

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

Кваліфікаційна наукова
праця на правах рукопису

ФІЛІНОВИЧ ВАЛЕРІЯ ВІКТОРІВНА

Прим. № _____
УДК

**ЗАБЕЗПЕЧЕННЯ ДОТРИМАННЯ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ У КІБЕРПРОСТОРІ: СВІТОВИЙ ДОСВІД ТА
ПРОПОЗИЦІЇ ДЛЯ УКРАЇНИ**

12.00.07 «Адміністративне право і процес;
фінансове право; інформаційне право»

08 - Право

Подається на здобуття наукового ступеня доктора юридичних наук

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

_____ В.В. Філінович

Київ – 2024

АНОТАЦІЯ

Філінович В.В. Забезпечення дотримання права інтелектуальної власності у кіберпросторі: світовий досвід та пропозиції для України. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» (08 – Право). – Національний авіаційний університет. – Київ, 2024.

У дисертації здійснено теоретичне узагальнення і наведено нове вирішення наукової проблеми розкриття сутності і змісту забезпечення дотримання права інтелектуальної власності у кіберпросторі на основі світового досвіду. Зміни в світі, викликані глобалізацією, призвели до переорієнтації економіки на інноваційну модель розвитку, де члени суспільства розробляють і використовують інноваційні активи, зокрема, у формі інтелектуальної власності, і в більшій мірі таке відбувається у кібернетичному просторі як четвертому вимірі людського буття (поруч із повітряним, земним та водним). Було обґрунтовано, що проблема забезпечення дотримання права інтелектуальної власності у кібернетичному просторі значно ускладнюється майже щоденною появою нових інтелектуальних активів, а законодавець не встигає реагувати на відповідні виклики. Додатково вказано на відсутність єдиної стратегії досягнення балансу між бажаннями споживачів цифрових інтелектуальних активів та правовласниками й транскордонність кіберпростору. Тому було обґрунтовано застосування комплексного підходу для вирішення зазначеної проблеми шляхом перегляду нормативно-правового регулювання, виокремлення та опрацювання доктринальних ідей та розробок представників академічних кіл, а також врахування думки інформаційної кіберспільноти.

Визначено, що "віртуальність" інтелектуальної власності не применшує її комерційну цінність як актива, а тому захист такого актива має забезпечуватися, зокрема, на основі основоположних засад - принципів, основними з яких зазначено принципи права власності на інтелектуальну власність, примусового ліцензування, справедливої поведінки, балансу прав правовласника та громадськості, а також гармонізації як взаємної узгодженості та підпорядкування єдиній взаємно-відповідній системі нормативних інструментів та стандартів. Обгрунтовано важливість слідування останньому принципу як основі для досягнення правової одноманітності в усьому світі, що спонукатиме творців активізувати свою творчо-інноваційну діяльність.

Надано визначення поняттю реалізації права як реальному, закріпленому на практиці втіленню в життя формально-визначених правових розпоряджень шляхом правомірних дій (діяльності або бездіяльності) суб'єктів суспільно-правових відносин, метою чого є задоволення основних потреб громадян, суспільства та всієї держави в цілому на підставі засобів та методів, встановлених державою в особі своїх органів. Виділено три форми реалізації правових норм (виконання, дотримання, використання) та обгрунтовано важливість реалізації як ключового етапу процесу правового регулювання, що має особливу практичну значимість безпосередньо для сфери права інтелектуальної власності. Її основою визначено правомірну поведінку суб'єктів суспільних відносин, а також створення і впровадження належного правового забезпечення інноваційно-творчої діяльності. Доведено, що через правореалізацію здійснюються права і обов'язки учасників правовідносин, тому для пришвидшення вирішення спорів між ними такі спори мають здійснюватися шляхом залучення до правозастосовчого процесу спеціальних державних органів.

Визначено, що кіберпростір як інтерактивний домен із цифрових мереж в інформаційному середовищі є елементом, центральним сегментом системи інформаційного середовища (сфери) на рівні із традиційним інформаційним простором, у ньому сконцентровані глобальні потоки економічно-політичної природи та соціальних взаємин. На основі даного твердження обґрунтовано необхідність формування ефективного та стабільного українського інформаційного простору з метою сприяння встановленню та розвитку стійкого кіберпростору в Україні. Ключовими для виконання вказаного визначено посилення нормативно-правового забезпечення функціонування українського кіберпростору програмними та регулюючими документами та системою принципів, серед яких принципи поваги прав і свободи людини, відповідальності, усвідомленості, потрібного втручання, розумності.

Надано визначення термінам, що пов'язані із забезпеченням дотримання права інтелектуальної власності у кібернетичному просторі: оцифруванню (як процесу створення цифрової об'єктивної форми фізичних об'єктів), цифровізації (як забезпеченню або поліпшенню ділових та інших процесів шляхом використання цифрових технологій та діджиталізованої інформації), цифровій трансформації (як безпосередній трансформації бізнесу, що забезпечується діджиталізацією). Зазначено позитивні та негативні результати цифровізації як одного з головних елементів кіберпростору та надано рекомендації щодо подолання пов'язаних із нею проблем для можновладців, зокрема: сприяти формуванню цифрової сумісності між країнами світу із обов'язковою розробкою та впровадженням набору глобальних правил з урахуванням їх економічних, політичних та культурних відмінностей; забезпечити цифровий розвиток нації з метою нівелювати цифровий розрив між різними соціальними групами; розробити та впровадити надійні технології для всіх громадян з одночасним зниженням рівня неефективності та витрат; створити та інтегрувати

міжнародну платформу, яка використовуватиметься для вирішення проблем, спричинених негативним впливом цифрових технологій; створити фонд підтримки, кошти якого мають спрямовуватися на розвиток цифрової інфраструктури та цифровізацію в країні.

Структуру відносин щодо дотримання права інтелектуальної власності у кіберпросторі визначено як симбіоз суб'єктів, що вступають у правовідносини з приводу інтелектуальної власності, і доцільного способу зв'язку між ними з основою на суб'єктивних юридичних правах та обов'язках по відношенню до певних соціальних благ чи інтересів у кіберпросторі. Елементами структури означено осуб'єктів, об'єкти правовідносин та зміст даних правовідносин. З метою виокремлення елементів структури відносин щодо дотримання права інтелектуальної власності в кіберпросторі перелік традиційних об'єктів інтелектуальної власності доповнено інформацію, інформаційними системами, ресурсами, продуктами, інформаційно-телекомунікаційними технологіями, доменними іменами тощо. В якості суб'єктів таких відносин визначено творців об'єктів права інтелектуальної власності, власників відповідних прав, правонаступників та інших осіб, чия діяльність пов'язана із використанням, захистом результатів творчо-інноваційної діяльності, а також тих, хто вступає у такі відносини в процесі діяльності у кіберсередовищі та безпосередньо Інтернеті (таких віднесено до групи онлайн-посередників - провайдери, оператори зв'язку, реєстратори, інтернет-реєстри тощо).

Встановлено, що для України вирішальними етапом генезису став період з отримання незалежності та активної розробки власного законодавства, яке нині покращується з урахуванням сучасних тенденцій у кіберсвіті. Визначено коло проблемних питань правового регулювання відносин щодо дотримання права інтелектуальної власності у глобальних інформаційних та комп'ютерних мережах, серед яких: в галузі авторського

права - онлайн-піратство, фреймінг, лінкінг; в сфері права промислової власності - питання захисту патентів та боротьби із незаконним використанням товарних знаків; в галузі специфічних об'єктів - кіберсквоттинг та тайпсквоттинг щодо доменних імен, сприяння вчиненню правопорушень при використанні технології штучного інтелекту.

На основі методу компаративістики зроблено порівняння правових засад регулювання відносин дотримання права інтелектуальної власності у кібернетичному просторі в країнах Європи, СНД та в США, на основі чого рекомендовано інкорпорацію дієвих положень зарубіжних законодавств та гармонізацію національного, запозичення європейської моделі превентивного захисту прав правовласників, прийняття одноманітного регіонального закону щодо відносин інтелектуальної власності в кіберсередовищі.

Визначено перелік міжнародних та регіональних суб'єктів галузі інтелектуальної власності у кіберпросторі, серед яких ВОІВ, ICANN, Товариство Інтернету, що прагнуть до формування єдиних регулятивних підходів та протидії правопорушенням у досліджуваній сфері. Обґрунтовано застосування Політики вирішення доменних суперечок ICANN при вирішенні таких суперечок через її легкість та дешевизну. Рекомендовано розробити стратегії створення збалансованого зв'язку між інтернет-платформами та режимами інтелектуальної власності із введенням на глобальному рівні мінімальних уніфікованих стандартів у відповідній галузі.

Доведено, що євроінтеграційний вектор розвитку України зумовив зміни в національне законодавство, зокрема, на прикладі нового закону про авторське право і суміжні права 2022 року. Визначено його переваги та недоліки, а також перешкоди на шляху ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі в різних країнах світу, серед яких: неспроможність нормотворців вчасно

реагувати на тренди цифрових трансформацій, недостатність ефективності заходів кібербезпеки, неможливість забезпечити надійний транскордонний захист таких прав, неврегульованість правового забезпечення великих обсягів даних, порушенням їх конфіденційності.

На основі аналізу практик країн світу у галузі забезпечення дотримання права інтелектуальної власності у кіберпросторі, доведено необхідність застосування багатогранного підходу, що передбачає правові, технологічні й соціальні рішення і взаємодію, серед яких: розробка стратегії інтелектуальної власності, впровадження механізму балансування вигод при розподілі прибутку, розробка законодавства на основі загальноприйнятих юридичних практик, нормативне врегулювання питання захисту об'єктів цифрового мистецтва та криптомистецтва, спрощення судових процедур.

Обгрунтовано на міжнародному рівні розробку універсального міжнародно-правового акту для врегулювання проблеми транскордонності Інтернету і досягнення глобальної правової одноманітності, типового (модельного) закону про захист цифрової інтелектуальної власності та уніфікованих правил з протидії кібер-правопорушенням у сфері інтелектуальної власності в Інтернеті та інших глобальних інформаційно-комунікаційних мережах. До такого правотворчого процесу рекомендовано залучити фахівців з права та технічних спеціалістів, міжнародних та регіональних суб'єктів галузі інтелектуальної власності у кіберпросторі та органи забезпечення міжнародного правопорядку.

Запропоновано практичні рекомендації щодо імплементації позитивного зарубіжного досвіду у вітчизняне законодавство, зокрема, в частині прийняття Інформаційного Кодексу України або, за неможливості зазначеного - доповнення діючих нормативно-правових актів, що регулюють інформаційну сферу і безпосередньо кіберпростір, положеннями про права і обов'язків інформаційних суб'єктів, про

інформаційне забезпечення органів державної влади, а також визначенням правового статусу інформаційних ресурсів з урахуванням права власності, рівнів захисту, доступу до інформації та визначенням суб'єктів правопорушення щодо інтелектуальної власності у кібердоміні, з метою чіткого розуміння щодо визначення відповідних осіб. Також обґрунтовано внесення змін до Закону України про авторське право і суміжні права 2022 р. як з метою забезпечення ефективного захисту прав та законних інтересів правовласників, так і задля забезпечення освітнього процесу.

Ключові слова: право інтелектуальної власності, кіберпростір, інформаційне законодавство, інформаційне право, інтелектуальна власність, авторське право, право промислової власності, інтернет-право, цифровий простір, цифрове середовище, дотримання прав інтелектуальної власності.

ABSTRACT

Filinovych V.V. Ensuring compliance with intellectual property law in cyberspace: global experience and suggestions for Ukraine. – Qualifying scientific work on the rights of a manuscript.

