні та спеціальні вимоги до систем ШІ, зокрема, прозорість алгоритмів, захист персональних даних і приватності, а також гарантування можливості людського нагляду. Для високоризикових систем відповідно до міжнародних стандартів варто запровадити додаткові вимоги, до яких доцільно віднести обов’язковий аудит, реєстрацію у державному реєстрі, сертифікацію відповідності та впровадження механізмів постійного моніторингу ризиків. Четвертий розділ повинен містити положення про те, що відповідальність у сфері штучного інтелекту ґрунтується на ризику, а не на намірі системи, а суб’єктами відповідальності є розробники, оператори, постачальники та користувачі. Важливим елементом повинен стати інститут суворої

відповідальності за шкоду, завдану високоризиковими системами життю, здоров'ю чи майну осіб. У таких випадках власник або оператор повинен нести відповідальність незалежно від вини. Для операторів та користувачів повинні бути встановлені стандарти належної обачності, порушення яких є підставою для відповідальності. У цьому ж розділі доцільно передбачити перелік заборонених систем, що створюють неприпустимий ризик, серед яких маніпуляція свідомістю, тотальне стеження тощо.

П'ятий розділ повинен передбачити створення національного органу з нагляду за штучним інтелектом, до повноважень якого належатиме реєстрація, аудит, контроль, застосування санкцій, а також взаємодія з європейськими та міжнародними структурами. Важливим елементом у цьому ключі стане державний реєстр високоризикових систем, який має бути публічним і забезпечувати доступ громадян до інформації. Визначено за доцільне запровадження обов'язкового страхування цивільної відповідальності для операторів високоризикових систем. У прикінцевих та перехідних положеннях слід передбачити поетапне впровадження закону: а) на першому етапі (протягом року) створення наглядового органу; б) на другому (протягом двох років) запровадження державного реєстру та процедур сертифікації; в) на третьому (протягом трьох років) повне набрання чинності положеннями про відповідальність і страхування.

Резюмовано, умови цифрових технологій висувають до інституту юридичної відповідальності низку нових вимог, серед яких гнучкість, технологічна нейтральність та міжнародна узгодженість. Перспективи його розвитку полягають не стільки у радикальній зміні сутності, адже базові принципи справедливості та вини залишаються непорушними, скільки у динамічній еволюції форм і методів реалізації відповідальності. Безперечно, трансформація правових інститутів у цифрову добу не є одномоментним процесом, а відбувається поступово та у тісному взаємозв'язку з глобальними тенденціями і міжнародними правотворчими ініціативами. Водночас саме на сучасному етапі, коли цифрові технології радикально

змінюють структуру суспільних відносин і механізми їх регулювання, закладаються підвалини нової юридичної реальності.

ВИСНОВКИ

У дисертаційному дослідженні здійснено комплексний теоретичний аналіз феномену юридичної відповідальності за правопорушення у мережі Інтернет, узагальнено сучасні наукові підходи та вироблено авторське бачення її загальнотеоретичних засад. Зокрема, сформульовано такі концептуальні положення:

Встановлено, цифровізаційні процеси зумовили виникнення якісно нових викликів для класичної доктрини юридичної відповідальності. Сучасна правова доктрина формує низку концептуальних підходів, спрямованих на адаптацію категорії відповідальності до умов цифрової доби: активно розробляється концепція розподіленої відповідальності, яка передбачає можливість одночасного залучення до відповідальності кількох суб'єктів цифрового простору, зокрема власників платформ, розробників алгоритмів та кінцевих користувачів; формується технологічна відповідальність, під якою розуміють юридичну відповідальність за створення, використання чи недосконаліть алгоритмів, систем штучного інтелекту та автоматизованих рішень, які здатні спричиняти юридично значущі наслідки; розвивається концепція деанонімізованої відповідальності, спрямована на пошук кореляції між забезпеченням права особи на приватність у мережі та необхідністю притягнення її до відповідальності у разі вчинення шкідливої чи протиправної поведінки.

Визначено, уніфікація та стандартизація термінології у сфері цифрових процесів має суттєве значення як для розвитку правової науки, так і для практики законотворення та правозастосування: забезпечує методологічну цілісність наукових досліджень, створюючи умови для узгодженості концептуальних підходів у різних галузях права; вказане унеможливлює дублювання понять, знімає семантичні суперечності та сприяє формуванню єдиної доктрини цифрової трансформації права; у практичному вимірі уніфікація термінів підвищує якість законодавчої

техніки, адже чітко окреслені дефініції зменшують ризик правових колізій і підвищують передбачуваність норм; сприяє єдності судової практики, оскільки стандартизований термінологічний апарат зменшує можливість неоднозначного тлумачення судами та адміністративними органами; 4) на міжнародному рівні уніфікація дозволяє гармонізувати національне законодавство з європейськими та глобальними правовими стандартами, що є необхідною умовою інтеграції України у світовий правовий простір.

Констатовано, глобалізація та цифрова модернізація суспільства виступають чинниками, що зумовлюють сутнісне переосмислення природи юридичної відповідальності. У сьогоденному правовому дискурсі простежується відхід від її традиційного трактування виключно крізь призму формально-юридичних ознак складу правопорушення. Натомість акцент поступово зміщується на оцінку суспільної результативності відповідальності, яка розглядається як інструмент відновлення порушених прав, превенції майбутніх правопорушень і підтримання довіри до державно-владних інститутів як системної цінності.

Репрезентовано, модель багаторівневої юридичної відповідальності передбачає взаємодію кількох взаємопов’язаних рівнів, що відображають сучасні тенденції розвитку правового регулювання. На державному рівні зберігається класична архітектоніка юридичної відповідальності, яка реалізується через кримінально-правові, адміністративно-правові, цивільно-правові механізми тощо. На міжнародному рівні юридична відповідальність набуває форми юрисдикції міжнародних судових та квазісудових органів, а також виражається у виконанні державами зобов’язань за міжнародними договорами, що посилює інтеграцію національних систем у глобальний правовий простір. Водночас формується недержавний рівень відповідальності, який охоплює механізми саморегулювання, зокрема цифрову етику, корпоративні кодекси поведінки, внутрішні регламенти цифрових платформ. Зазначений рівень відображає нові форми юридично

значущого впливу, що виникають у межах цифрового середовища та доповнюють класичні державні та міжнародні інструменти.

Наголошено, системний аналіз міжнародно-правових актів і стратегічних документів провідних міжнародних організацій свідчить про відсутність уніфікованого нормативного визначення поняття «кіберпростір». Водночас у більшості актів простежується його трактування як глобального інформаційно-комунікаційного середовища, у межах якого підлягають застосуванню загальновизнані норми міжнародного права. При цьому акценти розставляються по-різному, у доктринальних матеріалах НАТО домінує безпековий вимір, у позиціюванні Європейського Союзу пріоритет надається захисту прав і свобод людини. Спільним знаменником вказаних трактувань є визнання транснаціонального характеру кіберпростору та необхідності міжнародної координації у його регулюванні.

Підкреслено, правовий статус кіберпростору ще не врегульовано спеціальним міжнародним договором чи єдиним кодифікованим актом. Однак це не означає, що кіберсфера є правовим вакуумом, держави та міжнародні органи послідовно підтверджують застосовність до неї загальних норм міжнародного права, зокрема Статуту ООН, норм гуманітарного права та міжнародних стандартів у сфері прав людини.

Визначено, кіберпростір доцільно визначати як глобальну сферу діяльності людства, що поступово набуває рис особливого міжнародно-правового режиму. Він не може бути віднесений ані до класичних категорій території, ані до виключно техногенних об’єктів, оскільки за своєю природою постає новим виміром міжнародних відносин. У межах цього виміру вже функціонують основоположні норми міжнародного права, серед яких загальні принципи, імперативні норми, а також окремі галузеві договори. Водночас ці норми потребують подальшого розвитку та конкретизації з урахуванням специфіки цифрового середовища та особливостей правової кваліфікації дій у ньому.

Артикульовано, міжнародне співтовариство рухається шляхом поступового формування стандартів та правил належної поведінки в кіберпросторі. Остаточне визначення його правового статусу передбачатиме синтез кількох концепцій шляхом поєднання визнання кіберпростору як спільної сфери інтересів людства із водночас збереженням за державами суверенних прав на їхні інформаційні ресурси, а також юрисдикції над злочинною чи ворожою діяльністю, що виходить із чи спрямована проти їхньої території. За таких умов кіберпростір функціонуватиме як відкрите, стійке та мирне середовище, спрямоване на розвиток людства, а не перетворюватиметься на арену анархії або вседозволеності.

Акцентовано, важливою ознакою мережі Інтернет є її модель управління, позаяк він історично розвивався за багатосторонньою логікою, у межах якої поряд із державами ключову роль відіграють технічні спільноти стандартотворення, інституції ідентифікаторів, оператори мереж, платформи та громадянське суспільство. Вказана модель спирається на поєднання «твердого» права та «м'якого» регулювання (стандарти, кодекси, політики застосунків, угоди між операторами та реєстрами), що формує специфічний регулятивний режим співуправління. Для правового аналізу зазначене передбачає розщеплення центрів нормотворення, розмиті кордони юрисдикції та необхідність узгодження технічних стандартів із вимогами верховенства права та прав людини.

Доведено, кіберпростір та мережа Інтернет співвідносяться як широка правова категорія та її інфраструктурна основа. Їх поєднують спільні цінності, але відрізняє предмет регулювання, рівень інституціоналізації та специфіка суб'єктного складу управління. Кіберпростір слід розглядати як глобальне соціально-технічне середовище, що поєднує інформаційні потоки та комунікаційні системи, не має фізичних меж, однак, генерує реальні правові наслідки. Інтернет у системі кіберпростору виконує роль матеріальної та організаційної інфраструктури, яка забезпечує функціонування кіберпростору, проте водночас формує власний специфічний

правовий режим. Його регулятивна природа визначається поєднанням норм національного законодавства, міжнародного права та актів саморегуляторних спільнот.

Встановлено, з точки зору інституту юридичної відповідальності, вказані феномени виступають просторами, у яких класичні доктринальні категорії набувають нового змістовного навантаження. Транскордонний характер мережевих комунікацій ускладнює ідентифікацію правопорушника та визначення юрисдикції, що обумовлює потребу у розробці міжнародних стандартів поведінки у цифровому середовищі та активній участі держав в інституційних ініціативах. У цьому ключі саме через призму юридичної відповідальності стає можливим забезпечення належної кореляції між забезпеченням прав та свобод людини, суверенітетом держав, потребою у глобальній стабільності і безпеці кіберпростору та мережі Інтернет.

Встановлено, що сучасна трансформація глобального інформаційного простору зумовила формування багаторівневої системи міжнародних стандартів юридичної відповідальності у цифровому середовищі. Їх основу становлять як універсальні та регіональні договори (Конвенція Ради Європи №108 і Протокол 2018 р., Будапештська конвенція 2001 р. і Додатковий протокол 2003 р., Лансаротська конвенція 2007 р.), так і правові акти ЄС (директиви, регламенти, зокрема Digital Services Act 2022/2065 та AI Act 2024 р.), що визначають сучасну архітектуру цифрового врядування. Констатовано, що вказані акти закріплюють матеріально-правові та процесуальні підвалини юридичної відповідальності за правопорушення в мережі Інтернет та формують нові моделі її реалізації, серед яких концепція «цифрової приватності», принцип екстратериторіальності у сфері захисту персональних даних, доктрина «відповідальної платформи» та risk-based підхід до регулювання штучного інтелекту.

Визначено, що міжнародна практика передбачає багатоманітність векторів формування цифрових стандартів від обов’язкових міжнародно-правових актів (Африканська конвенція 2014 р., Арабська конвенція 2010 р.)

до актів «м'якого права» (рекомендації ОАД, APEC Privacy Framework тощо). Попри відмінності у правовій природі, констатовано тенденцію до гармонізації національних законодавств із положеннями Будапештської конвенції та європейськими стандартами у сфері кібербезпеки та захисту даних. Підкреслено, що значення цих актів виходить за межі суто правового виміру, позаяк вони задають нову парадигму відповідальності у цифрову добу, де належна кореляція між свободою обігу інформації, інноваційним розвитком і гарантіями прав людини виступає системоутворюючим чинником.

Аргументовано, що глобальний процес формування міжнародних стандартів у сфері кібербезпеки не обмежується лише договірними інструментами, а спирається і на доктринальні орієнтири, котрі деталізують застосування базових принципів міжнародного права, що підвищує рівень юридичної визначеності та формує концептуальне підґрунтя для подальшої кодифікації.