The dissertation carries out a theoretical generalization and provides a new solution to the scientific problem of revealing the essence and content of ensuring compliance with intellectual property rights in cyberspace based on world experience. Changes in the world caused by globalization have led to a reorientation of the economy towards an innovative development model, where members of society create and use innovative assets, in particular in the form of intellectual property, and to a greater extent this happens in cyberspace as the fourth dimension of human existence (along with air, ground and water). It was substantiated that the problem of enforcing intellectual property law in cyberspace is significantly aggravated by the almost daily emergence of new intellectual assets, and the legislator is often late with responding to the relevant

challenges. Further, the lack of a unified strategy for achieving a balance between the wants of consumers of digital intellectual assets and copyright holders and the trans-border nature of cyberspace are indicated. Therefore, it was justified to use an integrated approach to solve this issue by revising the legal regulation, highlighting and developing doctrinal ideas and developments of representatives of academic circles, as well as taking into account the opinions of the information cyber community.

It has been determined that the “virtuality” of intellectual property does not diminish its commercial value as an asset, therefore the protection of such an asset must be ensured, in particular, based on fundamental principles, the main of which are the principles of ownership of intellectual property, compulsory licensing, fair conduct, balance of rights of the copyright holder and the public, as well as harmonization as mutual consistency and subordination to a single mutually corresponding system of regulatory instruments and standards. The importance of following the last principle as the basis for achieving legal uniformity throughout the world is substantiated, this will encourage creators to intensify their creative and innovative activities.

A definition is given to the concept of implementation (realization) of law as a real, practical implementation of formally defined legal regulations through lawful activities (actions or inactions) of subjects of social and legal relations, the purpose of which is to satisfy the basic needs of citizens, society and the entire state as a whole based on means and methods established by the state through its bodies. Three forms of implementation of legal norms are identified (execution, compliance, use) and the importance of implementation is substantiated as a key stage in the process of legal regulation, which has particular practical significance directly in the field of intellectual property law. Its basis is determined by the lawful behavior of subjects of public relations, as well as the creation and implementation of appropriate legal support for innovative and creative activities. It has been proven that through legal implementation the rights and obligations

of participants in legal relations are exercised, therefore, to speed up the resolution of disputes between them, such disputes should be carried out by involving special government bodies in the law enforcement process.

It has been determined that cyberspace as an interactive domain of digital networks in the information environment is an element, a central segment of the system of information environment (sphere) together with the traditional information space; global flows of economic-political nature and social relationships are concentrated in it. Based on this statement, the need to form an effective and stable Ukrainian information space is substantiated to facilitate the establishment and development of a sustainable cyberspace in Ukraine. The key to achieving this is the strengthening of legal support for the functioning of Ukrainian cyberspace through program and regulatory documents and a system of principles, including the principles of respect for human rights and freedoms, responsibility, awareness, necessary intervention, and reasonableness.

Definitions are given to terms related to ensuring compliance with intellectual property law in cyberspace: digitization (as the process of creating a digital objective form of physical objects), digitalization (as ensuring or improving business and other processes through the use of digital technologies and digitalized information), digital transformation (as a direct transformation of business, which is ensured by digitalization). The positive and negative results of digitalization as one of the central elements of cyberspace are indicated and recommendations are given to overcome the problems associated with it for the authorities, in particular: to promote the formation of digital compatibility between countries of the world with the mandatory development and implementation of a set of global rules, taking into account their economic, political and cultural differences; ensure the digital development of the nation to bridge the digital gap between different social groups; develop and implement reliable technologies for all citizens while reducing inefficiencies and costs; create and integrate an international platform that will be used to solve problems

caused by the negative impact of digital technologies; create a support fund, the budgets of which should be directed to the development of digital infrastructure and digitalization in the country.

The structure of relations for compliance with intellectual property law in cyberspace is defined as a symbiosis of subjects entering into legal relations regarding intellectual property, and an appropriate way of connecting them with a basis on subjective legal rights and obligations concerning certain social benefits and interests in cyberspace. The elements of such a structure indicate the subjects, objects of legal relations and the content of such legal relations. To highlight the elements of the structure of relations of compliance with intellectual property law specifically in cyberspace, the list of traditional intellectual property objects was supplemented with information, information systems, resources, products, information and telecommunication technologies, domain names, and the like. The subjects of such relations are the creators of objects of intellectual property law, owners of relevant rights, successors and other persons whose activities are related to the use and protection of the results of creative and innovative activities, as well as those entering into such relations in the process of activities in the cyber environment and directly on the Internet (the last are classified as online intermediaries - providers, telecom operators, registrars, Internet registries, and the like).

It is proved that for Ukraine, the decisive stage of its genesis was the period of gaining independence and active development of its legislation, which is now being revised and improved taking into account modern trends in the cyber world. A range of problematic issues of legal regulation of relations of compliance with intellectual property law in global information and computer networks has been identified, including: in the field of copyright - online piracy, framing, linking; in the field of industrial property law – issues of protecting patents and combating the illegal use of trademarks; in the field of specific objects - cybersquatting and typosquatting on domain names, facilitating the commission of offenses in

connection with the use of artificial intelligence technology. The understanding of intellectual property as a component of the intangible assets of an enterprise, violations of which result in material and reputational losses, is noted.

Based on the method of comparative studies, a comparison of the legal framework for regulating relations of compliance with intellectual property law in cyberspace in the countries of Europe, the CIS, and the USA was made; based on the mentioned it was recommended to incorporate effective provisions of foreign legislation and harmonize national legislation, to borrow the European model of preventive protection of the rights of copyright holders, and to adopt of a uniform regional law on intellectual property relations in the cyber environment.

A list of international and regional actors of the intellectual property in cyberspace sphere was identified, including WIPO, ICANN, and the Internet Society, which strive to form common regulatory approaches and combat offenses in the area under study. The use of the ICANN Uniform Domain Name Dispute Resolution Policy in resolving such disputes is justified because of its ease and low cost. It is recommended to develop a strategy to create a balanced relationship between Internet platforms and intellectual property regimes, with the introduction of minimal unified standards in the relevant sphere at the global level.

It was proven that the European integration vector of Ukraine's development has led to changes in national legislation, in particular, using the example of the new law on copyright and related rights of 2022. Its advantages and disadvantages are identified, as well as obstacles to ensuring effective compliance with intellectual property law in cyberspace in different countries of the world, including: the inability of rule-makers to respond in a timely manner to digital transformation trends, the insufficient effectiveness of cybersecurity measures, and the inability to provide reliable cross-border protection, the unsettledness of legal support for large volumes of data, violation of their confidentiality.

Based on an analysis of the best practices of countries around the world in the field of ensuring compliance with the intellectual property law in cyberspace, the need for a multifaceted approach has been proven, providing for legal, technological and social solutions and interaction, including: development an intellectual property strategy for the next decade, introducing a mechanism for balancing benefits during the distribution of profits, development of legislation based on generally accepted legal practices, regulatory settlement of the issue of protecting objects of digital art and crypto art, simplification of judicial procedures.

It is justified to develop at the international level a universal international legal act to resolve the problem of transboundary of the Internet and achieve global legal uniformity, a model law on the protection of digital intellectual property and unified rules for combating cyber-offenses in the field of intellectual property on the Internet and other global information communication networks. It is recommended to involve legal and technical experts, international and regional intellectual property subjects in cyberspace, and international law enforcement agencies in such a law-making process.

Practical recommendations are suggested for the implementation of positive foreign experience in domestic legislation, in particular, in terms of the adoption of the Information Code of Ukraine or, if this is not possible, the amendment of existing regulations governing the information sphere and cyberspace itself, with provisions on the rights and responsibilities of subjects, information support for public authorities, as well as determining the legal status of information resources, taking into account ownership, levels of protection, access to information and identifying subjects of intellectual property offenses in the cyber domain in order to clearly understand the definition of the relevant persons. It is also justified to introduce amendments to the Law of Ukraine on Copyright and Related Rights of 2022, both in order to ensure effective protection

of the rights and legitimate interests of copyright holders, and to ensure the educational process.

Keywords: intellectual property law, cyberspace, information legislation, information law, intellectual property, copyright, industrial property law, Internet law, digital space, digital environment, compliance with intellectual property rights.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковано основні наукові результати дисертації

Статті в наукових фахових виданнях України

1. Філінович В. В. Передання прав на доменне ім'я та його трансфер до іншого реєстратора. *Науковий вісник Міжнародного гуманітарного університету. Серія «Юриспруденція»*. 2018. № 34. С. 62–64.
2. Філінович В. В. Сутність інтернаціоналізованих доменних імен та їх правове регулювання. *Електронне наукове фахове видання «Порівняльно-аналітичне право»*. 2019. №3. С. 99-101.
3. Filinovich V. V. Website regulatory laws of the USA. *Наукові праці Національного авіаційного університету. Серія: «Юридичний вісник «Повітряне і космічне право»*. 2019. №3 (52). С. 115–121.
4. Філінович В. В., Новгородська І.М. Захист прав власників доменних імен. *Електронне наукове фахове видання «Порівняльно-аналітичне право»*. 2019. №5. С. 136-138. *Внесок здобувача: 75%*
5. Filinovich V. V. Legal status of domain names in the legislation of Ukraine and doctrinal sources. *Наукові праці Національного авіаційного університету. Серія: «Юридичний вісник «Повітряне і космічне право»*. 2020. №2 (55). С. 144–150.

6. Filinovich V. Problems of Human Rights Violations Caused by Cybercrimes and Ways to Overcome Them. *Наукові праці Національного авіаційного університету. Серія: «Юридичний вісник «Повітряне і космічне право»*. 2020. №3 (56). С. 143–148.
7. Філінович В. В. Кібербезпека та інтернет речей: правовий аспект. *Наукові праці Національного авіаційного університету. Серія: «Юридичний вісник «Повітряне і космічне право»*. 2020. №4 (57). С. 122-127.
8. Voronova O., V. Filinovich. The Role of the Web-based Distance Learning Environment in the Education of Future Lawyers. *Наукові праці Національного авіаційного університету. Серія: «Юридичний вісник «Повітряне і космічне право»*. 2020. №4 (57). – С. 188–193. *Внесок здобувача: 50%*
9. Филинович В. В. Киберсталкинг: проблемы правовой защиты. *Наукові праці Національного авіаційного університету. Серія: «Юридичний вісник «Повітряне і космічне право»*. 2021. №1 (58). – С. 135-141.
10. Філінович В.В. Кібербезпека та загрози авіаційній сфері: правовий аспект. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. 2021. № 3 (60). С. 38–44. <https://doi.org/10.18372/2307-9061.60.15950>
11. Filinovich V. Violation of copyright and related rights on the internet: how to protect yourself and your creation. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. 2021. №4 (61). С. 144–150. <https://doi.org/10.18372/2307-9061.61.16362>
12. Filinovich V., Sukhanov O. Domain name in the system of objects of intellectual property rights. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне*

право». 2022. №3 (64). С. 146–152. <https://doi.org/10.18372/2307-9061.64.16884> Внесок здобувача: 75%

13. Filinovich V.V. Genesis of the legal regulation of the functioning of intellectual property in cyberspace. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. 2023. №1 (66). С. 133-139.
14. Filinovich V. Effectiveness of legal enforcement of intellectual property rights in cyberspace. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. 2024. Т. 2, № 71. С. 154–160. URL: <https://doi.org/10.18372/2307-9061.71.18804>.

Статті в наукових періодичних виданнях інших держав

15. Filinovich V. Domain Name as a Means of Individualization of Participants in Civil Turnover of Ukraine. *Journal of Law and Political Sciences*. 2020. Vol. 24. Issue 3. P. 180–211. / **Web of Science**.
16. Sopilko I., Filinovich V., Pankova L. O., Obshalov S.V., Chaplynskyi K. O. Protection of Intellectual Property Rights from Cyber Threats in the Global Information Environment. *Novum Jus*. 2023. Vol. 17(1). P. 237–258. <https://doi.org/10.14718/NovumJus.2023.17.1.10> Внесок здобувача: 20% / **Scopus**.
17. Filinovich V. Conceptual Grounds for Development of Effective Legal Enforcement of Intellectual Property Rights in Cyberspace. *Journal of International Legal Communication*. 2024. Vol. 13, № 2. P. 74–843. URL: <https://doi.org/10.32612/uw.27201643.2024.13.2.pp.74-84>
18. Sopilko I., Filinovich V., Prudnykova O. V., Krupnova A., Smetanina N. Ensuring the functioning of cyberspace in Ukraine: Legal and technical aspects. *Sapienza: International Journal of Interdisciplinary Studies*. 2024.

Vol. 5, no. 3. P. e24055. <https://doi.org/10.51798/sijis.v5i3.787> *Внесок здобувача: 20% / Scopus.*

Розділи в монографіях

19. Filinovich V. Cybersecurity guarantees as a factor of state information security. *Problems of implementation of state policy in the field of information security of Ukraine* : Collective monograph. Accent Graphics Communications & Publishing. Ottawa, 2020. С. 144–156.
20. Філінович В. В. Проблеми правового регулювання відповідальності органів державної влади за порушення прав громадян в сфері кіберзлочинів. *Проблеми правового регулювання відповідальності органів державної влади за порушення прав громадян* : колект. монографія. НАУ. Київ, 2021. С. 116–126.
21. Sopilko I., Filinovich V. Development of the Internet trust Environment as an Important Element for Cybersecurity. *University law science and education in the challenges of our time* : Collective monograph. Warszawa, 2021. С. 291–30. *Внесок здобувача: 50%*
22. Філінович В.В. Права інтелектуальної власності у кібернетичному просторі як неосновоположні, але важливі права людини. *Гарантії прав людини і громадянина в контексті європейської інтеграції України: монографія* / Юринець Ю.Л., Токарева К.С., Філінович В.В. та ін. - Чернівці: Технодрук. 2023. С. 166-177.

Наукові праці, які засвідчують апробацію матеріалів дисертації

23. Філінович В. В. GDPR та специфікація реєстраційних даних загальних доменів верхнього рівня. *АЕРО-2018. Повітряне і космічне право: матеріали Всеукраїнської конференції молодих учених і*

студентів, м. Київ, Національний авіаційний університет, 22 листопада 2018 р. Том 2. – Тернопіль: Вектор. 2018. С. 21–23.

24. Філінович В. В. Система DAAR та моніторинг зловживань у галузі доменних імен. Матеріали *IX Міжнародної науково-практичної конференції молодих учених і студентів «Юриспруденція в сучасному інформаційному просторі»*, (Київ, 1 березня 2019 р). 2019. Т. 2. С. 157-159.
25. Filinovich V. Violation of antitrust laws by UIA and well-known low-cost carriers. Тези доповідей *XIV Міжнародної науково-технічної конференції «AVIA-2019»*, (Київ, 23-25 квітня 2019 року). – С. 33.8–33.11.
26. Філінович В. В. Визначення поняття веб-сайт у національному законодавстві та правовій доктрині // *Інноваційний розвиток правової науки в умовах модернізації суспільства*: матеріали X Міжнародної науково-практичної конференції, м. Київ, Національний авіаційний університет, 28 лютого 2020 р. Тернопіль: Вектор. 2020. С. 174-176.
27. Филинович В.В. Фотография и авторское право: роль объекта и его правовая защита. *АЕРО-2020. Повітряне і космічне право*: зб. тез доп. всеукр. наук.-практ. конф., м. Київ, 20 листопада 2020 р. Київ, 2020. Том 2. С. 26-28.
28. Філінович В. В. Трестове середовище Інтернет як важливий елемент кібербезпеки. Матеріали *XI Міжнародної науково-практичної конференції «Сучасне право в епоху соціальних змін»*, (Київ, 26 лютого 2021 р). – С. 157-159.
29. Filinovich V. V. Cybersecurity gaps as a problem of modern aviation: legal aspect. «AVIA-2021» : матеріали XV міжнар. науково-техн. конф., м. Київ, 20–22 квіт. 2021 р. Київ, 2021. С. 31.1–31.4. URL: <http://conference.nau.edu.ua/index.php/AVIA/AVIA2021/paper/view/7995/663>.

30. Filinovich V. How to overcome intellectual property infringements in cyberspace: Ukrainian experience. Book of Abstracts. *International Conference: XXI century, new challenges and modern development tendencies of law*, December 21-22, 2021. Baku State University. Baku, Azerbaijan, 2021. С. 196-197.
31. Filinovich V., Hu Z. Aviation and the Cybersecurity Threats. *Proceedings of the International Conference on Business, Accounting, Management, Banking, Economic Security and Legal Regulation Research (BAMBEL 2021)* : Proceedings of the International Conference, Kyiv, 26–27 August 2021. Amsterdam, 2021. P. 120–126. URL: <https://doi.org/10.2991/aebmr.k.210826.021>. Внесок здобувача: 75%
32. Филинович В.В. Место киберпространства в информационной среде и правовое обеспечение их функционирования. Матеріали XII Міжнародної науково-практичної конференції "Права людини в епоху цифрових трансформацій", м. Київ, Національний авіаційний університет, 25 лютого 2022 р. Том 2. – Тернопіль: Вектор, 2022. – С. 106-109.
33. Filinovich V. Correlation between human rights and intellectual property rights. *III Міжнародна науково-практична конференція «Модернізація вітчизняної правової системи в умовах світової інтеграції»* (м. Кропивницький, 23-24 червня 2022 року). - Кропивницький, 2022. С. 240-242. URL: https://www.klanau.kr.ua/images/docs/Modernizacia_vitchiznianoy_praovoy_systemy_23062022.pdf.
34. Filinovich V.V. The structure of intellectual property rights relations in cyberspace. *Матеріали XIII Міжнародної науково-практичної конференції "Свобода, безпека та незалежність: правовий вимір"*, Національний авіаційний університет (Київ, 24 лютого 2023 р.). – С. 553-556.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АП – авторське право

ВОІВ – Всесвітня Організація Інтелектуальної Власності

ДІ – доменне ім'я

ДСІВ – Державна служба інтелектуальної власності

ЕІР – електронний інформаційний ресурс

ЄК – Європейська комісія

ЄС – Європейський Союз

ЗУ – Закон України

ІВ – інтелектуальна власність

ІКТ – інформаційно–комунікаційні технології

КМУ – Кабінет Міністрів України

КП – комп'ютерна програма

МЗП – мінімальна заробітня плата

МНКЦ – Мережа національних координаційних центрів

МПА – міжнародно–правовий акт

НПА – нормативно–правовий акт

ОБСЄ – Організація з Безпеки та Співробітництва в Європі

ОКУ – організація колективного управління

ООН – Організація Об'єднаних Націй

ПШОК – провайдери послуг обміну контентом

РНБО – Рада національної безпеки та оборони України

СКУ – система колективного управління

СНД – Співдружність Незалежних Держав

США – Сполучені Штати Америки

ТМ – торговельна марка

ЦКУ – Цивільний Кодекс України

ШІ – штучний інтелект

DMCA – Digital Millennium Copyright Act, Закон про авторське право в цифрову епоху

ICANN – Internet Corporation for Assigned Names and Numbers, Інтернет–корпорація з присвоєння імен та номерів

PTI – Public Technical Identifiers

UDRP – Uniform Domain Name Dispute Resolution Policy, Єдина Політика Розгляду Спорів про доменні імена

ЗМІСТ

ЗМІСТ	11
ВСТУП	14
РОЗДІЛ 1. МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ ПРОБЛЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ДОТРИМАННЯ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ У КІБЕРПРОСТОРІ	15
1.1. Генезис наукових поглядів щодо дотримання права інтелектуальної власності у кіберпросторі	15
1.2. Дотримання права інтелектуальної власності у кіберпросторі як предмет наукового дослідження	25
1.3. Принципи дотримання права інтелектуальної власності у кіберпросторі в Україні і світі: порівняльно-правовий аналіз	42
1.4. Правові форми дотримання права інтелектуальної власності у кіберпросторі: сучасні наукові погляди до визначення і застосування	59
Висновки до Розділу 1	71
РОЗДІЛ 2. ТЕОРЕТИКО-ПРАВОВА ХАРАКТЕРИСТИКА КІБЕРПРОСТОРУ ЯК ОСНОВИ ІСНУВАННЯ ЦИФРОВОГО КОНТЕНТУ	76
2.1. Місце кіберпростору у інформаційному середовищі	76
2.2. Якість правового забезпечення функціонування кіберпростору в Україні	89
2.3. Цифровізація як елемент кіберпростору у науці та законодавстві	105
Висновки до Розділу 2	120
РОЗДІЛ 3. АКТУАЛЬНІ ПИТАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ВІДНОСИН ЩОДО ДОТРИМАННЯ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ У КІБЕРПРОСТОРІ	124
3.1. Структура відносин щодо дотримання права інтелектуальної власності у кіберпросторі: юридична характеристика	124
3.2. Генеза правового регулювання функціонування окремих інститутів інтелектуальної власності у кіберпросторі	151
3.3. Актуальні питання правового регулювання відносин щодо дотримання права інтелектуальної власності у глобальних інформаційних та комп'ютерних мережах	172
Висновки до Розділу 3	189
РОЗДІЛ 4. ЮРИДИЧНА КОМПАРАТИВІСТИКА ЯК МЕТОД ДОСЛІДЖЕННЯ ПРАВОВИХ ОСНОВ РЕГУЛЮВАННЯ ВІДНОСИН ДОТРИМАННЯ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ У	

КІБЕРПРОСТОРИ	195
4.1. Правові основи регулювання відносин дотримання права інтелектуальної власності у кіберпросторі в країнах ближнього та дальнього зарубіжжя	195
4.1.1. США	197
4.1.2. Європейський Союз та країни Європи	219
4.1.2. Країни СНД	238
4.2. Суб'єкти міжнародно-правової охорони права інтелектуальної власності	249
4.2.1. Всесвітня організація інтелектуальної власності (ВОІВ)	251
4.2.2. Internet Corporation for Assigned Names and Numbers (ICANN)	261
4.2.3. Internet Society, World Wide Web Consortium та інші суб'єкти	268
Висновки до Розділу 4	276
РОЗДІЛ 5. НАУКОВО-ПРАКТИЧНА ОСНОВА ФОРМУВАННЯ ЕФЕКТИВНОГО ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ДОТРИМАННЯ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ У КІБЕРПРОСТОРИ	280
5.1. Нові підходи до формування правового забезпечення дотримання права інтелектуальної власності у кіберпросторі в Україні	280
5.2. Ефективність правового забезпечення дотримання права інтелектуальної власності у кіберпросторі в Україні і світі: шляхи впровадження найкращих світових практик	314
5.3. Концептуальні засади побудови ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі	338
Висновки до Розділу 5	361
ВИСНОВКИ	370
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	370

ВСТУП

Обґрунтування вибору теми дослідження. У епоху активного розвитку та застосування цифрових технологій захист інтелектуальної власності став більш критичним, ніж будь-коли, що особливо відмітно у зв'язку із "життям" майже кожної людини у кіберпросторі. Раніше ми всі існували лише у трьох просторах - водному, повітряному, земному, нині ж до них слід додати також і кібернетичний. Сучасна інтелектуальна власність не має єдиного вичерпного переліку об'єктів. Як традиційні її об'єкти, так і сучасні "цифрові" використовуються найчастіше тим чи іншим способом саме у кібервимірі. Творці та діячі-інноватори, що зрозуміло, покладаються на юридичні та технологічні інструменти з метою захисту своїх інтелектуальних активів від їх крадіжки, несанкціонованого розповсюдження та інших правопорушних дій.

Ризики та проблеми у даній сфері з'являються щоденно, адже технологічна обізнаність та навички правопорушників удосконалюються та розвиваються, тим не менш, саме поєднання правових заходів, технологій і загальнолюдської обізнаності є тим, що допоможе зберегти цілісність інтелектуальної власності, що існує в "цифрі". Вказане є запорукою того, що креативні особи зможуть отримати належну й справедливу винагороду і визнання за свої внески, а суспільство і держави в цілому - розвиток інновацій і творчості в епоху цифрових технологій, що відповідно, призведе до економічного зростання.