Сформулювано низку пропозицій, спрямованих на підвищення ефективності положень Конвенції ООН про кіберзлочинність 2024 року як міжнародно-правового інструменту: 1) у тексті Конвенції варто забезпечити чітке та однозначне визначення складів кіберзлочинів, позаяк наявність нечітких формулювань створює загрозу довільного правозастосування, надмірної криміналізації та може призвести до обмеження законної діяльності, зокрема журналістської, дослідницької чи правозахисної; 2) встановлені Конвенцією процедури збирання та обміну електронними доказами, а також заходи, що передбачають втручання у приватність, мають здійснюватися виключно на основі принципу пропорційності, котрий передбачає перевірку необхідності, доцільності та співмірності кожного втручання у сферу прав людини; 3) для забезпечення належної підзвітності та запобігання можливим зловживанням необхідним є створення міжнародного органу або спеціальної процедури оцінки дотримання державами стандартів Конвенції; вказаний механізм міг би здійснювати регулярний нагляд,

проводити експертні огляди та видавати рекомендації щодо усунення виявлених порушень; 4) Конвенція повинна бути гармонізована з уже чинними міжнародно-правовими інструментами у сфері кіберзлочинності, передусім із Будапештською конвенцією Ради Європи 2001 р., що дозволить уникнути дублювання норм, зменшить ризики колізій та сприятиме формуванню цілісної транснаціональної системи кримінальної юстиції у цифровому середовищі.

На основі аналізу міжнародних стандартів у сфері юридичної відповідальності за правопорушення у мережі Інтернет зроблено ряд висновків: міжнародна нормативна база у цій сфері є фрагментованою за географічною та предметною ознакою, проте спостерігається тенденція до її уніфікації; входження до глобальних домовленостей значно ширшого кола держав з різними правовими системами породжує виклик дотримання прав людини; як показав аналіз фінального тексту конвенції ООН, відсутність жорстких гарантій може бути використана авторитарними режимами для переслідування інакодумців під приводом боротьби з кіберзлочинами; найбільше розвинені стандарти стосуються саме кримінальної відповідальності, що історично обумовлено першочерговим фокусом на кіберзлочинності; натомість міжнародні механізми цивільно-правової та адміністративної відповідальності розвинені значно менше та носять характер радше рекомендацій, ніж обов’язкових норм; встановлено, у перспективі варто очікувати розвитку саме таких «горизонтальних» стандартів, зокрема, у сфері відповідальності постачальників цифрових послуг; ефективність міжнародних стандартів корелюється із належною імплементацією на національному рівні; навіть після приєднання до міжнародних договорів окремі держави не забезпечують повної гармонізації внутрішнього законодавства; не всі передбачені Конвенцією про кіберзлочинність діяння отримують належну криміналізацію, а процесуальні механізми щодо збирання та вилучення електронних доказів залишаються фрагментарними; у цьому зв’язку пріоритетного значення набуває системний

моніторинг виконання міжнародних зобов'язань та надання технічної допомоги державам у процесі імплементації.

Констатовано, міжнародні стандарти у сфері юридичної відповідальності за правопорушення у мережі Інтернет дедалі більше зміщуються у бік комплексного механізму шляхом поєднання відповідальності з просвітою користувачів, кібергігієною, партнерством з приватним сектором та повагою до відкритості мережі. Нові міжнародні документи та ініціативи мають шанс закріпити та розвинути зазначені принципи. Сьогодні міжнародні стандарти у сфері юридичної відповідальності за інтернет-правопорушення знаходяться в стадії динамічного розвитку, позаяк від фрагментарних регіональних норм вони еволюціонують до цілісної системи універсальних правил, що враховують як потребу у безпеці, так і необхідність збереження фундаментальних прав і свобод у цифрову епоху.

Визначено ключові характеристики юридичної відповідальності за правопорушення в мережі Інтернет: транснаціональний характер, оскільки переважна більшість правопорушень в мережі Інтернет виходять за межі національних юрисдикцій, що зумовлює складнощі у визначенні компетентного органу та виборі застосовного права; ускладнена ідентифікація суб'єкта, позаяк в умовах анонімності, використання псевдонімів, VPN-технологій, блокчейну та систем шифрування постає об'єктивна проблема встановлення особи правопорушника; комплексний характер складу правопорушення, адже правопорушення в мережі Інтернет поєднують технічні, поведінкові, інтелектуальні та інші елементи, що значно ускладнює правову кваліфікацію; множинність нормативного впливу, яка проявляється у взаємодії норм національного законодавства, міжнародно-правових стандартів, актів м'якого права та корпоративних політик цифрових платформ, що створює багаторівневу модель регулювання.

Репрезентовано класифікацію різновидів юридичної відповідальності за правопорушення в мережі Інтернет: вторинна (умовна) відповідальність,

яка стосується інтернет-провайдерів та адміністраторів онлайн-платформ та не передбачає безумовного обов'язку контролювати весь користувацький контент, однак зобов'язує реагувати на повідомлення про його протиправність від компетентних органів чи зацікавлених осіб; саморегуляторна відповідальність, що базується на внутрішніх правилах цифрових платформ і онлайн-спільнот, створює своєрідний рівень «квазізаконодавства» у цифровій сфері та забезпечує взаємодію користувачів, але водночас породжує низку проблем, зокрема, непрозорість алгоритмів, недостатність механізмів апеляції, вибірковість застосування стандартів та відсутність зовнішнього контролю.

Акцентовано, концепція подвійної легітимації саморегуляторної відповідальності за правопорушення у мережі Інтернет ґрунтується на визнанні ефективності внутрішніх правил платформ лише за умови їх відповідності двом взаємопов'язаним вимірам: внутрішньому (автономному), котрий передбачає, що спільнота користувачів сприймає правила як справедливі, прозорі та недискримінаційні, що забезпечується публічністю стандартів, доступністю процедур оскарження та гарантіями рівності у їх застосуванні; зовнішньому (міжнародно-правовому), відповідно до якого корпоративні політики узгоджуються з міжнародними стандартами у сфері прав людини, зокрема практикою ЄСПЛ та актами ЄС щодо свободи вираження поглядів, захисту персональних даних і протидії мові ворожнечі.

Колективна форма юридичної відповідальності у мережі Інтернет розглядається як реакція на складність атрибуції правопорушень, що виникають унаслідок взаємодії користувачів, адміністраторів платформ, розробників алгоритмів, хостинг-провайдерів тощо. У цьому контексті формується доктрина «розподіленої вини», яка передбачає покладення юридичних наслідків на сукупність учасників цифрової екосистеми.

Алгоритмічна (автоматизована) відповідальність пов'язана зі зростанням ролі штучного інтелекту та алгоритмів у процесі прийняття рішень. Її сутність полягає в необхідності вироблення особливих механізмів

юридичного реагування на делікти, що виникають внаслідок автономних рішень цифрових систем.

Множинна (гібридна) відповідальність, під якого варто розуміти комплексну форму правової реакції, яка виникає внаслідок поєднання транскордонної багатоюрисдикційності та взаємодії людського і алгоритмічного факторів у процесі вчинення правопорушення.

Сформульовано ознаки множинної (гібридної) відповідальності за правопорушення у мережі Інтернет: характеризується «подвійною атрибуцією», за якої деліктогенний результат одночасно є наслідком вольових рішень людини та автономних або напівавтономних дій цифрових систем; не зводиться до класичної індивідуалізації суб'єкта, а передбачає розподіл правових наслідків між кількома рівнями, зокрема, особою, яка ініціює чи контролює процес, оператором платформи, а також технічною інфраструктурою, що генерує правопорушний ефект; становить новий інститут загальної теорії права, що вимагає: а) формування критеріїв оцінки ступеня алгоритмічної автономії та меж людського контролю; б) перегляду традиційних категорій вини та необережності в умовах алгоритмізованого середовища; в) вироблення механізмів юрисдикційної координації для подолання колізій багатоярусного правозастосування.

Узагальнено усталені у правовій доктрині та міжнародній практиці різновидів правопорушень у мережі Інтернет:

1) за об'єктом посягання: правопорушення у сфері інформаційної безпеки (несанкціонований доступ до даних, злам інформаційних систем, поширення шкідливого програмного забезпечення); порушення персональних немайнових прав (кібербулінг, онлайн-образи, поширення недостовірної інформації, втручання у приватне життя); порушення прав інтелектуальної власності (піратство, нелегальне поширення цифрового контенту, несанкціоноване використання авторських творів); економічні правопорушення у кіберпросторі (шахрайство з використанням електронних платіжних систем, маніпуляції з криптовалютами, створення фінансових

пірамід у мережі); порушення регулятивних вимог цифрових платформ (порушення умов користування сервісами, зловживання алгоритмами, маніпуляція даними користувачів) тощо;

2) за способом здійснення (залежно від методів і технічних засобів): злом або несанкціонований доступ – правопорушення, котрі передбачають злом акаунтів, доступ до закритих інформаційних систем та злом захищених ресурсів; розповсюдження шкідливого програмного забезпечення – поширення вірусів, троянських програм та іншого шкідливого програмного забезпечення з метою завдання шкоди інформаційним системам; соціальна інженерія та фішинг – методи обману, що використовуються для отримання доступу до конфіденційної інформації шляхом маніпулювання довірою користувачів; шахрайські схеми з банківськими картками, інвестиційне шахрайство, а також різні фінансові незаконні операції в Інтернеті;

3) за принципом юрисдикційної належності (територіальною ознакою): національні правопорушення, що вчиняються всередині однієї держави; транскордонні правопорушення, які охоплюють кілька держав;

4) за рівнем суспільної небезпеки: кіберзлочини – тяжкі злочини, які завдають значної шкоди особам, організаціям та суспільству; адміністративні правопорушення у мережі Інтернет, що не несуть серйозної суспільної небезпеки, однак за їх вчинення можуть бути накладені адміністративні санкції.

Констатовано, аналіз правопорушень у кіберпросторі потребує врахування особливостей цифрового середовища, що відмежовують їх від класичних деліктів у межах традиційно усталеного розуміння, серед яких виокремлено наступні: 1) відсутність територіальної визначеності – одна і та сама протиправна дія може водночас зачіпати кілька держав та створювати феномен багатошарової юрисдикційності, що передбачає: а) юрисдикційну конкуренцію, коли декілька держав претендують на застосування власного права до одного і того ж делікту; б) правову лакунарність, оскільки відсутність єдиних стандартів створює ризик невідповідності національних

регулятивних норм; в) фрагментацію правозастосування, котра передбачає, що різні держави кваліфікують одні і ті самі дії по-різному, що перешкоджає уніфікованому реагуванню на глобальні кіберзагрози; 2) технологічна складність правопорушень у мережі Інтернет – їх вчинення та подальша ідентифікація ґрунтуються на застосуванні спеціальних знань у сфері програмування, криптографії, блокчейн-технологій, штучного інтелекту та інших високотехнологічних рішень; 3) дистанційність та віртуалізація дій; 4) анонімність та псевдоанонімність суб'єкта – анонімність у кіберпросторі має подвійний характер, позаяк забезпечує реалізацію права на приватність та свободу вираження поглядів і переконань, але одночасно створює правові прогалини, які активно використовуються правопорушниками для уникнення контролю та правозастосовних заходів; псевдоанонімність як проміжна форма маскування особи сприяє появі правової невизначеності щодо суб'єкта притягнення до юридичної відповідальності та має три ключові вектори: а) епістемологічний, позаяк ускладнює встановлення фактичних обставин і перешкоджає формуванню доказової бази; б) процесуальний, бо обмежує застосування класичних процедур переслідування, оскільки неможливо ідентифікувати конкретного носія деліктної поведінки; в) правоохоронний, що стимулює зростання кількості кіберделіктів через відчуття безкарності та мінімальні ризики для суб'єкта правопорушення; 5) масовість та колективний характер впливу правопорушень у мережі Інтернет; 6) розмитість об'єкта правопорушення у цифровому середовищі, котра передбачає відсутність матеріальної субстанційності, що ускладнює юридичну ідентифікацію шкоди, адже порушення нематеріальних прав не завжди можна виміряти у класичних економічних показниках; 7) варіативність правового регулювання у сфері Інтернет-правопорушень передбачає, що у цифровому середовищі на одне і те саме правопорушення можуть одночасно поширюватися різнорівневі регулятивні масиви, зокрема: а) норми національного законодавства, які визначають юрисдикційні межі та процесуальні механізми відповідальності; б) міжнародно-правові стандарти, що формують

універсальні гарантії прав людини та забезпечують транснаціональну координацію; в) інструменти soft law, у тому числі рекомендації міжнародних організацій, які хоч і не мають імперативного характеру, проте створюють стандарти належної поведінки у цифровому просторі; г) корпоративні політики онлайн-платформ, що фактично виконують функцію квазіправових норм та визначають правила поведінки для мільйонів користувачів; 8) транзитивність (перехідність), що може призвести до політичної дестабілізації через потенційні можливості впливу на виборчі процеси, національну безпеку та міжнародні відносини; 9) автоматизований характер, що передбачає розмитість суб'єктного складу; 10) високий рівень латентності, правова природа якої у сфері цифрових правопорушень має багатовимірний характер, позаяк: а) зумовлена технологічними особливостями Інтернету, які дозволяють правопорушникам приховувати сліди своєї діяльності; б) посилюється через інформаційну асиметрію між правопорушником та потенційною жертвою, оскільки потерпілі часто навіть не усвідомлюють факту посягання; в) в умовах швидкої глобалізації цифрових процесів традиційні інститути правозастосування виявляються неготовими до оперативного реагування, що створює часовий лаг між вчиненням правопорушення та його процесуальною фіксацією; 11) міждисциплінарний характер правопорушень у мережі Інтернет передбачає, що останні вимагають комплексного осмислення на перетині кількох галузей знань та передбачають: встановлення складу правопорушення, його кваліфікацію та визначення санкцій; необхідність глибокого розуміння алгоритмів, програмного забезпечення, технологій шифрування, блокчейну та інших цифрових інструментів, які використовуються як для вчинення, так і для приховування деліктів; пояснення закономірностей масової поведінки у віртуальному просторі, зокрема поширення кібербулінгу, фейкових новин чи деструктивних онлайн-спільнот; виявлення мотиваційних чинників правопорушників та специфіки сприйняття шкоди жертвами у ситуаціях, де

фізичний контакт відсутній, але психологічні наслідки є надзвичайно відчутними.

Встановлено, цифрові технології докорінно змінюють характер правопорушень і способи їх вчинення, розмивають межі юрисдикцій та створюють нові об’єкти та суб’єкти правовідносин. Наголошено, сам по собі розвиток цифрових технологій не «покращує» інститут відповідальності автоматично, навпаки, він виявляє його прогалини. Проте реагування на вказані виклики спонукає законодавця до оновлення правових рамок, що зрештою може удосконалити інститут юридичної відповідальності. У цьому ключі підкреслено наступне: цифрові інструменти виявляють і підсилюють прогалини чинного законодавства у сфері відповідальності; виникає нагальна потреба у переосмисленні критеріїв суб’єктності та атрибуції протиправної поведінки в умовах розподілених і анонімних систем; існує гострий дефіцит нормативного регулювання нових правових феноменів, що опосередковано впливають на зміст і форму юридичної відповідальності.

Наголошено, розгляд особливостей функціонування децентралізованих автономних організацій (далі – DAO) та смарт-контрактів засвідчив наявність глибокої концептуальної кризи традиційної моделі юридичної відповідальності у цифровому середовищі. Виявлено, що відсутність централізованого керівного органу в DAO, а також автоматизованість ухвалення рішень, значно ускладнюють можливість визначення суб’єкта відповідальності, а отже і реалізацію юридичної відповідальності як інституту. Саме тому у сучасній доктрині зростає інтерес до концепцій розподіленої, колективної або програмно зумовленої відповідальності, а також до моделі визнання DAO як окремого суб’єкта права.

Проаналізовані підходи у правовому полі Європейського Союзу, зокрема, в межах Регламенту MiCA, демонструють зародження доктрини юридичної відповідальності у сфері автоматизованих правочинів. У результаті проведеного аналізу констатовано: доктрина юридичної відповідальності

виявляє обмеженість при застосуванні до ситуацій, де немає чіткого людського волевиявлення, а дії є результатом виконання заздалегідь запрограмованого коду; залишається неусталеною позиція щодо правосуб'єктності DAO, що унеможливлює належне юридичне оформлення її відповідальності; чинне національне законодавство не враховує автономних характеристик блокчейн-середовища та не пропонує ефективних інструментів юридичного реагування у разі настання шкоди внаслідок дії смарт-контракту.

Наголошено, розвиток електронного урядування, онлайн-платформ та цифрових економічних відносин призводить до суттєвого зростання ризиків зловживання персональними даними. Відповідно, інститут юридичної відповідальності має адаптуватися до цих викликів шляхом: удосконалення процедур контролю за обробкою даних; підвищення рівня санкцій за порушення; запровадження превентивних правових засобів захисту.

Визначено, юридична відповідальність у сфері ШІ поступово набуває рис об'єктивної (суворої) відповідальності, подібної до моделі відповідальності за шкоду, завдану дефектною продукцією. У контексті цифрових технологій вказана відповідальність стає ефективним інструментом правового реагування на складні, технічно опосередковані випадки спричинення шкоди. Акцентовано, концепція відповідальності за ризик як альтернатива традиційному поняттю вини є перспективною парадигмою для оновлення інституту юридичної відповідальності. У сфері ШІ відповідальність повинна покладатися не на агента, що має волю та намір, а на суб'єкта, який створив або експлуатує джерело технологічного ризику.

Констатовано, доктринальна дискусія про статус «електронної особи» для ШІ, попри її теоретичну значущість, наразі не має правової реалізації, що підкреслює необхідність зосередження уваги не на фіктивній суб'єктності машин, а на побудові ефективної системи відповідальності фізичних і юридичних осіб, відповідальних за створення, навчання та функціонування

ШІ. Визнання правоздатності за системою, яка не має свідомості чи здатності до автономного морального вибору, створює ризик девальвації понять вини, наміру та справедливого покарання.

Визначено, становлення віртуального середовища як автономного цифрового простору призводить до трансформації уявлень про територіальну та персональну юрисдикцію, що унеможливлює застосування традиційних норм міжнародного приватного права без відповідної адаптації. Аргументовано, цифрові активи у вигляді невзаємозамінних токенів, віртуальної нерухомості та інших нематеріальних об'єктів набувають ознак майнової цінності та потребують правового режиму, подібного до інституту нематеріального майна у цивільному праві. Підкреслено, що моделі корпоративного (приватного) регулювання, засновані на правилах спільнот, не здатні забезпечити рівнозначний захист прав особи, порівняно з публічно-правовими механізмами, що обґрунтовує потребу державного втручання та встановлення загальнообов'язкових стандартів відповідальності у цифровому середовищі.

Визначено вектори розвитку інституту юридичної відповідальності у цифровому середовищі:

Фундаментальною передумовою є визначення юрисдикційних меж діяльності у метавсесвіті, оскільки простежується проблема відсутності територіальної прив'язки цифрових дій. Можливим шляхом розв'язання цієї прогалини є встановлення юрисдикції за місцем реєстрації оператора платформи або шляхом укладення міжнародної угоди про «електронну юрисдикцію», яка забезпечила б однакові стандарти для різних держав. Вказане створило б основу для правової визначеності та зменшило ризик колізій між національним законодавством держав.

Стратегічним напрямом удосконалення інституту юридичної відповідальності є криміналізація нових форм суспільно небезпечної поведінки, що виникають у віртуальних середовищах. Встановлено за доцільне, зокрема: 1) запровадити окрему кримінально-правову норму про

шахрайство з віртуальними активами, яка б визнавала їх специфічний правовий статус і враховувала економічну цінність цифрових об'єктів (криптовалют, NFT, токенів); обґрунтовано внесення змін до Кримінального кодексу України та суміжних нормативно-правових актів з метою закріплення спеціальних складів злочинів, пов'язаних із неправомірним використанням криптоактивів, серед яких: незаконне заволодіння віртуальними активами (крадіжка, шахрайство чи зловживання довірою у криптовалютному середовищі); відмивання коштів через криптовалюту, що становить одну з найбільш поширених практик використання блокчейн-технологій у кримінальних схемах; створення та функціонування фінансових пірамід із використанням токенів чи криптовалют, які завдають значної шкоди економічним інтересам громадян і держави; 2) встановити кримінальну відповідальність за кібербулінг у VR-середовищах та кваліфікувати його як різновид психологічного насильства, що здійснюється у віртуальному просторі із застосуванням аватарів та інтерактивних інструментів; 3) врегулювати посягання на віртуальну ідентичність користувача у вигляді створення фальшивих аватарів, викрадення або маніпуляції персоніфікованими даними у як окремий об'єкт кримінально-правової охорони; 4) розширити предмет кримінально-правового захисту шляхом включення до нього цифрових благ і нематеріальних об'єктів, що мають цінність у віртуальному середовищі.

Окремого вектору удосконалення інституту юридичної відповідальності потребує цивільно-правове (деліктне) регулювання шкоди, завданої у VR-, AR-середовищах та метаверсах. З метою забезпечення ефективності правового захисту запропоновано наступне: визнати віртуальну ідентичність користувача об'єктом цивільно-правової охорони, що дозволить застосовувати деліктні механізми у випадках неправомірного використання або викривлення образу аватара; розширити категорію майнової шкоди та включити до неї втрати, пов'язані з неправомірним використанням чи знеціненням віртуальних активів (криптовалюти, NFT, токенізованих

цифрових об’єктів), адже їх економічна вартість визнається як предмет цивільного обігу; зазначене, у свою чергу, розширить доктрину особистих немайнових прав та створить передумови для ефективного судового захисту від порушень, які нині здебільшого залишаються у «сірій зоні»; запровадити компенсацію моральної шкоди у випадках віртуального булінгу чи переслідування у VR-середовищах, що передбачає визнання, що психологічні наслідки таких дій можуть бути не менш значущими, ніж у традиційних офлайн-взаєминах; закріпити спеціальні презумпції причинного зв’язку у деліктних спорах щодо застосування ШІ, що дозволить зменшити тягар доказування для потерпілих, які стикаються з інформаційною асиметрією у відносинах із розробниками чи провайдерами технологій; забезпечити формування багаторівневої системи юридичної відповідальності, як власне передбачено міжнародними стандартами у досліджуваній сфері: первинна – за розробником і постачальником технології, вторинна – за інтегратором чи провайдером, і додаткова – за користувачем, який зловживає інструментами VR чи метаверсу; наведена модель відповідальності дозволить адекватно враховувати складність цифрових ланцюгів і мінімізувати ризик уникнення деліктної відповідальності через розмитість суб’єктного складу.

Акцентовано на важливості здійснення законодавчого встановлення спеціальних обов’язків провайдерів цифрових платформ, що функціонують у метавсесвіті. Серед них: ідентифікація користувачів із метою запобігання анонімному вчиненню правопорушень та забезпечення належного реагування у випадках шкоди; захист персональних даних відповідно до сучасних стандартів права ЄС з урахуванням принципів мінімізації, цільового використання та обмеження зберігання; гарантії безпеки неповнолітніх, що передбачають обмеження доступу до небезпечного контенту, застосування батьківського контролю та превентивні механізми протидії кібербулінгу; налагодження співпраці з правоохоронними органами, зокрема щодо обов’язкового інформування про випадки вчинення протиправних дій та забезпечення доступу до цифрових доказів.

Визначено за доцільне впровадження так званої «структурної відповідальності» провайдерів, яка передбачає їх обов'язок запобігати правопорушенням через архітектуру платформи та алгоритми модерації. Її сутність полягає у зміщенні акценту з реактивного позиціювання, відповідно до якого провайдери зобов'язані тільки усувати наслідки правопорушень, на превентивний, що передбачає створення такої архітектури платформи та алгоритмів модерації, які мінімізують імовірність вчинення протиправних дій. Відповідальність провайдерів за таких умов набуває організаційно-превентивного характеру, оскільки вони стають зобов'язаними враховувати потенційні ризики правопорушень уже на етапі проектування цифрового середовища.

Розвиток інституту юридичної відповідальності у метавсесвіті передбачає застосування концепції «цифрового делікту» як окремої категорії правопорушення, що вимагає нормативного оформлення, виникає виключно у віртуальному середовищі та має низку специфічних рис, що відрізняють його від класичних правопорушень: а) характеризується нематеріальністю об'єкта посягання; якщо у традиційному деліктному праві предметом захисту є майнові або немайнові блага, що мають чітко визначену матеріальну чи соціальну природу, то у метавсесвіті об'єктом може виступати віртуальна ідентичність, цифровий аватар, віртуальний актив чи репутація у VR-просторі; відтак постає завдання доктринального визнання таких об'єктів як самостійних цінностей, що підлягають юридичній охороні; б) суттєвою ознакою цифрового делікту є його транскордонний характер – діяльність у метавсесвіті апріорі виходить за межі юрисдикції однієї держави, а тому правопорушення у віртуальному середовищі не може бути належним чином врегульоване винятково національним законодавством, що потребує вироблення уніфікованого розуміння на рівні міжнародного права, а також механізмів взаємного визнання юрисдикції та співпраці держав у сфері цифрової відповідальності; в) особливість анонімності суб'єкта – використання технологій шифрування, анонімізаторів, блокчейн-мереж та

аватарів у VR-середовищах значно ускладнює ідентифікацію правопорушників, що вимагає перегляду традиційних доктринальних положень щодо суб'єктного складу правопорушення та запровадження нових механізмів ідентифікації, які водночас не повинні порушувати права на приватність.