Варто розуміти, що захист об'єктів інтелектуальної власності в кіберсередовищі значно ускладнений через транснаціональний характер кіберпорушень, сприяє даній проблемі й недосконалість національного правового забезпечення в різних країнах, зокрема, Україні. У законодавстві останньої ще з 2007 року було встановлено одним із головних пріоритетів саме перетворення українського суспільства на інформаційно-орієнтоване

та відкрите для кожного, що має чітке спрямування на захист прав та інтересів людини. Такий вектор спрямування сприяє соціально-економічному розвитку, а отже, і покращенню якості життя кожного з нас.

Для України належне та якісне забезпечення дотримання права інтелектуальної власності у кіберпросторі є сьогодні вкрай актуальним ще й через те, що в країні введено режим воєнного стану у зв'язку із повномасштабним вторгненням на її територію агресивно-налаштованої Російської Федерації. Остання веде проти нашої держави не лише "конвенційну", тобто мілітарну війну, але й застосовує психологічні та інформаційні воєнні засоби. Проявом останніх є, крім іншого, війна в інформаційному, зокрема, кібернетичному просторі, із вчиненням правопорушень і в сфері інтелектуальної власності у кіберсередовищі. Лише одним із великої кількості є приклад крадіжки та розкриття відомостей щодо дронів та іншої воєнної техніки, яка зараз управляється комп'ютерами та подібними високотехнологічними пристроями. Відповідно, навіть одне таке порушення може впливати на хід війни. А таких прикладів, пов'язаних із використанням інтелектуальної власності у кібернетичному просторі, є чимало.

Відповідно, захист таких об'єктів загалом та, зокрема, забезпечення дотримання права інтелектуальної власності у кіберпросторі є надактуальним питанням як для України, так і для світу в цілому, тобто це питання загальносвітової безпеки. І дане дисертаційне дослідження покликане, на основі наявного світового досвіду, винайти шляхи забезпечення дотримання права інтелектуальної власності у кіберпросторі найкращим чином.

У наукових дослідженнях з інформаційного права та права інтелектуальної власності безпосередньо проблема забезпечення дотримання права інтелектуальної власності у кіберпросторі ще не була

достатньо проаналізована, хоча здобутки вчених по окремих аспектах вказано теми займають важливе місце.

Теоретичне підґрунтя для підготовки та написання дисертації склали праці сучасних українських та іноземних вчених-правознавців. Як і будь-яка галузь права, інформаційне право та право інтелектуальної власності мають свої витоки у загальній теорії держави і права. Тому в процесі роботи над даним дисертаційним дослідженням окрема увага була приділена відповідним фундаментальним розробкам О. Ф. Скакун, О.П. Віхрова, І.О. Віхрової, П. М. Рабіновича, О. В. Петришина та інших вчених-теоретиків права, на основі чого було сформовано загально-теоретичні правові засади для проведення дослідження проблеми правового забезпечення дотримання права інтелектуальної власності у кіберпросторі.

Означена проблема також не могла бути вирішена без детального огляду та вивчення окремих аспектів використання та правового забезпечення інтелектуальної власності загалом.

Інформаційне середовище, без якого не існувало б кібернетичного середовища, стало предметом глибокого та всебічного дослідження П. Ретгера та Б. Ведреса, які також в своїй роботі акцентують увагу на впливі відповідного феномену на окремих індивідів та цілі групи людей. Вивченню структури та функціональних параметрів інфопростору присвятив свою роботу К. А. Дубняк, а І. А. Грузіна дослідила в деталях його вплив на діяльність сучасних підприємства, в той час як В.Г. Воронкова та В.О. Нікітенко охарактеризували цифрову стратегію таких суб'єктів. Праця В. Горового висвітлює особливості посилення глобальних інформаційних впливів в розрізі національних інформаційних ресурсів. Проблематику взаємодії індивідів із інформаційним середовищем якісно аналізує О. О. Жидкова, а роботи Г. Бонч-Бруєвич та Т. Носенко розкривають особливості взаємодії безпосередньо із цифровою інформацією.

Визначенню суті поняття та особливостей кібернетичного домену (кіберпростору) присвячені роботи таких вчених як Т. Фолсом, який шукав у відповідному концепті не лише "віртуальні", але є "реальні" складові та детально їх охарактеризував. А. Келлерман здійснив класифікацію кіберпростору на інформаційний та комунікаційний, О. Зубко О. розробив сучасну концепцію його адміністративно-правового захисту в Україні. Кіберпростір як складова інформаційної сфери є предметом дослідження в роботах О. Яременко, де основний фокус зроблено на проблемі правової інституалізації.

Цифровізація (діджиталізація) як елемент кіберпростору у науці та законодавстві також є предметом всебічного дослідження багатьох вчених. Так, О. І. Піжук, вивчає даний концепт з точки зору зміни парадигми розвитку економічних систем, а К. Маркевичем викладено наукові положення щодо його переваг й шляхів подолання пов'язаних з ним викликів. Розробка О. Клевець дає чітке розуміння того, чим цифровізація відрізняється від автоматизації, а П. Богуш в своїй роботі детально пояснює різницю між нею та оцифруванням, М.С. Гупта додав до порівняння двох останніх категорій також цифрову трансформацію. На якостях діджиталізації державного управління наголосив в своєму науковому доробку Н. Чередніченко. Слід також вказати на практичну важливість монографії А. Остенди та інших, що присвячена, зокрема, соціальним та гуманітарним аспектам цифровізації у формуванні інформаційного суспільства та актуальним проблемам розвитку цифрової економіки.

Стабільність інформаційного та кібернетичного простору, а з ним, відповідно, і цифрової інтелектуальної власності максимально залежить від забезпечення належного рівня інформаційної та кібербезпеки в кожній окремій країні та загалом в світі. Саме тому для досягнення цілей даної дисертації було важливим дослідити і останні феномени. Розкриттю поняття та принципів інформаційної безпеки присвячено працю Дж.

Фрулінгера, її соціальній складовій - Є. О. Архіпової, а В. М. Фурашев зосередив увагу на її співвідношенні із кібербезпекою та загалом із кібер- та інформаційним простором. Різниця між інформаційною та кібернетичною безпекою детально охарактеризована в роботі Л. Ірвіна, якісне співставлення вказаних понять в правовому аспекті зроблено також І. Сопілко. Світовим тенденціям і сучасним викликам, які стосуються кіберпростору свою увагу приділили Д. Дубов Д. та М. Ожеван. Правові та організаційні засади інформаційної безпеки та відповідної політики досліджують такі вчені як Б. А. Кормич, О. Проскуріна та інші.

Кіберсередовище як віртуальний простір - є плацдармом для комунікації та побудови суспільних відносин завдяки використанню глобальних мереж передачі даних і, зокрема, Всесвітньої мережі Інтернет. Відповідно, розкриття сутності та особливостей останнього було вкрай важливим для досягнення мети даного дисертаційного дослідження. Так, в роботах Р. Еннана надано аналіз специфіки та суті Інтернету, зроблено класифікацію відносин щодо нього, та, зокрема, висвітлено особливості правовідносин інтелектуальної власності у ЄС. К. В. Єфремова теж приділила увагу в своїх працях правовій природі та регулювання правовідносин в Інтернеті, а також визначила перспективи такого правового регулювання, спрямувавши свій фокус саме на господарсько-правовий аспект. Суб'єкти та об'єкти правовідносин інтелектуальної власності є наскрізною темою робіт О. І. Харитонової.

Означена в темі дослідження проблема також не могла б бути вирішена без детального огляду та вивчення окремих аспектів використання та правового забезпечення інтелектуальної власності загалом. Вказана категорія є предметом наукових досліджень в роботі багатьох вчених. Зокрема, С. Гарна, А. Шнурко та інші проаналізували її як складову нематеріальних активів підприємства, К. Сінь прояснив, як її захист сприяє технологічним інноваціям серед суб'єктів господарювання, В.

Д. Базилевич, В.М. Крижна, Н.Є. Яркіна й О. П. Світличний визначили поняття, особливості й сутність, а П. Гордон - її основні принципи. В роботах В. В. Вірченко та Г. М. Филюк акцент зроблено на архітектоніці й основних функціях інтелектуальної власності на тлі постіндустріальної економіки, а Дяченко Н. П. наголошує на важливості дотримання відповідних прав при формуванні передумов зростання суспільної довіри. Роль інтелектуальної власності в кіберправі є предметом детального аналізу в роботі А. Діксита, а Дж. Ф. Морін висвітлив в своїй роботі основні аспекти зміни парадигми в глобальному режимі відповідної концепту. Надважливе питання юрисдикції у кіберпросторі та пов'язаного із цим транскордонного захисту інтелектуальної власності підняте і розкрито в роботах, зокрема, К. Сарангі та Т. Коно.

Для розуміння особливостей становлення та розвитку права інтелектуальної власності у кіберпросторі важливим було розкрити генезу правового регулювання функціонування її окремих інститутів в Україні та світі, чому всіляко сприяло заглиблення у відповідні наукові праці. Однією з таких є дисертація Г. В. Довгань, в якій детально досліджено відповідні історико-правові аспекти становлення нормативно-правових інструментів та механізмів дотримання права інтелектуальної власності в 19-20 століттях на українських та сусідніх землях. Не менш важливим є і більш ранні періоди, зокрема 1550–1800 рр., що детально проаналізовані в роботі А. Моссоффа, де основний упор зроблено саме на становленні патентного права. З урахуванням досить тривалого періоду знаходження українських земель у складі Польщі, і, відповідного впливу на формування як права загалом, так і, зокрема, регулювання інтелектуальної власності, важливим було висвітлити основні моменти розвитку такого права у відповідній країні, чому присвячено праця С. Пляза. Становлення сучасного права інтелектуальної власності в інших країнах є не менш важливим для формування загально-світової картини формування інтелектуальної

власності загалом, та у кіберпросторі зокрема, тому в процесі роботи над даним дисертаційним дослідженням були використані також праці Б. Шермана, який поділився відповідним досвідом Великої Британії 1760-1911 рр., та інших вчених.

Д. Гончаренко присвятив свою працю місцю та проявам інтелектуальної власності у Всесвітній Мережі, як і О. І. Харитонова та інші вчені, в роботах яких досліджено проблемні питання визначення правової природи і структури відповідних правовідносин, що виникають в Інтернеті, й їх співвідношення. Н.О. Шпак, В.М. Гавецька та інші зробили основний аспект в своїх наукових здобутках на проблематиці дотримання прав інтелектуальної власності у медіа-просторі. Окремі виклики та ризики, що постають перед правом інтелектуальної власності в Інтернет-епоху вивчає й Л. Гао.

Питання забезпечення авторського права у цифровому середовищі є наскрізною темою в роботах Н. Елькін-Корен, М. Гільдебрандта, Р. Фатіма, Р. Джа, К. Мантрі, Н. Мітри, Н. С. Сансаре, С. Сінгха, К. Заїді. А. Ананд всебічно досліджує цифрове піратство, що сьогодні є однією з найбільш розповсюджених проблем у галузі права інтелектуальної власності та, зокрема авторського права, а Л. Орландо висвітлює дане питання з точки зору патентного права. С. Н. Ядав провів розрізнення авторського права та піратства. Практичні та теоретичні аспекти строку дії авторського права означені в доробку Т. Очоа. І.М. Сопілко та О. В. провели якісний аналіз українського законодавства щодо охорони об'єктів авторського права.

І. Т. Харді присвятив своє дослідження кримінальним правопорушенням авторських прав, що є вельми актуальним, адже зазвичай такі порушення відносять до відання цивільного права (наприклад, як це зроблено у О. Штефана). Порухні дії нахталт фреймінга та лінкінга є нині викликом для захисту інтелектуальної власності в кібернетичному середовищі, тому і їм присвячені роботи деяких вчених, зокрема, Р. Мітала,

П. Зітера. Захист інтелектуальної власності в епоху цифрових технологій: захист творчості у В'єтнамі.. Викликає зацікавленість також концепція Н. В. Троцюк та А. С. Кудзіновського щодо покладення відповідальності за порушення в авторсько-правовій сфері на інтернет-посередників. Практику порушень у вказаній галузі із використанням інструментів штучного інтелекту висвітлює у своїх роботах Дж. Вінсент. Зловживанням правами інтелектуальної власності в кіберпросторі в контексті патентного права є предметом дослідження Ю. Р. Квін.

Окремо варто приділити увагу дисертації Г. Монаха щодо проблем в галузі інтелектуальної власності в кіберпросторі, які не підпадають під регулювання законами про авторське право. В ній дослідження зроблене на основі індійської та світової практики з метою вивчення особливостей та масштабів порушення прав інтелектуальної власності в цифровому середовищі. Дослідник наголошує на необхідності розробки нового законодавства з урахуванням сучасних реалій, казуючи на нездатність "традиційних" правових механізмів встигати за швидким розвитком Всесвітньої мережі Інтернет та її глобальною роллю.

Серед робіт, присвячених окремим об'єктам інтелектуальної власності та їх використанню в кіберпросторі, варто зазначити дослідження П. Чакраборти по сучасним тенденціям щодо торговельних марок та прав на них у кіберпросторі; Г. І. Зекоса, що здійснив правовий та економічний аналіз авторського права та торгових марок у кіберпросторі; Р. Верми та Н. Тарін - щодо прав на ТМ у кіберпросторі та М. Д. Мюррейа - щодо товарних знаків, NFT та Закону про метавсесвіт. Щодо доменних імен, які є невід'ємним елементом використання Інтернету та предметом палких спорів щодо віднесення їх до об'єктів інтелектуальної власності, слід вказати на роботи М. Зальнерюте - щодо подолання розриву в управлінні в міжнародному законодавстві про доменні імена та приведення UDRP у

відповідність до міжнародно визнаних прав людини, С. Б. Булеци та А. В. Тегзи - по кіберсквотингу, та А. Рудри і С. Белла - по тайпсквотингу.

Окремо група літературних джерел, що використані в роботі над даним дисертаційним дослідженням стосується факту того, що в грудні 2022 року в Україні було прийнято новий Закон про авторське право та суміжні права, який прийшов на зміну нормативно-правовому акту 1993 року. Більш сучасний та такий, що може врегулювати питання, зокрема, дотримання прав щодо "цифрової" інтелектуальної власності, новий закон став предметом жвавих дискусій та наукових розробок багатьох вітчизняних теоретиків та практиків. Так, О. Мисенко в своїх роботах аналізує основні новели вказаного документу (як і К. Зеров), а також окремо досліджує питання компенсації за порушення авторського права в ньому. Перспективи даного закону та виклики, що перед ним постають детально проаналізовані Л. Тарасенком. Заслуговує уваги й робота М. Молокодавець, що присвячена майновим авторським правам на код як результату інтелектуальної діяльності та об'єкти штучного інтелекту. Науковий доробок В. Коноваленка містить якісне обґрунтування умов ілюстрування навчальних видань за нормами означеного нормативно-правового акту 2022 р.

Разом з тим, проблема забезпечення дотримання права інтелектуальної власності у кіберпросторі все ще не була вирішена комплексно, а тому потребує поглибленого наукового опрацювання, що і зроблено в даному дисертаційному дослідженні.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертаційне дослідження виконане відповідно до Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони від 27 червня 2014 р., ратифікованої Законом України від 16 вересня 2014 р. № 1678-VII; Стратегії сталого розвитку

«Україна – 2020», схваленої Указом Президента України від 12.01.2015 № 5, Стратегії розвитку сфери інноваційної діяльності на період до 2030 року, схваленої розпорядженням Кабінету Міністрів України від 10.07.2019 № 526; Національної економічної стратегії на період до 2030 року, затвердженої постановою Кабінету Міністрів України від 03.03.2021 № 179; Загальнодержавної програми адаптації законодавства України до законодавства Європейського Союзу, затвердженої Законом України від 18 березня 2004 р. № 1629-IV; Плану заходів з виконання Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, затвердженого постановою Кабінету Міністрів України від 25 жовтня 2017 р. № 1106; Національної стратегії сприяння розвитку громадянського суспільства в Україні на 2021–2026 роки, затвердженої Указом Президента України від 27.09.2021 № 487; Стратегії розвитку Національної академії правових наук України на 2021-2025 роки, затвердженої Постановою загальних зборів НАПрН України від 26.03.2021 р. № 12-21.

Мета і завдання дослідження. Мета дослідження полягає у розкритті змісту і особливостей забезпечення дотримання права інтелектуальної власності у кіберпросторі з урахуванням світового досвіду та вироблення на його основі пропозиції для України.

Досягнення поставленої мети забезпечено вирішенням таких **задач**:

- розкрити генезис наукових підходів щодо дотримання права інтелектуальної власності у кібернетичному просторі;
- встановити сутність дотримання права інтелектуальної власності у кіберпросторі;
- виділити принципи дотримання права інтелектуальної власності у кіберпросторі в Україні і світі;

- виявити правові форми правові форми дотримання права інтелектуальної власності у кіберпросторі з урахуванням сучасних наукових поглядів;
- встановити суть та місце кіберпростору у інформаційному середовищі;
- розкрити етимологію та зміст цифровізації як елементу кіберпростору у науці та нормативно-правовому регулюванні;
- розкрити категорію якості правового забезпечення функціонування кіберпростору в Україні;
- виділити структуру відносин щодо дотримання права інтелектуальної власності у кіберпросторі;
- розкрити генезу правового регулювання функціонування окремих інститутів інтелектуальної власності у кіберпросторі;
- виявити та розкрити актуальні питання правового регулювання відносин щодо дотримання права інтелектуальної власності у глобальних інформаційних та комп'ютерних мережах;
- виділити правові основи регулювання відносин дотримання права інтелектуальної власності у кіберпросторі в країнах ближнього та дальнього зарубіжжя, зокрема, США, ЄС, СНД;
- проаналізувати особливості діяльності головних міжнародних суб'єктів міжнародно-правової охорони права інтелектуальної власності, зокрема, ВОІВ, ICANN, Internet Society та інших;
- виявити нові підходи до формування правового забезпечення дотримання права інтелектуальної власності у кіберпросторі в Україні;
- встановити ефективність правового забезпечення дотримання права інтелектуальної власності у кіберпросторі в Україні і світі, проаналізувавши шляхи впровадження найкращих світових практик у даній сфері;

- запропонувати концептуальні підходи щодо побудови ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі.

Об'єктом дослідження є суспільні відносини, що виникають у зв'язку із забезпеченням дотримання права інтелектуальної власності у кіберпросторі.

Предметом дослідження є забезпечення дотримання права інтелектуальної власності у кіберпросторі.

Методи дослідження. Загальнонаукові та спеціальні юридичні методи наукового пізнання стали основою для здійснення даного дисертаційного дослідження. Зокрема, поєднання аналітичного та логіко-семантичного методів уможливило сформулювати авторські підходи до таких понять як: «реалізація права», «кіберпростір», «принципи дотримання права інтелектуальної власності у кіберпросторі», «оцифрування», «цифрова трансформація», «місце кіберпростору у інформаційному середовищі», «кібернетичний домен», «інформаційне середовище», «цифрове середовище», «концептуальні засади побудови ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі», «цифровізація (діджиталізація) як елемент кіберпростору», «структура відносин щодо дотримання права інтелектуальної власності у кіберпросторі» тощо (підрозділи 1.1–1.3, 2.1–2.4, 3.1–3.3, 4.1-4.3). Поєднання методів аналізу й синтезу, а також гносеологічного методу дозволило встановити зміст дотримання права інтелектуальної власності у кіберпросторі (підрозділи 1.1, 1.2.) й запропонувати концептуальні засади побудови ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі з урахуванням найкращих світових практик (підрозділ 5.3). Використання структурно-функціонального методу та методу класифікації сприяло виділенню принципів дотримання права інтелектуальної власності у

кіберпросторі в Україні і світі (підрозділ 1.3), визначенню коло суб'єктів, об'єктів та інших структурних елементів відносин щодо дотримання права інтелектуальної власності у кіберпросторі (підрозділ 3.1). За допомогою методів узагальнення, системно-структурного методу, а також методу групування здійснено систематизацію наукових поглядів щодо дотримання права інтелектуальної власності у кіберпросторі (підрозділ 1.1) та правового регулювання функціонування окремих інститутів інтелектуальної власності у кіберпросторі (підрозділ 3.2), виявлено правові форми дотримання права інтелектуальної власності у кіберпросторі з урахуванням сучасних наукових поглядів до їх визначення і застосування (підрозділ 1.4), встановлено суб'єктний склад міжнародно-правової охорони права інтелектуальної власності (підрозділ 4.2), систематизовано наукові погляди й підходи щодо місця кіберпростору у інформаційному середовищі (підрозділ 2.1) й цифровізації як елементу кіберпростору у науці та законодавстві (підрозділ 2.3), а також визначено актуальні питання правового регулювання відносин щодо дотримання права інтелектуальної власності у глобальних інформаційних та комп'ютерних мережах (підрозділ 3.3). За допомогою статистичного та документального аналізу розкрито якісні показники ефективності правового забезпечення дотримання права інтелектуальної власності у кіберпросторі в Україні і світі (підрозділ 5.2). Використання системно-функціонального методу дозволило систематизувати нові підходи до формування правового забезпечення дотримання права інтелектуальної власності у кіберпросторі в Україні (підрозділ 5.1), розкрити категорію якості правового забезпечення функціонування кіберпростору в Україні (підрозділ 2.2). Метод юридичної компаративістики був використаний в процесі аналізу та співставлення правових основи регулювання відносин дотримання права інтелектуальної власності у кіберпросторі в країнах ближнього та дальнього зарубіжжя (підрозділ 4.1).

За допомогою методів дедукції та індукції розкрито генезис наукових поглядів щодо дотримання права інтелектуальної власності у кіберпросторі (підрозділ 1.1) та правового регулювання функціонування окремих інститутів інтелектуальної власності у кіберпросторі (підрозділ 3.2), сформульовано напрямки побудови ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі (підрозділ 5.3). За допомогою прогностичного та порівняльно-правового методів розкрито сутність дотримання права інтелектуальної власності у кіберпросторі (підрозділ 1.2), запропоновано концептуальні підходи до побудови ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі (підрозділ 5.3).

Науково-теоретичне підґрунтя дослідження становлять наукові роботи філософського та соціального спрямування, а також роботи у галузі загальної теорії держави і права, інформаційного права, цивільного права, інших суміжних наукових досліджень, зокрема, роботи зарубіжних науковців. Нормативне підґрунтя дисертаційного дослідження склали Конституція України, Цивільний кодекс та інші кодекси України, низка міжнародних угод та договорів, директиви та Регламенти ЄС, закони та підзаконні нормативно-правові акти, положення яких стосуються забезпечення дотримання права інтелектуальної власності у кіберпросторі. Емпіричною та інформаційною основою роботи склали матеріали узагальнення практики діяльності суб'єктів міжнародно-правової охорони права інтелектуальної власності, матеріали судової практики української та інших держав, а також соціологічні матеріали й довідкові видання.