Запропоновано наступне визначення досліджуваному поняттю: цифровий делікт – це протиправне винне діяння, що здійснюється у віртуальному середовищі і характеризується нематеріальністю об'єкта посягання, транскордонністю юрисдикції та ускладненою ідентифікацією суб'єкта, внаслідок чого завдається шкода майновим чи немайновим правам особи, а також суспільним інтересам, які підлягають правовій охороні.

Встановлено, ще одним напрямом розвитку інституту юридичної відповідальності у цифровому середовищі є нормативне визначення критеріїв відповідальності за автономні рішення, що приймаються із застосуванням систем штучного інтелекту. У сферах медицини, транспорту, фінансів автономні технології дедалі частіше використовуються для ухвалення рішень, однак чинне законодавство не визначає меж відповідальності людини у випадках їх застосування. Доцільним є закріплення правила, відповідно до якого використання автоматизованої системи не звільняє оператора від юридичної відповідальності, якщо тільки не буде доведено виняткових обставин, наприклад, технічного збою чи форс-мажору.

Визначено за доцільне запровадження системи безперервного навчання суддів та слідчих щодо особливостей роботи з цифровими доказами, методів встановлення причинно-наслідкового зв'язку у випадках алгоритмічних рішень, а також стандартів оцінки надійності програмних продуктів і цифрової інфраструктури. Інвестиції у людський капітал правосуддя сьогодні постають як ключова умова ефективного розвитку інституту юридичної відповідальності у цифрову епоху, позаяк сприятимуть зниженню інформаційної асиметрії між технологічними компаніями та органами правосуддя, забезпечать можливість якісного розслідування новітніх

правопорушень та підвищать довіру суспільства до спроможності держави гарантувати захист прав у цифровому середовищі.

Наголошено, Україна повинна посилити участь у діючих міжнародних механізмах та ініціювати нові форми співробітництва, спрямовані на забезпечення невідворотності відповідальності незалежно від місця вчинення правопорушення. Розвиток міжнародної співпраці у сфері притягнення до відповідальності за правопорушення у мережі Інтернет є необхідною умовою формування дієвого механізму захисту прав у цифрову епоху. Лише за умови поєднання національних і міжнародних інструментів можна досягти належного рівня правової визначеності та забезпечити принцип невідворотності відповідальності за правопорушення у кіберпросторі.

Окремим напрямом розвитку інституту юридичної відповідальності є використання цифрових технологій як інструментів підсилення механізмів притягнення до відповідальності. Сучасні інтелектуальні системи здатні виконувати превентивні та доказові функції, що значно підвищує ефективність правозастосування. Водночас впровадження таких систем потребує належного правового врегулювання, зокрема забезпечення гарантій дотримання прав людини та фундаментальних свобод, а також принципів пропорційності, необхідності та законності при застосуванні алгоритмічних інструментів у діяльності правоохоронних органів та судів.

Визначено доцільним закріплення принципів цифрової етики у правовій площині з метою їх трансформації у юридично значущі регулятори поведінки, що дозволить узгодити вимоги, які висуває суспільство до етичності функціонування віртуальних спільнот, із нормативними приписами, що забезпечуються державним примусом. Підкреслено, йдеться не про підміну права етикою, а про взаємодію двох систем регуляції, де етичні стандарти виконують роль методологічної основи для створення нових правових норм у сфері цифрових відносин.

Визначено доктринально обґрунтованою необхідність розробки та ухвалення спеціального закону «Про штучний інтелект». У зазначеному

нормативному акті мають бути чітко визначені критерії відповідальності суб'єктів: розробника, якщо шкода спричинена дефектом алгоритму, впроваджувача у разі неналежного впровадження системи у виробничий процес, користувача за умови неправомірного або необережного застосування технології тощо. Наголошено, принципово важливим є закріплення норми, згідно з якою системи штучного інтелекту не визнаються самостійними носіями прав і обов'язків, а отже, відповідальність завжди покладається на визначених фізичних або юридичних осіб.

Встановлено, Проєкт Закону України «Про штучний інтелект» повинен передбачати такі структурні елементи: Розділ I. Загальні положення; Розділ II. Класифікація систем штучного інтелекту за рівнем ризику; Розділ III. Вимоги до створення, впровадження та використання систем штучного інтелекту; Розділ IV. Юридична відповідальність за використання систем штучного інтелекту; Розділ V. Інституційне забезпечення функціонування систем штучного інтелекту; Розділ VI. Прикінцеві та перехідні положення.

Репрезентовано ключові положення кожної з структурних частин запропонованого законопроєкту. У розділі I «Загальні положення» слід: 1) визначити предмет і мету закону, які полягатимуть у встановленні єдиних засад правового регулювання функціонування штучного інтелекту, а також у забезпеченні гармонійного поєднання технологічного прогресу з охороною основоположних прав і свобод людини; 2) закріпити базові терміни, зокрема «штучний інтелект», «система високого ризику», «оператор», «розробник», «постачальник», а також основні принципи відповідальності – ризик, сувора відповідальність, стандарти належної обачності. У розділі II доцільно передбачити класифікацію систем штучного інтелекту за рівнем ризику та розрізняти системи низького, обмеженого, високого та неприпустимого ризику. Критеріями такого поділу повинні стати сфера застосування (медицина, транспорт, безпека, правосуддя), масштаб потенційної шкоди та рівень вразливості користувачів. У розділі III слід закріпити загальні та спеціальні вимоги до систем ШІ, зокрема, прозорість алгоритмів, захист

персональних даних і приватності, а також гарантування можливості людського нагляду. Для високоризикових систем відповідно до міжнародних стандартів варто запровадити додаткові вимоги, до яких доцільно віднести обов'язковий аудит, реєстрацію у державному реєстрі, сертифікацію відповідності та впровадження механізмів постійного моніторингу ризиків. Четвертий розділ повинен містити положення про те, що відповідальність у сфері штучного інтелекту ґрунтується на ризику, а не на намірі системи, а суб'єктами відповідальності є розробники, оператори, постачальники та користувачі. Важливим елементом повинен стати інститут суворої відповідальності за шкоду, завдану високоризиковими системами життю, здоров'ю чи майну осіб. У таких випадках власник або оператор повинен нести відповідальність незалежно від вини. Для операторів та користувачів повинні бути встановлені стандарти належної обачності, порушення яких є підставою для відповідальності. У цьому ж розділі доцільно передбачити перелік заборонених систем, що створюють неприпустимий ризик, серед яких маніпуляція свідомістю, тотальне стеження тощо. П'ятий розділ повинен передбачити створення національного органу з нагляду за штучним інтелектом, до повноважень якого належатиме реєстрація, аудит, контроль, застосування санкцій, а також взаємодія з європейськими та міжнародними структурами. Важливим елементом у цьому ключі стане державний реєстр високоризикових систем, який має бути публічним і забезпечувати доступ громадян до інформації. Визначено за доцільне запровадження обов'язкового страхування цивільної відповідальності для операторів високоризикових систем. У прикінцевих та перехідних положеннях слід передбачити поетапне впровадження закону: а) на першому етапі (протягом року) створення наглядового органу; б) на другому (протягом двох років) запровадження державного реєстру та процедур сертифікації; в) на третьому (протягом трьох років) повне набрання чинності положеннями про відповідальність і страхування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Адміністративне право: підручник / Ю.П. Битяк, І.М. Балакарєва, І.В. Бойко, В.М. Гаращук [та 22 інших]; за загальною редакцією Ю.П. Битяка; Міністерство освіти і науки України, Національний юридичний університет імені Ярослава Мудрого. Харків: Право, 2020. 390 с.

2. Арістотель. Політика. Київ : Основи, 2005. 240 с.

3. Балинська О. М., Ященко В. А. Принципи діалектики та метафізики (формальної логіки) у праві. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична*. 2017. № 3. С. 259–268.

4. Балинська О. М., Ященко В. А. Синергетика як методологічна парадигма юридичних досліджень. *Науковий вісник Львівського державного університету внутрішніх справ. серія юридична*. 2017. №4. С. 3–12.

5. Бандура О. О. Єдність цінностей та істини у праві : монографія. Київ : НАВСУ, 2000. 200 с.

6. Басін К. В. Юридична відповідальність: природа, форми реалізації та права людини : дис. … канд. юрид. наук : 12.00.01. Київ. 2006. 214 с.

7. Безклубий І. Правова відповідальність. *Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки.* 2012. № 91. С. 8–10.

8. Безпека як потреба людства. Вступ до кібербезпеки. 2023. URL: https://research.kr-labs.com.ua/introduction-to-cybersecurity/ (дата звернення: 17.01.2024).

9. Биков О. М., Савченко В. В. Захист персональних даних у сучасному законодавстві. *Legal Bulletin*. 2024. №4(14). С. 67–72. https://doi.org/10.31732/2708-339X-2024-14-A9

10. Блокчейн і Метавсесвіт: правові аспекти / О.В. Костенко, О.Е. Радутний. *Юридичний науковий електронний журнал*. 2022. № 9. С. 499–506.

11. Бутузов В. Системно-структурний аналіз як метод дослідження протидії комп’ ютерній злочинності. *Правова інформатика*. 2011. № 1. С. 67–71.

12. Васильковский І. І. Поняття, класифікація та характеристика окремих видів кіберзлочинів. *Прикарпатський юридичний вісник*. Випуск 1(16), том 2. 2017. С. 196–201. URL: http://www.pjv.nuoua.od.ua/v1-2_2017/44.pdf

13. Голишева О. С. Смарт-контракти у договірних відносинах. *Літописець*. 2024. № 19. С. 58–62.

14. Гуренко М. М. Розвиток національно-правової думки про гарантії прав і свобод людини і громадянина : монографія. Київ : Логос, 2002. 252 с.

15. Демиденко Г. Сократ. Велика українська юридична енциклопедія : в 20 т. Харків Право, 2017. Т. 2 . Філософія права. С. 782–784.

16. Директива 2000/31/ЄС Європейського парламенту та Ради Про деякі правові аспекти інформаційних послуг, зокрема, електронної комерції, на внутрішньому ринку («Директива про електронну комерцію») від 8 червня 2000 року. URL: https://zakon.rada.gov.ua/laws/show/994_224#Text (дата звернення: 24.01.2024).

17. Директива 2011/93/ЄС Європейського Парламенту та Ради (переклад українською мовою). 2023. URL: https://jurfem.com.ua/dyrektyva-2011-92-eu-pereklad/ (дата звернення: 31.01.2024).

18. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп’ютерні системи. URL: https://zakon.rada.gov.ua/laws/show/994_687#Text (дата звернення: 07.02.2024).

19. Донеллі Дж. Права людини у міжнародній політиці. Львів : Світ, 2004. 280 с.

20. Європейський словник філософії: Лексикон неперекладностей / під кер. Б. Кассен. Київ : Дух і Літера, 2009. Т. 1. 576 с.

21. Жорнокуй Ю. М. Штучний інтелект: питання відповідальності на сучасному етапі розвитку доктрини. *Forum Prava*. 2024. № 2. С. 118–127.

22. З серпня набув чинності AI Act – перший закон про штучний інтелект в ЄС. 2024. URL: https://iaa.international/publication/z-serpnia-nabuv-chinnosti-ai-act--pershii-zakon-pro-shtuchnii-intelekt-v-es (дата звернення: 10.09.2024).

23. Загальна теорія держави і права: [Підручник для студентів юридичних вищих навчальних закладів] / М. В. Цвік, О. В. Петришин, Л. В. Авраменко та ін.; За ред. д-ра юрид. наук, проф., акад. АПрН України М. В. Цвіка, д-ра юрид. наук, проф., акад. АПрН України О. В. Петришина. Харків: Право, 2009. 584 с.