Наукова новизна отриманих результатів полягає в тому, що дисертація є однією з перших робіт, в якій на основі новітніх здобутків науки інформаційного права та права інтелектуальної власності, з використанням актуальних методів наукового пізнання, комплексно здійснено спробу розкрити сутність і особливості забезпечення дотримання

права інтелектуальної власності у кіберпросторі на основі світового досвіду, що надало змогу обґрунтувати низку висновків концептуального характеру, які є новими, а також надати практичні рекомендації з опрацьованих питань. До основних належать наступні:

вперше:

- обґрунтовано важливість для принципів інтелектуальної власності ґрунтуватися на об'єктивних законах розвитку суспільства та спеціальних законах, які регулюють безпосередньо відносини, що стосується результатів творчо-інтелектуальної діяльності. Визначено, що такі принципи мають відповідати суспільним інтересам, принципам гуманізму, а також моралі, як і основним цілям та завданням української держави в особі відповідних органів публічної влади. Зазначене сприятиме роль наданню більш якісної охорони та захисту суб'єктивних прав суб'єктам права інтелектуальної власності;
- запропоновано визнати у якості загальних інтелектуально-правових принципів (принципів права інтелектуальної власності) наступні: право власності на інтелектуальну власність, що належить їй творцю або передано ним, принцип примусового ліцензування, принцип справедливої поведінки, принцип балансу прав правовласника та громадськості, принцип гармонізації як взаємної узгодженості та підпорядкування єдиній взаємно-відповідній системі нормативних інструментів та стандартів. Слідування відповідним принципам сприятиме забезпеченню належного захисту правам та інтересам правовласників і ,відповідно, активізації творчо-інноваційної діяльності, а також досягненню правової одноманітності;
- запропоновано розуміння місця кіберпростору у інформаційному середовищі як елемента, центрального сегмента системи інформаційного середовища (сфери) на рівні із традиційним інформаційним простором. Виявлено, що в кіберпросторі

сконцентровані глобальні потоки економічно-політичної природи та соціальних взаємин. Обґрунтовано, на основі такого визначення, необхідність формування ефективного та стабільного українського інформаційного простору, що сприятиме встановленню та розвитку стійкого кіберпростору в країні. Обґрунтовано, що виконання такого завдання базується на необхідності посилення нормативно-правового забезпечення функціонування українського кібернетичного простору програмними та регулюючими документами та системою принципів, що включають, зокрема, принципи поваги прав і свободи людини, відповідальності, розумності, усвідомленості та потрібного втручання й деяких інших;

- сформовано визначення оцифрування як процесу створення цифрової об'єктивної форми фізичних об'єктів, що дало змогу розуміти його, з правової точки зору, як один із способів надання об'єктивної форми вираження твору;
- сформовано визначення цифровізації (діджиталізації) як забезпечення або поліпшення ділових та інших процесів шляхом використання цифрових технологій та діджитизованої інформації;
- розроблено рекомендації для владних інститутів, втілення яких сприятиме подоланню викликів у галузі цифровізації й посилення її сильних сторін на різних рівнях;
- запропоновано розуміти структуру відносин щодо дотримання права інтелектуальної власності у кіберпросторі як симбіоз суб'єктів, що вступають у правовідносини з приводу інтелектуальної власності, і доцільного способу зв'язку між ними з основою на суб'єктивних юридичних правах та обов'язках по відношенню до певних соціальних благ чи інтересів у кіберпросторі. Це сприяє якісному та повному розумінню елементів такої структури, і, відповідно,

кращому розумінню особливостей врегулювання відносин з дотримання права інтелектуальної власності у кіберпросторі;

- запропоновано визначення концептуальних засад побудови ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі як основоположного розуміння відповідної побудови ефективного правового забезпечення, сукупність поглядів на неї вчених та практиків, а також нормотворців, що втілюють відповідні ідеї та концепції у нормативно-правове регулювання щодо права інтелектуальної власності у кіберпросторі;
- зроблено порівняння правових засад регулювання відносин дотримання права інтелектуальної власності у кіберпросторі в країнах Європи, Співдружності Незалежних Держав та в США. Обґрунтовано, що для забезпечення такого дотримання в Україні слід: гармонізувати українське законодавство до більшості Директив ЄС з питань захисту інтелектуальної власності, зокрема, в кіберпросторі та запозичити європейську методику превентивного захисту прав власників інтелектуально-творчих об'єктів; прийняти одноманітний закон в рамках СНД щодо відносини інтелектуальної власності в кіберсередовищі й впровадити особливу підвідомчість спорів про захист виняткових прав при використанні контенту у такому просторі арбітражним судам для досягнення правової одноманітності та подолання прогалів у законодавстві;
- запропоновано будувати правове забезпечення дотримання права інтелектуальної власності у кіберпросторі в Україні шляхом: активної співпраці світової спільноти, створення загальновизнаної системи юрисдикції в кіберсередовищі через плідну міжнародну взаємодію, гармонізацію законів та інноваційних підходів; подолання проблеми екстериторіального охоплення та втамування потреби в гармонізації

між юрисдикціями; зазначення у відповідних нормативно-правових актах про віднесення справ з цифрового порушення прав інтелектуальної власності, вчиненого представниками іншої країни, судам своєї держави; подолання технологічної необізнаності; надання правового захисту технологічним методам охорони прав авторів та правовласників та введення в дію жорстких положень щодо відповідальності за обхід технологічних заходів; розробки й нормативного закріплення положень щодо нового розширеного режиму обміну файлами і посилення відповідальності онлайн-посередників; впровадження програм громадської освіти серед інтернет-користувачів тощо;

- визначено головні переваги та недоліки нового Закону України про авторське право і суміжні права 2022 р.;
- обґрунтовано, на основі аналізу передових практик країн світу у галузі забезпечення дотримання права інтелектуальної власності у кіберпросторі, застосування багатогранного підходу, що передбачає правові, технологічні й соціальні рішення та взаємодію;
- запропоновано практичні рекомендації на міжнародному рівні по забезпеченню дотримання права інтелектуальної власності у кіберпросторі, а саме розробка та впровадження в дію: універсального міжнародно-правового акту (конвенції), що б урегулював проблему транскордонності Інтернету як сегменту кіберпростору й цифрового простору загалом, типового (модельного) закону про захист цифрової інтелектуальної власності, з урахуванням відмінності відповідних об'єктів від традиційних об'єктів інтелектуальної власності, уніфікованих правил з протидії кібер-правопорушенням у сфері інтелектуальної власності в Інтернеті та інших глобальних інформаційно-комунікаційних мережах, задля своєчасного попередження викликів та реагуванні на інциденти у

відповідній галузі, із залученням до їх розробки розробки юристів, представників основних міжнародних суб'єктів, чия діяльність пов'язана із функціонуванням кіберпростору, технічних спеціалістів та органи забезпечення міжнародного правопорядку;

- запропоновано практичні рекомендації по удосконаленню національного законодавства задля забезпеченню дотримання права інтелектуальної власності у кіберпросторі, а саме: прийняття Інформаційного Кодексу України, у разі неможливості його прийняття - доповнити діючі нормативно-правові акти, що регулюють інформаційну сферу і безпосередньо кіберпростір положеннями про права і обов'язків інформаційних суб'єктів, про інформаційне забезпечення органів державної влади, а також визначенням правового статусу інформаційних ресурсів з урахуванням права власності, рівнів захисту, доступу до інформації та визначенням суб'єктів правопорушення щодо інтелектуальної власності у кібердоміні, з метою чіткого розуміння щодо визначення відповідних осіб. Обгрунтовано також внесення змін і доповнень до Закону України про авторське право і суміжні права 2022 р.: з метою забезпечення ефективного захисту прав та законних інтересів правовласників - доповнити Статтю 1 визначенням терміну "цифрова інтелектуальна власність", повернути в Статтю 1 визначення терміну «виключне право», зазначити ч. 2 Статті 5 зазначити, що до кола суб'єктів авторського права включено й суб'єктів майнових авторських прав, доповнити п. 39 Статті 1 про приватне копіювання роз'ясненням, яких саме осіб віднесено до "...близьких знайомих такої сім'ї...", внести зміни до ч. 1 Статті 12 щодо невичерпності переліку способів використання творів; з метою забезпечення освітнього процесу - викласти п. 2 ч. 2 Статті 22: у такій редакції: "...відтворення в електронній (цифровій) формі, інтерактивне надання доступу до

правомірно оприлюднених статей та інших невеликих за обсягом творів, художніх творів, а також уривків з письмових творів як ілюстрацій для дистанційного навчання...” (це дозволить вільно використовувати в навчальній діяльності малюнки, фотографії тощо для більш якісного ілюстрування навчального матеріалу), а також доповнити п. 2 ч. 2 Статті 22 у частині переліку суб'єктів вільного відтворення таким суб'єктом як видавництво;

удосконалено:

- визначення реалізації права, на додаток до усталених, як реального, закріпленого на практиці втілення в життя формально-визначених правових розпоряджень шляхом правомірних дій (бездіяльності) суб'єктів суспільно-правових відносин, метою чого є задоволення основних потреб громадян, суспільства та всієї держави в цілому на підставі засобів та методів, встановлених державою в особі своїх органів;
- визначення цифрової трансформації як безпосередньої трансформації бізнесу, що забезпечується діджиталізацією, яке, на відміну від існуючих, охоплює не лише кращу орієнтацію на потребах споживача, але й включає розуміння необхідності проведення цифровізації на підприємстві;
- перелік об'єктів відносин щодо дотримання права інтелектуальної власності у кіберпросторі, який, на відміну від існуючих, включає окрім об'єктів авторських та суміжних прав, об'єктів промислової власності та нетрадиційних об'єктів, інформацію, інформаційні системи, доменні імена, інформаційно-телекомунікаційні технології, інформаційні ресурси й продукти (за концепцією К.В. Єфремової);
- перелік суб'єктів відносин щодо дотримання права інтелектуальної власності у кіберпросторі, який, на відміну від існуючих, включає окрім творців, власників прав інтелектуальної власності,

правонаступників та інших осіб, чия діяльність пов'язана із використанням, захистом результатів творчо-інноваційної діяльності, також і інших учасників відносин в процесі діяльності у кібернетичному просторі (зокрема, онлайн-посередників - провайдерів, операторів зв'язку, реєстраторів, інтернет-реєстри тощо). Обґрунтовано, що таке визначення і правова кваліфікація сприятиме якісному аналізу наявних нормативно-правових актів та розпізнаванню їх уразливих сторін, на основі чого в подальшому можна буде розробляти політики удосконалення відповідного законодавства, розроблення нового й вироблення шляхів розвитку у відповідній сфері;

дістало подальшого розвитку:

- визначення ступеню наукової розробленості проблеми дотримання права інтелектуальної власності у кіберпросторі з огляду на її значущість у захисті прав, свобод, законних інтересів у суспільно-правових відносинах;
- періодизація становлення правового регулювання функціонування окремих інститутів інтелектуальної власності загалом, та, зокрема, у кіберпросторі, що характеризується як загальними закономірностями, так і специфічними ознаками. Обґрунтовано необхідність знати особливості генези правового регулювання функціонування інститутів права інтелектуальної власності у кіберпросторі тим, що на основі таких відомостей можна визначити помилки та недоліки попередніх інструментів забезпечення дотримання відповідних прав і, на такому підґрунті, розробити та впровадити нове, більш досконале, правове регулювання;
- підходи щодо забезпечення дотримання права інтелектуальної власності у глобальних інформаційних та комп'ютерних мережах неюридичними засобами та методами у додаток до правових;

- характеристика кіберпростору з позиції його транскордонності, що є викликає суперечки при віднесенні кіберпорушень до відання того чи іншого правопорядку та негативно сказується на визначенні суб'єктів відповідного правопорушення;
- виявлення кола перешкод та викликів на шляху ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі в різних країнах світу.

Практичне значення отриманих результатів виконаної роботи зумовлене їх завершеністю та обґрунтованістю. Результати виконаної роботи можуть бути використані:

- у правотворчій діяльності – для вдосконалення положень актуальних законів та підзаконних нормативних актів у сфері забезпечення дотримання права інтелектуальної власності у кіберпросторі (лист Секретаріату Уповноваженого Верховної Ради України з прав людини №69396.4/15745/1/24/45.1 від 13.11.2024);
- у правозастосуванні – для здійснення офіційного тлумачення положень законодавства щодо забезпечення дотримання права інтелектуальної власності у кіберпросторі, і, зокрема, при розгляді судових справ у досліджуваній сфері суспільних відносин (лист щодо впровадження результатів дисертаційного дослідження Державної організації «Український національний офіс інтелектуальної власності та інновацій» №8958/2901-06-24 від 25.11.2024, довідка про використання результатів дисертаційного дослідження Державної служби якості освіти України №01/01-23/2413 від 11.11.2024, довідка про впровадження Дочірнього підприємства “Центр компетенції адресного простору мережі Інтернет” Консорціуму “Український центр підтримки номерів і адрес” №1 від 28.10.2024);
- при здійсненні навчального процесу – для видання підручників, навчальних посібників з дисциплін «Інформаційне право», «Право

інтелектуальної власності», інших методичних та навчальних матеріалів, виданні іншої спеціальної літератури з роз'яснення положень актуального інформаційного законодавства та законодавства з інтелектуальної власності про впровадження в освітній процес (акт про впровадження в освітній процес Національного авіаційного університету від 23.10.2024).