24. Загребельна Н. А. Поширення юридичної відповідальності за правопорушення в мережі Інтернет в умовах воєнного стану в Україні. *Електронне наукове видання «Аналітично-порівняльне правознавство»*. 2023. № 2. С. 28–32. https://doi.org/10.24144/2788-6018.2023.02.4

25. Загребельна Н.А., Дубовой А.С. Теоретичні аспекти визначення змісту юридичної відповідальності в системі права. *Legal Bulletin*. Київ, 2023. № 2 (8). С. 17–23. DOI https://doi.org/10.31732/2708-339X-2023-08-17-23.

26. Інститут юридичної відповідальності у демократичних правових системах : монографія / за заг. ред. Н. М. Оніщенко. Київ: Юрид. думка, 2009. 216 с.

27. Кельман М. С. Загальна теорія держави і права / М. С. Кельман, О. Г. Мурашин. Київ: Кондор, 2006. 477 с.

28. Коваленко А. Класифікація електронних (цифрових) слідів кримінального правопорушення. *Проблеми законності*. 2023. № 161. С. 202–214. DOI:10.21564/2414-990X.161.278117

29. Кодекс України про адміністративні правопорушення. URL: https://zakon.rada.gov.ua/laws/show/80731-10#n4217 (дата звернення: 14.02.2024).

30. Колич О. І. Детермінанти діалектики у праві: окремі аспекти. *Вісник ЛТЕУ. Юридичні науки*. 2018. № 7. С. 45–51. 2616-7611-2018-07-05.pdf

31. Колюх В. Інститут конституційної скарги як засіб правового захисту прав і свобод людини і громадянина. 2022. https://web.ccu.gov.ua/sites/default/files/prava_lyudyny_ta_publichne_vryaduvannya_v_suchasnyh_umovah_2022.pdf#page=12 (дата звернення: 17.04.2024).

32. Конвенція ООН проти транснаціональної організованої злочинності 2000 р. URL: https://zakon.rada.gov.ua/laws/show/995_789#Text (дата звернення: 21.02.2024).

33. Конвенція про запобігання геноциду та покарання за нього 1948 р. URL: https://zakon.rada.gov.ua/laws/show/995_155#Text (дата звернення: 28.02.2024).

34. Конвенція про кіберзлочинність: міжнародний документ від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 06.03.2024).

35. Конвенція Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних». Страсбург. 1981. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 13.03.2024).

36. Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства. URL: https://zakon.rada.gov.ua/laws/show/994_927#Text (дата звернення: 20.03.2024).

37. Конституція України : Закон України від 28 червня 1996 р. № 254к/96-ВР. *Відомості Верховної Ради України (ВВР)*. 1996. № 30. Ст. 141. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 07.07.2024).

38. Корабльова Н. С. Законність і справедливість у державному управлінні: читаючи Платона. *Теорія та практика державного управління.* 2010. Вип. 1. С. 3–14. URL: http://nbuv. gov. ua/UJRN/Tpdu_2010_1_3.

39. Корольова В.В., Чорна В.О. Поняття та сутність ІТ-права як галузі права. *Legal Bulletin*. 2025. № 1(15). С. 77–81. https://doi.org/10.31732/2708-339X-2025-15-A11

40. Кримінальний Кодекс України. *Відомості Верховної Ради України (ВВР)*. 2001. № 25–26. Ст. 131. URL: https://zakon.rada.gov.ua/laws/show/2341-14/ed20241101 (дата звернення: 07.07.2025).

41. Кудь О. О., Кучерявенко М. П., Смичок Є. М. Цифрові активи та їх правове регулювання у світі розвитку технології блокчейн : монографія. Харків : Право, 2019. 216 с.

42. Куйбіда В., Карпенко О., Наместнік В. Цифрове врядування в Україні: базові дефініції понятійно-категоріального апарату. *Вісник Національної академії державного управління при Президентові України. Серія: Державне управління*. 2018. № 1. С. 5–10. URL: https://org2.knuba.edu.ua/pluginfile.php/71367/mod_resource/content/1/%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F.pdf (дата звернення: 07.07.2025).

43. Машков А. Обґрунтування доцільності двохаспектного погляду на юридичну відповідальність для сучасної правової науки. Про українське право. Часопис кафедри теорії та історії держави і права Київ. нац. ун-ту імені Тараса Шевченка / За ред. проф. І. Безклубого. Київ, 2010. Част. V. С. 74–85.

44. Міжнародна конвенція про ліквідацію расової дискримінації 1965 р. URL: https://zakon.rada.gov.ua/laws/show/995_105#Text (дата звернення: 27.03.2024).

45. Мікічурова О. В. Африканська система та механізми захисту прав людини. *Dictum Factum*. № 2 (7). 2020. С. 80–86.

https://df.duit.in.ua/index.php/dictum/article/view/154/132 (дата звернення: 07.07.2025).

46. Міхровська М. Цифрова термінологія в публічному управлінні: від оцифровування до цифрового урядування. *Юридичний науковий електронний журнал*. № 6. 2021. С. 142–144. DOI https://doi.org/10.32782/2524-0374/2021-6/38

47. Неволя В. В. Інтерпол та Європол: співвідношення діяльності міжнародних організацій в боротьбі з організованою злочинністю. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2011. № 24. С. 15–20.

48. Некіт К. Г. Віртуальні активи як різновид цифрових речей. *Часопис цивілістики*. 2022. № 45. С. 53–57. DOI:10.32837/chc.v0i45.466

49. Овчаренко А. С., Полатай В. Ю. Криптовалюта в системі міжнародного приватного валютного права. Щодо окремих питань оподаткування віртуальних активів в Україні. *Recht der Osteuropäischen Staaten (ReOS) (Право країн Східної Європи)*. 2018. № 4. С. 15–162.

50. Олейник А. Етичні феномени соціальних мереж: мова ворожнечі, кіберненависть та кібербулінг. *Вісник Львівського університету. Серія філос.-політолог. студії*. 2022. № 42. С. 118–124. DOI: https://doi.org/10.30970/PPS.2022.42.15

51. Організація Об'єднаних Націй ухвалила новаторський Пакт майбутнього з метою трансформації глобального управління. 2024. URL: https://surl.li/ednzpc (дата звернення: 03.04.2024).

52. Орлов Ю. Ю., Джужа О. М., Орлова О. Ю. Синергетика та пізнання правових явищ. *Науковий вісник Національної академії внутрішніх справ*. 2014. № 1. С. 75–90.

53. Палій А. Закони майбутнього: чого чекати від регулювання метавсесвіту. *Юридична газета онлайн*. URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/zakoni-maybutnogo-chogo-chekati-vid-regulyuvannya-metavsesvitu-

.html#:~:text=%D0%9F%D1%80%D0%BE%D1%82%D0%B5%20%D1%94%20%D1%96%20%D0%B2%D0%B8%D0%BD%D1%8F%D1%82%D0%BA%D0%B8,%D0%BA%D0%BE%D0%BC%D1%83 . (дата звернення: 10.04.2024).

54. Панишко Г. Змістова характеристика міжнародної міжурядової організації кримінальної поліції Інтерпол. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2022. № 2 (13). С. 16–28.

55. Платон. Держава / Пер. з давньогр. Д. Коваль. Київ : Основи, 2000. 355 с.

56. Прийма С. В. Справедливість при тлумаченні права: огляд аспектів. *Вісник Національної академії правових наук України*. 2016. № 4. С. 66–76.

57. Про віртуальні активи: Закон України. *Відомості Верховної Ради України (ВВР)*. 2023. № 15. Ст. 51 (не набрав чинності). https://zakon.rada.gov.ua/laws/show/2074-20#Text (дата звернення: 17.12.2024).

58. Про захист персональних даних: Закон України. *Відомості Верховної Ради України (ВВР)*. 2010. № 34. Ст. 481. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 17.04.2024).

59. Про медіа: Закон України. *Відомості Верховної Ради України (ВВР)*. 2023. №№ 47–50. Ст. 120. URL: https://zakon.rada.gov.ua/laws/show/2849-20#Text (дата звернення: 17.04.2024).

60. Про основні засади забезпечення кібербезпеки України: Закон України. *Відомості Верховної Ради (ВВР)*. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 17.04.2023).

61. Про охорону дитинства: Закон України. *Відомості Верховної Ради України (ВВР)*. 2001. № 30. Ст. 142. URL: https://zakon.rada.gov.ua/laws/show/2402-14#Text (дата звернення: 17.08.2025).

62. Проблеми правової відповідальності: монографія / Ю. П. Битяк, Ю. Г. Барабаш, Л. М. Баранова та ін.; за ред. В. Я. Тація, А. П. Гетьмана, В. І. Борисової. Харків : Право, 2014. 348 с.

63. Рабінович П. М. Основи загальної теорії права та держави : навч. посіб. Вид. 6-те. Харків : Консум, 2002. 160 с.

64. Рамкова конвенція Ради Європи про штучний інтелект: перемога чи поразка? URL: https://dslua.org/publications/ramkova-konventsiia-rady-yevropy-pro-shtuchnyy-intelekt-peremoha-chy-porazka/ (дата звернення: 17.04.2024).

65. Регламент Європейського Парламенту і Ради ЄС 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 24.04.2024).

66. Резолюція ООН 65/230. 2011. URL: https://www.unodc.org/documents/justice-and-prison-reform/AGMs/A_RES_65_230r.pdf (дата звернення: 01.05.2024).

67. Ришкова О. В. Юридичні засоби захисту прав інтелектуальної власності. *Наукові праці Одеської національної юридичної академії.* 2005. Т. 4. С. 235–242.

68. Сабадаш В. П. Фішинг як найбільш розвинений вид шахрайства в Інтернеті. *Університетські наукові записки*. 2006. № 1. С. 228–233.

69. Сіроштан Ю. В. Функції юридичної відповідальності: загальнотеоретична характеристика. *Юридичний науковий електронний журнал*. 2016. № 4. С. 18–21.

70. Скоморовський В. Б., Корольова В. В. Міжнародні стандарти регулювання юридичної відповідальності за правопорушення в Інтернеті. *Актуальні питання у сучасній науц*і. 2025. № 12 (42). С. 1411–1419. https://doi.org/10.52058/2786-6300-2025-12(42)-1411-1419

71. Скоморовський В.Б., Корольова В.В. Теоретико-правові засади формування складу правопорушень у мережі Інтернет. *Наукові інновації та передові технології*. 2025. № 12 (52). Серія «Право». С. 2903–2912.

72. Скоморовський В.Б., Степаненко Н.В. Український досвід розвитку наукових підходів до інституту юридичної відповідальності у сфері Інтернет-правопорушень. *Науковий вісник УжНУ*. Серія «Право». 2025. Випуск 92. С. 138–144. https://doi.org/10.24144/2307-3322.2025.92.1.19

73. Спасова К. І. Відшкодування моральної шкоди при порушенні немайнових прав у соціальних мережах: автореф. дис. на здоб. наук. ступ. канд. юр. наук. Спеціальність 12.00.03 – цивільне право та цивільний процес; сімейне право; міжнародне приватне право. 2021. URL: https://dspace.onua.edu.ua/server/api/core/bitstreams/af61ad48-8baf-4312-80b5-72c5638e31a3/content (дата звернення: 15.05.2024).

74. Статут ООН. Ред. Від 16.09.2005. URL: https://zakon.rada.gov.ua/laws/show/995_010#Text (дата звернення: 22.05.2024).

75. Степаненко Н.В., Махно М.І. Особливості правового захисту інтелектуальної власності в мережі Інтернет. *Legal Bulletin*. 2024. № 3(13). С. 72–78. https://doi.org/10.31732/2708-339X-2024-13-A10

76. Степаненко Н.В., Піддубний Д.Д. Сучасні проблеми запобігання і протидій злочинності у сфері інформаційних технологій. *Legal Bulletin*. 2024. № 4(14). С. 73–80. https://doi.org/10.31732/2708-339X-2024-14-A10

77. Суперечлива угода. Чому навколо конвенції ООН про кіберзлочинність точаться тривалі суперечки. URL: https://netfreedom.org.ua/article/superechliva-ugoda-chomu-navkolo-konvenciyi-oon-pro-kiberzlochinnist-tochatsya-trivali-superechki? (дата звернення: 29.05.2024).

78. Теорія держави і права : навч. посіб. для підгот. фахівців з інформ. безпеки / [О. О. Тихомиров, М. М. Мікуліна, Ю. А. Іванов та ін.] ; за заг. ред. Л. М. Стрельбицької. Київ : Кондор-Видавництво, 2016. 332 с.

79. Тєтєвін М. С., Хорватова О. О. З історії питання міжнародно-правового розуміння кіберпростору. *Часопис Київського ун-ту права*. 2022. №2–4. С. 22–25.

80. Тихомиров О. О. Інформаційні правопорушення: теоретико-правова концепція держави. *Інформаційна безпека людини, суспільства, держави*. 2015. №. 1 (17). С. 38–47. https://www.academia.edu

81. Ткачук Б. П. Класифікація «ботів», які використовуються у соціальних мережах для протидії розслідуванню кримінальних правопорушень: *Матеріали IX Міжнародної науково-практичної конференції «Малиновські читання».* 2021. С. 94–95.

82. У Європейському Союзі в четвер, 1 серпня, набув чинності закон, що регулюватиме правила у сфері штучного інтелекту (Artificial Intelligence Act). 2024. URL: https://www.ukrinform.ua/rubric-world/3891086-u-evrosouzi-nabuv-cinnosti-persij-u-sviti-zakon-pro-stucnij-intelekt.html (дата звернення: 05.02.2025).

83. У ЄС набув чинності Акт про цифрові послуги – він зобов'язує інтернет-платформи видаляти шкідливий контент. 2023. URL: https://zmina.info/news/u-yes-nabuv-chynnosti-akt-pro-czyfrovi-poslugy-vin-zobovyazuye-internet-platformy-vydalyaty-shkidlyvyj-kontent/ (дата звернення: 12.06.2024).

84. Україна у партнерстві з Канадою та УНЗ ООН розпочинає новий проєкт з посилення протидії та запобігання кіберзлочинності в Україні. 27 травня 2025 р. URL: https://surl.li/obfmhi (дата звернення: 23.06.2025).

85. Факультативний протокол до Конвенції ООН про права дитини 2000 р. щодо торгівлі дітьми і дитячої порнографії. URL: https://zakon.rada.gov.ua/laws/show/995_b09#Text (дата звернення: 26.06.2024).

86. Харитонов Є., Харитинова О. Юридична відповідальність: пошук парадигми. *Про українське право*. 2010. № 5. С. 23-30.

87. Ховпун О. Блокчейн у праві. *Proceedings of the eleventh international scientific-practical conference Internet-Education-Science.* Vinnytsia. 22–25 May. 2018. С. 33–34.

88. Худолєй Я. Г. Деякі аспекти юридичної відповідальності за правопорушення в мережі Інтернет. *Діяльність органів публічної влади*

України в умовах війни: пошуки оптимальних моделей: матеріали міжнародної правової школи (м. Ужгород, 11 травня 2023 р.). Ужгород. 2023. С. 36–38.

89. Худолєй Я. Г. Інтерпретація юридичної відповідальності в умовах глобалізації та цифровізації. *Наукові інновації та передові технології*. 2025.

№ 4 (44). С. 1829–1835.

90. Худолєй Я. Г. Класифікаційно-функціональні характеристики юридичної відповідальності у мережі Інтернет. *Актуальні питання у сучасній науці*. 2025. №. 4 (34). С. 909–914.

91. Худолєй Я. Г. Методологічні орієнтири дослідження юридичної відповідальності в умовах інформаційного суспільства. *Українська жінка в умовах війни: міждисциплінарний дискурс: матеріали міжнародної правової школи, м. Ужгород, 28 березня 2025 р*. Ужгород: Ужгородський національний університет. 2025. С. 81–83.

92. Худолєй Я. Г. Міжнародна операція «Black Axe» та юридична відповідальність за кіберзлочини. *Реалізація конституційного права на свободу пересування в умовах війни: правові стандарти та практичні можливості: матеріали міжнародної правової школи (м. Ужгород, 24 лютого 2023 р.)*. Ужгород. 2023. С. 36–38.

93. Худолєй Я. Г. Міжнародне співробітництво у сфері правопорушень в мережі Інтернет. *Міжнародний фактор перемоги України над московією: правові, інституційні, матеріально-технічні складові матеріали міжнародної правової школи (м. Ужгород, 2 червня 2023 р.)*. Ужгород. 2023. С. 32–35.

94. Худолєй Я. Г. Особливості множинної (гібридної) відповідальності за правопорушення у мережі Інтернет. *Collection of Scientific Papers with the Proceedings of the 3rd International Scientific and Practical Conference «Modern Problems of Science and Technology» (September 22–24, 2025, Tallinn, Estonia)*. European Open Science Space. 2025. С. 75–77.

95. Худолєй Я. Г. Поняття та правовий статус кіберпростору у міжнародному праві. *Наука і техніка сьогодні*. 2025. №. 4 (45). С. 283–291.

96. Худолєй Я. Г. Цифрова термінологія у міжнародно-правовій площині. *Правові проблеми мобільності в умовах надзвичайних режимів: конституційні, економічні, соціальні, культурні та духовні аспекти: матеріали міжнародної правової школи, м. Ужгород, 27 лютого 2025 р.* Ужгород: Ужгородський національний університет. 2025. С. 67–73.

97. Цивільний кодекс України. *Відомості Верховної Ради України (ВВР)*. 2003. №№ 40–44. Ст. 356. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення: 01.10.2025).

98. Чи відповідає міжнародним стандартам захист персональних даних в Україні? 2021. URL: https://gurt.org.ua/news/informator/66213/ (дата звернення: 24.04.2024).

99. Чуб А.В., Карпічков В.О. Міжнародні аспекти правового регулювання Інтернету. *Наука і техніка сьогодні.* 2025. Випуск № 13 (54). С. 364–371

100. Чуб А.В., Карпічков В.О. Нормативне забезпечення функціонування мережі Інтернет. *Legal Bulletin*. 2025. № 4(18) С. 96–102. DOI 10.31732/2708-339X-2025-18-A12

101. Чуб А.В., Карпічков В.О. Юридична відповідальність у кіберпросторі: аналіз зарубіжних доктрин. *Економіка. Фінанси. Право*. 2026. № 1. С. 55–57

102. Штучний інтелект і закон: хто відповідає, коли машини роблять помилки? *Судовий репортер*. URL: https://surl.li/zkxxuf (дата звернення: 17.05.2025).

103. Штучний інтелект: правове регулювання – матеріали Школи суддів (HSA), 2023. URL: https://surl.lt/dadesb (дата звернення: 07.08.2024).

104. Якімець І., Рудавська А. Кіберзлочинність: особливості та проблеми боротьби. https://fpk.in.ua/images/biblioteka/4bac_finan/innovatsiyi-na-rynku-finansovykh-posluh.pdf#page=313 (дата звернення: 24.05.2025).

105. A guide to the Digital Services Act, the EU's new law to rein in Big Tech. 2023. URL: https://algorithmwatch.org/en/dsa-explained/ (date of application: 14.08.2024).

106. Abbot R., Borges G., Dacoronia E., Devillier N., Jankowska-Augustyn M., Karner E., et al. Liability for Artificial Intelligence and other emerging digital technologies. Report from the Expert Group on Liability and New Technologies Formation. 2019. URL: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2020/01-09/AI-report_EN.pdf (date of application: 21.08.2024).

107. Afina Y. et al. Towards a global approach to digital platform regulation. *Chatham House*, 2024. URL: https://www.chathamhouse.org/2024/01/towards-global-approach-digital-platform-regulation/04-establishing-global-frameworks (date of application: 28.08.2024).

108. African Union Convention on Cyber Security and Personal Data Protection. URL: https://au.int/en/treaties/ african-union-convention-cyber-security-and-personal-data-protection (date of application: 04.09.2024).

109. Almada M. The EU AI Act: Between the rock of product safety and the hard place of fundamental rights. *Common Market Law Review*. 2025. Vol. 62. № 1. 2025. P. 85–120.

110. Alon-Barkat S., Busuioc M. Human–AI interactions in public sector decision making: «automation bias» and «selective adherence» to algorithmic advice. *J Public Adm Res Theory*. 2022. №33 (1). P. 153–169.

111. Annas J. Epicurus on pleasure and happiness. *Philosophical Topics*. 1987. №15 (2). P. 5–21.

112. Annex III: Group of Governmental Experts on Cyber-Crime (OAS). URL: https://www.oas.org/en/sla/dlc/cyber-en/grupo-trabajo.asp (date of application: 11.09.2024).

113. APEC Privacy Framework. Asia-Pacific Economic Cooperation, 2005. URL: https://www.apec.org/docs/default-

source/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf (date of application: 18.09.2024).

114. Application of international law to states conduct in cyberspace: UK statement Published 3 June 2021. URL: https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement#:~:text=cyber%20capabilities%2C%20subject%20to%20any,using%20such%20information%20technology%20infrastructures (date of application: 25.09.2024).

115. Arab Convention on Combating Information Technology Offences. Adopted by the Council of Arab Ministers of Justice, League of Arab States, Cairo, 21 Dec. 2010. URL: https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf (date of application: 02.10.2024).

116. Aristotle. Nicomachean Ethics. In: The Complete Works of Aristotle. 1999. URL: https://historyofeconomicthought.mcmaster.ca/aristotle/Ethics.pdf (date of application: 09.10.2024).

117. Arslan G., Wong P. T. Measuring personal and social responsibility: an existential positive psychology approach. *Journal of Happiness and Health*. 2022. Vol. 2. № 1. P. 1–11.

118. Artificial Intelligence and Civil Liability. 2020. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/621926/IPOL_STU(2020)621926_EN.pdf (date of application: 16.10.2024).

119. Artificial intelligence and liability: Key takeaways from recent EU legislative initiatives – Norton Rose Fulbright (Global), July 2024. URL: https://www.nortonrosefulbright.com/en/knowledge/publications/7052eff6/artificial-intelligence-and-liability#:~:text=Global%20,2024 (date of application: 23.10.2024).

120. Artificial intelligence, judicial decision-making and fundamental rights. 2025. URL: https://ssm-italia.eu/wp-content/uploads/2025/02/JuLIA_handbook-Justice_final.pdf (date of application: 23.08.2025).

121. Ayres I., Balkin J. The Law of AI is the Law of Risky Agents Without Intentions. URL: https://lawreview.uchicago.edu/online-archive/law-ai-law-risky-agents-without-intentions (date of application: 06.11.2024).

122. Barlow J. P. A Declaration of the Independence of Cyberspace. Davos, 08.02.1996. URL: https://www.eff.org/cyberspace-independence (date of application: 13.11.2024).

123. Barratt M. J., Lenton S., Allen M. Internet content regulation, public drug websites and the growth in hidden Internet services. *Drugs Edu Prev Policy*. 2013. №20 (3). P. 195–202.

124. Bobonich C. Plato's Utopia Recast – His Later Ethics and Politics. *Utopian Studies.* 2002. №14 (1). P. 165–166.

125. Brickhouse T. C., Smith N. D. Socrates. The Blackwell guide to ancient philosophy. 2003. P. 55–69.

126. Buiten M. The law, economics of AI liability. 2023. URL: https://www.sciencedirect.com/science/article/pii/S0267364923000055 (date of application: 20.11.2024).

127. Burkert W. Lore and Science in Ancient Pythagoreanism. Harvard University Press, 1972. URL: https://philocyclevl.wordpress.com/wp-content/uploads/2016/10/walter-burkert-edwin-l-minar-jr-lore-and-science-in-ancient-pythagoreanism-harvard-university-press-1972.pdf (date of application: 27.11.2024).

128. Calo R. Robotics and the Lessons of Cyberlaw. *California Law Review*. 2015. Vol. 103(3). P. 513–563.

129. Chałubińska-Jentkiewicz K. Cyberspace as an area of legal regulation. *Cybersecurity.* 2022. URL:

https://library.oapen.org/bitstream/handle/20.500.12657/51461/9783030785512.pdf?sequence=1#page=36 (date of application: 04.12.2024).

130. Charon P., Vilmer J.-B. Chinese Influence Operations: A Machiavellian Moment. Report by the Institute for Strategic Research (IRSEM) / Ministry for the Armed Forces. Paris, 2021. URL: https://www.researchgate.net/publication/367252670_Chinese_Influence_Operations_A_Machiavellian_Moment . (date of application: 11.12.2024).

131. Commission staff working document. Ukraine 2023 Report. European Commission. 2023. URL: https://neighbourhood-enlargement.ec.europa.eu/system/files/2023-11/SWD_2023_699%20Ukraine%20report.pdf (date of application: 18.12.2024).

132. Community Standards Enforcement Report. 2024. URL: https://transparency.meta.com/reports/community-standards-enforcement/ (date of application: 25.12.2024).

133. Comprehensive Study on Cybercrime. 2013. URL: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (date of application: 01.01.2025).

134. Cyber War – A Duty to Hack and the Boundaries of Analogical Reasoning. 2015. URL: https://www2.law.temple.edu/voices/cyber-war-a-duty-to-hack-and-the-boundaries-of-analogical-reasoning/ (date of application: 08.01.2025).