Особистий внесок здобувача. Дослідження виконане автором самостійно. У дисертації наукові ідеї та розробки співавторів, а також матеріали і висновки кандидатської дисертації не використовувалися. Усі сформульовані положення, висновки та пропозиції обґрунтовано на основі особистих досліджень автора.

У статті Філінович В. В., Новгородська І.М. Захист прав власників доменних імен. Електронне наукове фахове видання «Порівняльно-аналітичне право». 2019. №5. – С. 136-138 авторський внесок становить 75% і стосується положень щодо визначення сутності та особливостей доменних імен, проблем захисту прав на них та розробки рекомендацій по подоланню таких проблем.

У статті Voronova O., V. Filinovich. The Role of the Web-based Distance Learning Environment in the Education of Future Lawyers. Наукові праці Національного авіаційного університету. Серія: «Юридичний вісник «Повітряне і космічне право». 2020. №4 (57). С. 188–193 авторський внесок становить 50% і стосується положень щодо розкриття особливостей та сутності веб-середовища дистанційного навчання та критичної оцінки основних систем дистанційного навчання у кіберсередовищі.

У статті Filinovich V., Sukhanov O. Domain name in the system of objects of intellectual property rights. Scientific Works of National Aviation University. Series: Law Journal "Air and Space Law". 2022. №3 (64). P. 146–152. <https://doi.org/10.18372/2307-9061.64.16884> авторський внесок становить 75% і стосується положень щодо визначення поняття доменних

імен та їх місця у системі об'єктів права інтелектуальної власності, виявлення проблемних питань у відповідній сфері та розробки пропозицій щодо їх вирішення.

У статті Sopilko I., Filinovych V., Pankova L. O., Obshalov S.V., Chaplynskyi K. O. Protection of Intellectual Property Rights from Cyber Threats in the Global Information Environment. *Novum Jus*. 2023. Vol. 17(1). P. 237–258. <https://doi.org/10.14718/NovumJus.2023.17.1.10> авторський внесок становить 20% і стосується положень щодо встановлення сутності кібербезпеки та пов'язаних з нею кіберзагроз і їх наслідків, а також вироблення рекомендацій по протидії їм.

У статті Sopilko I., Filinovych V., Prudnykova O. V., Krupnova A., Smetanina N. Ensuring the functioning of cyberspace in Ukraine: Legal and technical aspects. *Sapienza: International Journal of Interdisciplinary Studies*. 2024. Vol. 5, no. 3. P. e24055. <https://doi.org/10.51798/sijis.v5i3.787> авторський внесок становить 20% і стосується положень щодо вдосконалення правової основи функціонування кіберпростору в Україні з урахуванням його технічних аспектів.

У статті Sopilko I., Filinovych V. Development of the Internet trust Environment as an Important Element for Cybersecurity. *University law science and education in the challenges of our time : Collective monograph*. Warszawa, 2021. P. 291–30 авторський внесок становить 50% і стосується положень щодо особливостей та перспектив розвитку середовища довіри в Інтернеті як важливого елемента кібербезпеки та конкретних рекомендацій в цьому напрямку.

У статті Filinovych V., Hu Z. Aviation and the Cybersecurity Threats. *Proceedings of the International Conference on Business, Accounting, Management, Banking, Economic Security and Legal Regulation Research (BAMBEL 2021) : Proceedings of the International Conference*, Kyiv, 26–27 August 2021. Amsterdam, 2021. P. 120–126. URL:

<https://doi.org/10.2991/aebmr.k.210826.021> авторський внесок становить 75% і стосується положень щодо наслідків запровадження концепції кібербезпеки та її наслідків для авіаційного сектору та вирішення проблем кібербезпеки в ньому.

Апробація результатів дисертації. Результати дослідження доповідалися та обговорювалися на всеукраїнських і міжнародних науково-практичних конференціях: «АЕРО-2018. Повітряне і космічне право» (м. Київ, 2018 р.), «Юриспруденція в сучасному інформаційному просторі» (м. Київ, 2019 р.), «АВІА-2019» (м. Київ, 2019 р.), «Інноваційний розвиток правової науки в умовах модернізації суспільства» (м. Київ, 2020), «АЕРО-2020. Повітряне і космічне право» (м. Київ, 2020 р.), «Сучасне право в епоху соціальних змін» (м. Київ, 2021 р.), «АВІА-2021» (м. Київ, 2021 р.), «Business, Accounting, Management, Banking, Economic Security and Legal Regulation Research» (м. Київ, 2021 р.), «International Conference: XXI century, new challenges and modern development tendencies of law» (м. Баку, 2021 р.), «Права людини в епоху цифрових трансформацій» (м. Київ, 2022 р.), «Модернізація вітчизняної правової системи в умовах світової інтеграції» (м. Кропивницький, 2022 р.), «Свобода, безпека та незалежність: правовий вимір» (м. Київ, 2023 р.).

Публікації. Основні положення та наукові результати дослідження викладено в 34 наукових працях, зокрема у 14 наукових фахових виданнях України з галузі науки, з якої підготовлено дисертацію, 4 розділах колективних монографій, 4 статтях у зарубіжних наукових виданнях, 3 з яких у виданнях, що проіндексовані в базах даних Web of Science Core Collection та Scopus. Крім того, серед публікацій, які додатково відображають наукові результати дисертації, 12 тез доповідей у матеріалах науково-практичних конференцій різного рівня.

Структура та обсяг дисертації. Дисертація складається зі вступу, п'яти розділів, які включають у себе п'ятнадцять підрозділів, висновків,

списку використаних джерел і додатка. Загальний обсяг дисертації становить 450 сторінок, з яких 370 сторінок основного тексту. Список використаних джерел містить 351 найменувань і займає 56 сторінок, додаток викладено на 6 сторінках.

РОЗДІЛ 1. МЕТОДОЛОГІЯ ДОСЛІДЖЕННЯ ПРОБЛЕМИ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ДОТРИМАННЯ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ У КІБЕРПРОСТОРИ

1.1. Генезис наукових поглядів щодо дотримання права інтелектуальної власності у кіберпросторі

"Навряд чи є найвища з насолод, як насолода творити", - сказав якимось видатний український письменник М. Гоголь. І справді, творчість була відрадою для багатьох людей протягом усієї людської історії. На жаль, далеко не відразу автори, винахідники та інші творці зрозуміли, що можна і потрібно захищати свої права та інтереси. Але коли таке усвідомлення прийшло, з'явилося й поняття "інтелектуальна власність".

Сьогодні інтелектуальну власність розглядають і як об'єкти, що її представляють, і як сукупність правомочностей, яких відповідні суб'єкти набувають у зв'язку зі створенням та використанням таких об'єктів. Але зародження розуміння її суті мало свої особливості. Стрімкий капіталістичний розвиток суспільства, зростання обсягу промисловості - все це сформувало відчутну потребу творців та інших суб'єктів у захисті прав на інтелектуальну власність з боку держави.

Якщо звернутися до епохи Просвітництва, то простежимо, як у побут входить поняття інтелектуальної власності, що пов'язують із творчістю французьких філософів того часу - Руссо, Вольтера, Гольбаха, Дідро та інших. Тоді існувала теорія, за якою всі праці певної людини, як матеріальні речі, так і результати творчої активності, це її безпосередня власність. Відповідно, автор, який створив об'єкт, мав виняткове право розпоряджатися ним.

І все ж почати варто з 1624 р., коли світ побачив Статут про монополії, а також 1710 р., що подарував нам Британський статут Анни. Саме їх по праву вважають витоками патентного та авторського права [273, с. 26]

відповідно, з ними з'являється і концепція інтелектуальної власності. Вперше використання терміна на громадському рівні було зафіксовано у 1769 р., коли його вказали у статті видання *Monthly Review* [211]. Цікавий і факт того, що при заснуванні Північнонімецької Конфедерації її Конституція накладала на неї повноваження із законодавчої активності у сфері захисту інтелектуальної власності (нім. *Schutz des geistigen Eigentums*) [212].

Патентне право як важлива частина права інтелектуальної власності бере свій початок, на думку А. Моссофа, із королівських грантів Єлизавети I на монопольні привілеї (1558–1603 рр.). Через два століття після закінчення правління даної монаршої особи патент являв собою вже цілком законне право винахідника, згідно з яким той отримував винятковий контроль над виробництвом та продажем результатів своєї інтелектуальної праці. Як зазначає вчений, це демонстрація еволюційного шляху патентів від королівської прерогативи до доктрини загального права [241, с. 1255].

У жовтні 1845 р. в Окружному суді Массачусетса слухалась справа про патент *Davoll et al. v. Brown*. У своїй ухвалі за цим кейсом суддя Ч.Л. Вудбері зазначив, що "тільки таким чином можна заохочувати винахідливість і наполегливість, щоб проявити себе таким чином з користю для суспільства; і тільки таким чином ми можемо захистити інтелектуальну власність, розумову працю, твори та інтереси людини так само, як і плоди її чесної праці, як пшеницю, яку вона обробляє, чи стада, що вона вирощує...." [141, с. 2]. Це ще одна офіційна згадка інтелектуальної власності як поняття, концепту.

І все ж таки, знаковими для захисту інтелектуальної власності стали 1883 і 1886 роки, коли було прийнято Паризьку конвенцію з охорони промислової власності (англ. *Paris Convention for the Protection of Industrial Property*) та Бернську конвенцію про охорону літературних та художніх творів (англ. *Berne Convention for the Protection of Literary and Artistic Works*)

відповідно, що по праву вважаються "Бібліями" промислової власності та авторського права. У 1967 р. відповідною Конвенцією у рамках Організації Об'єднаних Націй було засновано Всесвітню організацію інтелектуальної власності. І з цього моменту термін отримав повсюдне використання та загальноприйняте розуміння.

Як зазначив у 2014 р. Ж.Ф. Морен, «глобальний режим інтелектуальної власності нині перебуває у процесі зміни парадигми». Вчений вважає, що до початку поточного століття на глобальному рівні для інтелектуальної власності утвердилися високі стандарти охорони, якими відрізняється європейське та американське законодавство, що зроблено для одноманітного застосування таких норм у всіх державах. На його думку, глобальний режим інтелектуальної власності прагне до формування більшої гнучкості в політиках і надання вільного і широкого доступу до знань, особливо для країн з економікою, яка ще розвивається [240, с. 277].

У зв'язку із вказаним зазначимо, що з кінця минулого століття, коли особливого поширення набула Всесвітня Мережа Інтернет, питання дотримання прав інтелектуальної власності та надання необхідної охорони її об'єктам вийшло на перший план не лише для ВОІВ, а й для всієї світової громадськості.

Дійсно, Інтернет дав нам практично необмежені можливості, зокрема, і для творчості, а також щодо поширення об'єктів своєї креативно-інтелектуальної активності. Сьогодні ми легко розміщуємо у хмарних сховищах книги, музику, ділимося своєю творчістю та результатами винахідницької діяльності на спеціалізованих веб-платформах. Так, вказане допомагає нам, за потреби, не тільки знайти "свого читача", а й залучити фінансування для стартапу чи наукового дослідження. Але, разом з тим, Всесвітня мережа стала осередком безперервних порушень у галузі інтелектуальної власності.