135. Czuryk M. Restrictions on the exercising of human and civil rights and freedoms due to cybersecurity issues. *Studia Iuridica Lublinensia*. 2022. Vol. 31.

№ 3. P. 31–43.

136. DAOs and the law: Legal Wrappers. URL: https://www.lexology.com/library/detail.aspx?g=4666ef91-101d-4f81-9c0e-e09c3df9fbf2 (date of application: 15.01.2025).

137. De Sá Lima E. P. P., de Oliveira R. X. P. The Possession and Treatment of Tangible and Intangible Assets: A Procedural Analysis of the Defense of Digital Assets. *Beijing Law Review*. 2024. Vol. 15. № 3. URL: https://www.scirp.org/journal/paperinformation?paperid=136327&utm (date of application: 22.01.2025).

138. Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. URL: https://eur-lex.europa.eu/eli/dir/2017/541/oj/eng (date of application: 29.01.2025).

139. Directive (EU) 2019/713 of the European Parliament and of the Council of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA. URL: https://eur-lex.europa.eu/eli/dir/2019/713/oj/eng (date of application: 05.02.2025).

140. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. URL: https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng (date of application: 12.02.2025).

141. Due Diligence in Cyberspace An Assessment of Rule 6 in the Tallinn Manual 2.0. 2020. URL: https://www.diva-portal.org/smash/get/diva2%3A1417207/FULLTEXT01.pdf (date of application: 19.02.2025).

142. Encyclopædia Britannica. Cyberspace – Definition. URL: https://www.britannica.com/topic/cyberspace (date of application: 26.02.2025).

143. ENISA. European Union Agency for Cybersecurity Annual Report. 2022. URL: https://www.enisa.europa.eu/sites/default/files/all_files/ENISA%20Annual%20Activity%20Report%202022.pdf (date of application: 05.03.2025).

144. European Commission and High Representative. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, February 2013. URL: https://www.eucybernet.eu/wp-content/uploads/2020/08/2013-cybersecurity-strategy-of-the-european-union.pdf (date of application: 12.03.2025).

145. European Union Agency for Fundamental Rights (FRA). Getting the Future Right – Artificial Intelligence and Fundamental Rights. 2022. URL: https://fra.europa.eu/en/publication/2020/artificial-intelligence-and-fundamental-rights (date of application: 19.03.2025).

146. Exploring the Conceptual Framework of Cyberspace: A Journey Beyond Physical Limits November 2, 2023. URL: https://journalism.university/information-and-communication-technologies/conceptual-framework-cyberspace-journey-beyond-limits/ (date of application: 26.03.2025).

147. Fifth Meeting of Ministers of Justice or of Ministers or Attorneys General of the Americas – Conclusions and Recommendations of REMJA-V. URL: https://www.oas.org/juridico/english/remjav_final_report.pdf (date of application: 02.04.2025).

148. Floridi L. The logic of information: A theory of philosophy as conceptual design. *Oxford University Press*. 2019. URL: https://books.google.com.ua/books?hl=uk&lr=&id=nYZUEAAAQBAJ&oi=fnd&pg=PP1&dq=Floridi+L.+The+Logic+of+Information:+A+Theory+of+Philosophy+as+Conceptual+Design.+Oxford:+Oxford+University+Press,+2018.&ots=uxqSwPX0LO&sig=rpQEOmwpoQTcQ95SiROoDCKydK0&redir_esc=y#v=onepage&q=Floridi%20L.%20The%20Logic%20of%20Information%3A%20A%20Theory%20of%20Philosophy%20as%20Conceptual%20Design.%20Oxford%3A%20Oxford%20University%20Press%2C%202018.&f=false (date of application: 09.04.2025).

149. Foulon M., Meibauer, G. How cyberspace affects international relations: The promise of structural modifiers. *Contemporary Security Policy*. 2024. Vol. 45. № 3. P. 426–458.

150. Getman A. P., Danilyan O. G., Dzeban A. P., Kalynovskyi Y. Y. Modern ontology: reflection on the continuity of cyberspace and virtual reality. *Revista de Filosofía*. 2022. Vol. 39. № 102. P. 78–94.

151. Ghoulam K., Bouikhalene, B. From classrooms to cyberspace: Understanding pedagogical approaches and outcomes in Metaverse learning environments. *Mobile Learning Educational Research*. №4 (1). 2024. P. 983–993.

152. Gobble M. M. Digitalization, digitization, and innovation. *Research-Technology Management*. 2018. Vol. 61. № 4. P. 56–59.

153. Goel S., Nussbaum, B. Attribution across cyber attack types: network intrusions and information operations. *IEEE Open Journal of the Communications Society*. 2021. Vol. 2. P. 1082–1093.

154. Gradillas M., Thomas L. D. Distinguishing digitization and digitalization: A systematic review and conceptual framework. Journal of Product Innovation Management. 2025. Vol. 42. № 1. P. 112–143.

155. Guidi B., Michienzi A. From NFT 1.0 to NFT 2.0: A review of the evolution of non-fungible tokens. *Future Internet*. 2023. Vol. 15. № 6. P. 189. URL: https://www.mdpi.com/1999-5903/15/6/189 (date of application: 16.04.2025).

156. Hacker P. The European AI liability directives – Critique of a half-hearted approach and lessons for the future. 2023. URL: https://www.sciencedirect.com/science/article/pii/S026736492300081X . (date of application: 23.04.2025).

157. Hazel S. H. Personal Data as Property. *Syracuse Law Review.* 2020. Vol. 70. URL: https://lawreview.syr.edu/wp-content/uploads/2020/12/1055-1113-Hazel.pdf (date of application: 30.04.2025).

158. Hillier D. Facebook is deleting valuable drug harm reduction groups. VICE. 2024. URL: https://www.vice.com/en/article/facebook-is-deleting-valuable-drug-harm-reduction-groups-safe-sesh/ (date of application: 07.05.2025).

159. Hong Yu., and G. Thomas Goodnight. How to think about cyber sovereignty: The case of China. *China's globalizing internet*. Routledge, 2022. P. 7–25.

160. Honneth A. Reification: A new look at an old idea. Oxford University Press. 2008. URL: https://books.google.com.ua/books?hl=uk&lr=&id=TYGrnFL737UC&oi=fnd&pg=PR7&dq=Honneth+A.+Reification:+A+New+Look+at+an+Old+Idea.+Oxford:+Oxford+University+Press,+2008.&ots=7cXahlB84Q&sig=VugG4Zcc715kwufU9jAtajk7yG4&redir_esc=y#v=onepage&q=Honneth%20A.%20Reification%3A%20A%20New%20Look%20at%20an%20Old%20Idea.%20Oxford%3A%20Oxford%20University%20Press%2C%202008.&f=false (date of application: 14.05.2025).

161. Horky Ph. S. Exoterism and the History of Pythagorean Politics. Plato and Pythagoreanism. Oxford : Oxford Scholarship Online. 2013. P. 85–124.

162. Illinois v. Hemi Group LLC, 622 F.3d 754 (7th Cir. 2010). URL: https://www.thesedonaconference.org/node/5157 (date of application: 28.05.2025).

163. International law in cyberspace. 2015. URL: https://www.aalco.int/userfiles/file/54thSession/Cyberspace%202015.pdf (date of application: 04.06.2025).

164. Interpol operation strikes major blow against West African financial crime. 2024. URL: https://www.interpol.int/News-and-Events/News/2024/INTERPOL-operation-strikes-major-blow-against-West-African-financial-crime (date of application: 11.06.2025).

165. Investigating Cybercrime: The Key Jurisdictional and Technical Challenges Faced by Law Enforcement and Ways to Address Them. URL: https://www.york.ac.uk/media/law/documents/eventsandnewsdocs/2.%20Investigating%20Cybercrime_The%20Key%20Jurisdictional%20and%20Technical%20Challenges%20Faced%20by%20Law%20Enforcement%20and%20Ways%20to%20Address%20Them.pdf . (date of application: 18.06.2025).

166. IT Governance Institute. The EU Cybersecurity Strategy – An Open, Safe and Secure Cyberspace, 2013. URL: https://www.itgovernance.eu/en-ie/eu-cybersecurity-strategy-ie (date of application: 25.06.2025).

167. Jeuring J. H. G., Haartsen T. Destination branding by residents: The role of perceived responsibility in positive and negative word-of-mouth. *Tourism Planning & Development*. 2017. Vol. 14. № 2. P. 240–259.

168. Kahn C. Pythagoras and the Pythagoreans: A Brief History. Hackett, 2001. URL: https://archive.org/details/pythagoraspythag0000kahn (date of application: 02.07.2025).

169. Kapustina N. B. Конфліктна комунікативна поведінка у цифровому середовищі. *Соціологія*. 2024. Vol. 62. № 3. С. 54–64.

170. Kaushik D. Cyberspace as A Global Commons. 2021. URL: https://southasiajournal.net/cyberspace-as-a-global-commons/ (date of application: 09.07.2025).

171. Kello L. Cyber Legalism: Why It Fails and What to Do. Journal of Cybersecurity. 2021. URL: https://academic.oup.com/cybersecurity/article/7/1/tyab014/6343244 (date of application: 16.07.2025).

172. Kirk G. S., Raven, J. E. The Presocratic Philosophers. Cambridge University Press. 1971. 501 p.

173. Koto I. Cyber crime according to the ITE law. *International Journal Reglement & Society (IJRS)*. 2021. Vol. 2. № 2. P. 103–110.

174. Kraut R. Aristotle on the Human Good. Princeton University Press, 1991. 392 p.

175. Kulesza J. International Internet Law. Routledge, 2012. 224 p.

176. Laks A., Most G. W. Early Greek Philosophy. Harvard University Press, 2016. 272 p.

177. Lazarus S. Cybercriminal networks and operational dynamics of business email compromise (BEC) scammers: Insights from the «black Axe» confraternity. *Deviant Behavior*. 2025. Vol. 46. № 4. P. 456–480.

178. Lipinsky D. A. Social bases of positive responsibility. *Mediterranean Journal of Social Sciences*. 2015. Vol. 6. № 6. P. 402–409.

179. Lubis M., Handayani D. O. D. The relationship of personal data protection towards internet addiction: Cyber crimes, pornography and reduced physical activity. *Procedia Computer Science*. 2022. Vol. 197. P. 151–161.

180. Luke Lee Examining the Legal Status of Digital Assets as Property: A Comparative Analysis of Jurisdictional Approaches. 2024. URL: https://arxiv.org/abs/2406.15391 (date of application: 23.07.2025).

181. Marcovich M. Heraclitus: Greek Text with a Short Commentary. Sankt Augustin: Academia Verlag, 1967. 665 p.

182. Meta's Hate Speech Problem. 2024. URL: https://www.statista.com/chart/21704/hate-speech-content-removed-by-facebook/ (date of application: 30.07.2025).

183. Mincewicz W. Explication and classification of social deviations on the Internet: cyberdeviation as a new social phenomenon. *Polish sociological review*. 2023. Vol. 222. № 2. P. 231–248.

184. Morrison R., Mazey N. C., Wingreen S. C. The DAO controversy: the case for a new species of corporate governance? *Blockchain*. 2020. №3. URL: https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2020.00025/full. (date of application: 06.06.2025).

185. Muhammadovich M. F. Kiberhuquq va kiberetika madaniyatining shakillantirishda «kiberxavfsizlik asoslari» fanini o 'qitishning dolzarbligi. *Al-Farg'oniy avlodlari*. 2024. №1. P. 110–115.

186. Nadini M., Alessandretti L., Di Giacinto F., Martino M., Aiello L. M., Baronchelli A. Mapping the NFT revolution: market trends, trade networks, and visual features. *Scientific reports.* №11(1). 2021. URL: https://www.nature.com/articles/s41598-021-00053-8 (date of application: 13.04.2025).

187. NATO CCDCOE. About us. 2023. URL: https://ccdcoe.org/ (date of application: 20.03.2025).

188. NATO CCDCOE. NATO recognises cyberspace as a domain of operations at Warsaw Summit. 2016. URL: https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/ (date of application: 27.05.2025).

189. NATO. Warsaw Summit Key Decisions. Warsaw, July 2016. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_02/20170206_1702-factsheet-warsaw-summit-key-en.pdf (date of application: 03.04.2025).

190. Ness S., Khinvasara, T. Emerging threats in cyberspace: implications for national security policy and healthcare sector. *Journal of Engineering Research and Reports*. 2024. Vol. 26, № 2. P. 107–117.

191. Nye J. The Regime Complex for Managing Global Cyber Activities. Global Commission on Internet Governance Paper. 2014. URL: https://www.cigionline.org/static/documents/gcig_paper_no1.pdf . (date of application: 10.02.2025).

192. O'Keefe T., Johnson M. R. Epicureanism. Aestimatio: Sources, *Studies in the History of Science.* № 9. 2012. P. 1–8.

193. Outcome document: Pact for the Future. URL: https://surl.lt/zecaog (date of application: 17.04.2025).

194. Pagallo U. The Laws of Robots: Crimes, Contracts, and Torts. Dordrecht: Springer, 2013. URL: https://link.springer.com/series/8808 (date of application: 24.06.2025).

195. Palmer J. Plato: Complete Works: edited with introduction and notes. *The Classical Review*. 1998. № 48 (2). P. 482–482.

196. Part II: With New DAO Law on the Books, Utah Joins Race with Wyoming and Tennessee to Become U.S. «Crypto Capital». 2023. URL: https://natlawreview.com/article/part-ii-new-dao-law-books-utah-joins-race-wyoming-and-tennessee-to-become-us-crypto . (date of application: 07.05.2025).

197. Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. URL: https://rm.coe.int/16808ac918 (date of application: 08.06.2025).

198. Ramazonova M. et al. Internet etikasining ochiq muammolari. *The theory of recent scientific research in the field of pedagogy*, 2024, №2 (20). P. 45–49.

199. Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace, adopted by the UNESCO General Conference, Paris, 15 October 2003.

200. Reno v. American Civil Liberties Union, 521 U.S. 844. 1997. URL: https://supreme.justia.com/cases/federal/us/521/844/ (date of application: 15.06.2025).

201. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2013. URL: https://digitallibrary.un.org/record/799853?v=pdf (date of application: 22.06.2025).

202. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. 2015. URL: https://digitallibrary.un.org/record/799853?v=pdf (date of application: 29.06.2025).

203. Sabbagh K., Friedrich R., El-Darwiche B., Singh M., Ganediwalla S., Katz R. Maximizing the impact of digitization. *The global information technology report*. 2012. P. 121–133.

204. SANS Institute. The Fifth Domain: NATO's Cyber Frontline. Podcast, 2023. URL: https://www.sans.org/podcasts/cyber-leaders/fifth-domain-natos-cyber-frontline-manfred-boudreaux-dehmer-9 (date of application: 05.11.2024).

205. Schmitt M. (ed.). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge, 2017. URL: https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf (date of application: 12.04.2025).

206. Shackelford S. J. Managing Cyber Attacks in International Law, Business, and Relations. In: Managing Cyber Attacks in International Law, Business, and Relations: In Search of Cyber Peace. Cambridge University Press;

2014:i-ii. URL: https://www.cambridge.org/core/books/abs/managing-cyber-attacks-in-international-law-business-and-relations/managing-cyber-attacks-in-international-law-business-and-relations/817FACBAC3E116A19E43B24E168EC661 (date of application: 19.04.2025).

207. Shrestha S. Nature, Nurture, or Neither?: Liability For Automated and Autonomous Artificial Intelligence Torts Based on Human Design and Influences. 2021. URL: https://lawreview.gmu.edu/print__issues/nature-nurture-or-neither-liability-for-automated-and-autonomous-artificial-intelligence-torts-based-on-human-design-and-influences/ (date of application: 26.05.2025).

208. Solove D. Understanding Privacy. Harvard University Press, 2008. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888 (date of application: 03.12.2024).

209. Stanley R. Perceived responsibility: Structure, significance. *Behaviour Research, therapy*. №33 (7). 1995. P. 779–784.

210. Strikwerda L. Theft of virtual items in online multiplayer computer games: an ontological and moral analysis. *Ethics Inf Technol*. №14 (2). 2012. P. 89–97.

211. Sudhakar K. N., Shanthi M. Deepfake: an endanger to cyber security. *2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS)*. IEEE. 2023. P. 1542–1548.

212. Sukhai N. B. Hacking and cybercrime. In: Proceedings of the 1st Annual Conference on Information Security Curriculum Development, InfoSecCD ‘04, New York, NY, USA. Association for Computing Machinery. 2004. P. 128–132.

213. Surajo A. Z., Karim A. H. M. Z. An assessment of Black Axe Confraternity Cult in Nigeria: Its impact on the university educational system. *South Asian Anthropologist*. 2017. Vol. 17. № 1. P. 1–7.

214. Taherdoost H. Non-fungible tokens (NFT): A systematic review. Information, №14(1), 2022. URL: https://www.mdpi.com/2078-2489/14/1/26 (date of application: 10.12.2024).

215. Taylor C. C. W. The Atomists: Leucippus and Democritus. Fragments. University of Toronto Press, 1999. 288 p.

216. Teubner G. Networks as connected contracts: edited with an introduction by Hugh Collins. Bloomsbury Publishing. 2011. URL: https://books.google.com.ua/books?hl=uk&lr=&id=Rh7cBAAAQBAJ&oi=fnd&pg=PA1&dq=Teubner+G.+Networks+as+Connected+Contracts.+Oxford:+Hart+Publishing,+2011.&ots=tC8zGjCPbG&sig=hep0SPPWx6w7zJ-Bh5IGRwy8avE&redir_esc=y#v=onepage&q=Teubner%20G.%20Networks%20as%20Connected%20Contracts.%20Oxford%3A%20Hart%20Publishing%2C%202011.&f=false (date of application: 17.12.2024).

217. Teubner G., Golia Jr, A. Societal constitutionalism in the digital world: An introduction. Ind. J. Global Legal Stud., 30, 2023. URL: https://heinonline.org/HOL/LandingPage?handle=hein.journals/ijgls30&div=23&id=&page= (date of application: 24.12.2024).

218. The AI Act Explorer. URL: https://artificialintelligenceact.eu/ai-act-explorer/ (date of application: 23.08.2024).

219. Tikk E., Kaska K., Vihul L. International Cyber Norms: Legal, Policy & Industry Perspectives. NATO CCD COE, 2015. URL: https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_full_book.pdf (date of application: 07.01.2025).

220. UN General Assembly, Resolution 57/239, Creation of a Global Culture of Cybersecurity, 2002. URL: https://digitallibrary.un.org/record/482184?v=pdf (date of application: 14.02.2024).

221. United Nations Convention against Cybercrime. 7.07.2025. URL: https://www.eurojust.europa.eu/publication/united-nations-convention-against-cybercrime? (date of application: 28.07.2025).

222. Valentine S., Godkin, L. Ethics policies, perceived social responsibility, and positive work attitude. *Irish journal of Management*. 2016. Vol. 35. № 2. P. 114–128.

223. Wang N., Zhou J., Li J., Han B., Li F., Chen S. Hardenvr: Harassment detection in social virtual reality. *2024 IEEE Conference Virtual Reality and 3D User Interfaces (VR)*. IEEE. 2024. P. 94–104.

224. Woods A. K. Against Data Exceptionalism. *Stanford Law Review*, Vol. 68. 2016. URL: https://www.stanfordlawreview.org/wp-content/uploads/sites/3/2016/04/68_Stan_L._Rev._729_-_Woods.pdf (date of application: 28.01.2024).

225. Zeran v. America Online, Inc., 958 F. Supp. 1124 (E.D. Va. 1997). URL: https://law.justia.com/cases/federal/district-courts/FSupp/958/1124/1881560/ (date of application: 04.02.2025).

226. Zhmud L. Pythagoras and the Early Pythagoreans. Oxford University Press, 2012. 491 p.

227. Zwitter A., Hazenberg J. Cyberspace, blockchain, governance: how technology implies normative power and regulation. *Blockchain, law and governance. Springer International Publishing*, Cham. 2021. P. 87–97.

ДОДАТОК А

Список публікацій здобувача наукового ступеня доктора філософії з галузі знань 08 Право за спеціальністю 081 Право

Наукові праці, в яких відображені основні результати дослідження:

1. Худолєй Я. Напрями вдосконалення законодавчого регулювання в контексті легалізації та цифровізації ІТ-бізнесу в мережі Інтернет. *Аналітично-порівняльне правознавство.* 2023. № 02. С. 38–42. DOI: https://doi.org/10.24144/2788-6018.2023.02.6

2. Худолєй Я., Загребельна Н. Захист персональних даних у період дії в Україні правового режиму воєнного стану: загальнотеоретичні аспекти. *«Legal Bulletin»: зб. наук. праць ВНЗ «Університет економіки та права «КРОК».* 2023. Вип. 2(8). С. 75–82. DOI: https://doi.org/10.31732/2708-339X-2023-08-75-82

3. Худолєй Я.Г. Інтерпретація юридичної відповідальності в умовах глобалізації та цифровізації. *Наукові інновації та передові технології.* 2025. № 4 (44). С. 1829–1835. DOI: https://doi.org/10.52058/2786-5274-2025-4(44)-1829-1835

4. Худолєй Я.Г. Класифікаційно-функціональні характеристики юридичної відповідальності у мережі Інтернет. *Актуальні питання у сучасній науці.* 2025. № 4 (34). С. 909–914. DOI: https://doi.org/10.52058/2786-6300-2025-4(34)-909-914

5. Худолєй Я.Г. Поняття та правовий статус кіберпростору у міжнародному праві. *Наука і техніка сьогодні.* 2025. № 4 (45). С. 283–291. DOI: https://doi.org/10.52058/2786-6025-2025-4(45)-283-291

6. Худолєй Я.Г., Бакуменко А.В. Правосуб'єктність штучного інтелекту між юридичною фікцією та онтологічною реальністю. *Legal Bulletin.* 2025. Вип. 4(18). С. 10–18. DOI: https://doi.org/10.31732/2708-339X-2026-18-A1

Наукові праці, які засвідчують апробацію матеріалів дисертації:

7. Худолєй Я.Г. Міжнародна операція «Black Axe» та юридична відповідальність за кіберзлочини. *Реалізація конституційного права на свободу пересування в умовах війни: правові стандарти та практичні можливості: матеріали міжнародної правової школи (м. Ужгород, 24 лютого 2023 р).* Ужгород. 2023. С. 36–38.

8. Худолєй Я.Г. Чинники, що визначають сутність поняття інституту юридичної відповідальності. *Сімдесят четверті економіко-правові дискусії. Серія: Соціальні та гуманітарні науки: матеріали Міжнародної мультидисциплінарної наукової інтернет-конференції* (м. Львів, 25-26 квітня 2023 р). http://www.spilnota.net.ua/ua/article/id-4329/

9. Худолєй Я.Г. Деякі аспекти юридичної відповідальності за правопорушення в мережі Інтернет. *Діяльність органів публічної влади України в умовах війни: пошуки оптимальних моделей: матеріали міжнародної правової школи (м. Ужгород, 11 травня 2023 р).* Ужгород. 2023. С. 36–38.

10. Худолєй Я.Г. Міжнародне співробітництво у сфері правопорушень в мережі Інтернет. *Міжнародний фактор перемоги України над московією: правові, інституційні, матеріально-технічні складові матеріали міжнародної правової школи (м. Ужгород, 2 червня 2023 р).* Ужгород. 2023. С. 31–35.

11. Худолєй Я.Г. Мережа Інтернет як простір для здійснення правових відносин. *Global Society in Formation of New Security System and World Order: Proceedings of the 2nd International Scientific and Practical Internet Conference* (м. Дніпро, 27–28 липня 2023 р). URL: http://www.wayscience.com/wp-content/uploads/2023/08/Conference-Proceedings-July-27-28-2023-1.pdf

12. Худолєй Я.Г. Юридичні особи та їх відповідальність за дії в мережі Інтернет. *Інноваційні дослідження та перспективи розвитку науки і техніки у XXI столітті: Міжнародна науково-практична конференція до 30-річчя*

Приватного вищого навчального закладу «Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука» (м. Рівне, 19 жовтня 2023 р). URL: https://dspace.megu.edu.ua:8443/jspui/handle/123456789/4419

13. Худолєй Я.Г. Цифрова термінологія у міжнародно-правовій площині. *Правові проблеми мобільності в умовах надзвичайних режимів: конституційні, економічні, соціальні, культурні та духовні аспекти: матеріали міжнародної правової школи, м. Ужгород, 27 лютого 2025 р.* Ужгород: Ужгородський національний університет. 2025. С. 67–73.

14. Худолєй Я.Г. Методологічні орієнтири дослідження юридичної відповідальності в умовах інформаційного суспільства. *Українська жінка в умовах війни: міждисциплінарний дискурс: матеріали міжнародної правової школи. м. Ужгород. 28 березня 2025 р.* Ужгород: Ужгородський національний університет. 2025. С. 84–86.