Інтернет - це важливий елемент кібернетичного домену (простору), а тому обидва концепти й будуть розглянуті у даному дисертаційному дослідженні у тісному взаємозв'язку. Їхні поняття та характерні особливості будуть досліджені більш детально у Розділі 1.2.

Якщо повернутися до генези наукових і практичних поглядів щодо права інтелектуальної власності, особливо в кіберпросторі, то відправною точкою в даному питанні варто, на нашу думку, вважати 20 грудня 1996 р., коли ВОІВ, під час Дипломатичної конференції, були прийняті так звані "інтернет-договори", а саме Договір ВОІВ з авторського права та Договір ВОІВ з виконань та фонограм.

Не меншу значущість у цьому питанні мав і Порядок денний з Розвитку (англ. *Development Agenda*) ВОІВ 2007 р., в якому також зазначалися 45 рекомендацій щодо адаптації діяльності цієї організації до конкретних поточних потреб країн, що розвиваються. Спрямовані вони були, крім іншого, на поліпшення ситуації в питаннях доступу інтернет-користувачів (також - *юзерів*) до інформації, програмістів - до вихідних кодів, учнів та студентів - до наукових матеріалів. Але такий зсув парадигми, упевнений Морін, ще не було відзначено у конкретних правових реформах на міжнародному рівні [240, с. 283].

Що стосується поглядів науковців, то варто зазначити думку Н. Елькін-Корен щодо авторського права в кіберпросторі. Прихильниця свободи сторін договору у встановленні будь-яких обмежень на доступ та використання інформації у кібердоміні, вона впевнена, що кіберпростір сприяє зазначеному, тому що дає можливість постачальникам інформації поширювати свої твори на договірній основі. Вчена зазначає, що доступ до матеріалів кіберсередовища може надаватися з урахуванням технічної можливості обмежень при прийнятті умов ліцензії на використання. Вона також використовує спеціальний термін «приватний порядок». По ньому розповсюджувачі інформації можуть встановити права, еквівалентні

авторсько-правовим, але із своїми особливостями. Такі правомочності формуються виходячи з засобів самодопомоги, а не законодавчих норм. Поведінка користувачів та умови отримання ними доступу до інформаційного об'єкта можуть регулюватися системою, що надає такий доступ. Вона ж визначає і умови використання контенту (тобто матеріалів, що містяться на веб-ресурсі), наприклад, дозволяючи читати текст, але забороняючи скопіювати його. Із зазначеного випливає, що мережева архітектура і програмне забезпечення (також - ПЗ), що становлять кіберпростір, можуть визначати тип використання, яким наділяється користувач розміщених в онлайн-доступі матеріалів, тобто мається на увазі традиційне право власності на річ [176, с. 1156-1158].

Н. Елькін-Корен також зазначає наявність двох конкуруючих моделей регулювання використання інформації у кібернетичному домені. Перша базується на традиційному праві власності, створеному та затвердженому централізованими інституціями держави. Друга модель ґрунтується на режимі правил, який все формується у приватному порядку. Тобто існує громадський порядок (в нашому випадку у вигляді авторського права) і приватний порядок (на основі договору, контракту) регулювання доступу до інформації. Вчена наполягає на привабливості переходу до режиму приватного порядку у кіберпросторі, адже тоді творцям інформаційних активів не потрібно буде покладатися на централізовані регулюючі інститути, натомість можна самостійно приймати рішення щодо умов використання свого контенту [176, с. 1159].

Ю.Р. Куїнн-молодший наголошує на тому, що веб-присутність, яка забезпечує використання Інтернету 24/7, має вирішальне значення для будь-якої комерційної справи, тому так активно використовуються права інтелектуальної власності у кібернетичному просторі. При цьому зазначається, що саме інтелектуальна власність (далі – ІВ) – це "ефективний бар'єр для входу", що пов'язане із винятковістю прав на неї. У контексті

патентів дослідник вказує на наявність прямого свідчення на підтримку повсюдного використання прав інтелектуальної власності у кіберпросторі американською бізнес-спільнотою. Таким він вважає тривалу затримку, з якою заявник стикається при спробі отримати патент на бізнес-метод, відповідно, відчувається сильний корпоративний інтерес до цієї форми права ІВ. Тому підприємства, що спеціалізуються на електронній комерції, й намагаються використовувати патентні права у кіберпросторі частіше та частіше. Щодо "бар'єрів для входу", Куїн-молодший вказує на презумпцію дійсності після видачі патентів які об'єктивно виглядають як недійсні. Видані одного разу, вони можуть стати серйозним стримуючим фактором для суб'єктів, які бажають торгувати через Всесвітню мережу. А тому важливо відстежувати факти бар'єрного патентування, щоб унеможливити надання виняткових прав тим суб'єктам, яким де-факто вони не належать. В іншому випадку результатом стане створення мегамонополь, які контролювали б кожен інтернет-транзакцію [253, с. 964-966, 999].

Індійські дослідники також відзначають особливу, набуту інтернетом важливість як інструмента для сектора електронної комерції. Взаємодія кібернетичного простору та індустрії е-комерції нерідко стає однією з причин виникнення проблем, пов'язаних із інтелектуальною власністю, а тому для будь-якого бізнесу важливо захищати останню. Примусова реєстрація інтелектуальної власності є підтвердженням справжності та очікуваної якості продукту чи послуги. У зв'язку зі складністю регулювання кожної веб-платформи відзначають високу ймовірність для кіберпростору стати "розсадником" порушень відповідних інтелектуальних прав, на кшталт прав на доменні імена, торгові марки та авторські права. Саме на останні і наголошують дослідники, відзначаючи такі найбільш поширені причини порушень:

- легкість копіювання творів, захищених авторським правом, в кібернетичному домені. Недобросовісні користувачі,

використовуючи лазівки в режимах авторського права, роблять копії творів, що охороняються, не тільки для приватного використання. Згодом, буває важко відстежити початкового власника такої роботи. На відміну від фізичної передачі авторсько-правового об'єкта, в кіберсередовищі його можна легко поширити за допомогою бездротових каналів між практично необмеженої кількості користувачів, що суттєво посприяло розвитку піратства;

- безліч посилань також може сприяти порушенню авторських прав у кіберпросторі. Так, користувач, перебуваючи на певній веб-сторінці, одним "кліком" (тобто клацанням комп'ютерної миші) по посилальному тексту або зображенню може переглянути зовсім інший сайт, ніж той, на якому користувач знаходиться. На думку дослідників, це не вигідно для сайтів, які заробляють на кількості відвідувачів їхньої домашньої сторінки. А у нашому прикладі посилання, минаючи останню, веде безпосередньо на сторінку пов'язаного сайту. Також посилання можуть створити оманливе враження у юзера про те, що певна сторінка сайту пов'язана з іншою, навіть якщо вони явно відносяться до різних товарів та послуг [221].

Адвокат та науковець Н.Мітра вказав на проблеми, пов'язані із дотриманням авторських прав у кібернетичному домені. Так, під час оцифрування різні компоненти об'єкта, що захищається, отримують можливість виникнути в різних формах шляхом посилань і кадрування практично без необхідності отримати будь-які дозволи, що, відповідно, виливається у неможливість для власників авторських прав контролювати використання їх об'єктів. Дослідник, також як і його колеги, серед основних проблем у сфері виділяє глибокі посилання і вбудовані посилання, додаючи до них кадрування або фреймінг (від англ. *framing*) [238]. Останній термін має на увазі можливість для "веб-авторів" ділити веб-сторінки на так звані "фрейми", тобто незалежно керовані вікна на сайті. Через них користувач

може переглядати веб-сторінки з іншого веб-ресурсу. Таким чином, програміст може «фреймувати» чужі матеріали під своїми банерами та іншим контентом, тобто чужий контент використовується для продажу банерної реклами на іншому веб-сайті [237, с. 24].

Як зазначає Н. Мітра, фреймінг став предметом юридичних суперечок, оскільки автор контенту не відповідає за копіювання та розповсюдження свого авторського права в Мережі, а лише надає браузерам *modus operandi* для отримання захищеного контенту, який використовує користувач у своєму браузері. У зв'язку із зазначеним ведеться дискусія про юридичну можливість "вилучення" деяких елементів з мультимедійного середовища власника авторських прав з їх подальшим об'єднанням із іншим контентом для створення своїх власних похідних робіт. Дослідник упевнений, що часті порушення авторських прав в Інтернеті вимагають більш жорсткого правового захисту. При цьому, зазначає він, відповідальність покладається не лише на законодавців, а й на самих власників авторських прав та організації-розробники програмного забезпечення. Важливо завчасно повідомляти про відповідні права, а також доводити до відома потенційних користувачів ліцензії та обмеження при роботі з кіберконтентом. Детально опрацьована нормативно-правова база та якісне юридичне тлумачення – це ключові фактори для захисту творців від зловживань, що маскуються під виглядом свободи Інтернету. Для зміцнення прав інтелектуальної власності у кібердоміні, який де-факто не має меж, особливе значення має гармонізація міжнародного права та внутрішніх законів [238].

Сучасний технічний рівень розвитку світу зиждеться на застосуванні складних з технічної та структурної точок зору системах, чий правовий захист включає використання ряду структурно пов'язаних об'єктів ІВ. Технології, як прояв останньої, зазвичай включають набір інтелектуальних прав, які допомагають їх реалізувати та захистити. Крім традиційних прав,

дослідник включає у цей комплекс також технологічний досвід практичного застосування технологічного інтелектуального результату, кваліфікацію персоналу та подібні. Сукупність цих елементів, на думку більшості вчених, і забезпечує виробництво конкретного продукту з певними якісними характеристиками із метою отримання конкурентоспроможного високотехнологічного результату. І такі технології як об'єкти ІВ беруть активну участь у формуванні глобального кіберпростору, що тим самим сприяє трансформації застосування правової конструкції інтелектуальної власності. Кіберфізичний світ вже існує, онлайн- і офлайн-світи злилися воедино, зачепивши різні сфери, у тому числі: поширився 3D-друк, що вже змінює виробничі та логістичні процеси багатьох галузей; активно застосовується робототехніка; формуються масштабні бази даних, які підкріплюються просунутою аналітикою, що позитивно впливає на динаміку та якість прийняття рішень.

Можна виділити такі інтелектуальні фактори, які визначають сучасний розвиток світу: штучний інтелект, синтетична біологія, матеріалознавство, до них також додають робототехніку й нано- та біотехнології [9, с. 9]. Варто, на нашу думку, доповнити цей перелік кіберфізичними системами. Спільно з іншими досягненнями творчої діяльності людей вказані фактори стали каталізатором виникнення нової об'єктивної реальності, з якої складається сучасний кіберпростір. До неї ввійшли Інтернет речей (англ. *Internet of Things, IoT*), глобальні бази даних (англ. *Big Data*), мобільні технології, соціальні мережі та медіа, гаджети (тобто "розумні" високотехнологічні пристрої), системи бізнес-аналітики, хмарні технології (англ. *Cloud Computing*) [159, с. 287, 313, 315, 555] та інтелектуальні системи (англ. *Smart Everything*) [308] тощо.

Назване дійсно важливе, адже кібертехнології справляють потужний вплив на різноманітні управлінські структури, у тому числі державні органи, сприяють поширенню та спрощенню доступу громадян до

державних послуг (наприклад, в Україні діє цифрова система Дія). Відповідно, роль інтелектуальної власності, до якої належать і інформаційні технології, дуже велика, а, отже, вимагає якісного детального регулювання та захисту. І це питання хвилює не лише Україну, воно давно вже перейшло у глобальний вимір.

Проведений у даному розділі дисертаційного дослідження аналіз доктринальних підходів до визначення проблем у сфері охорони та захисту прав інтелектуальної власності та дотримання відповідних прав у кіберпросторі дав можливість виділити низку ймовірних загроз для інтелектуально-правових об'єктів, а саме:

- кіберпростір, головним елементом якого варто вважати всесвітню мережу Інтернет, не має єдиного централізованого управління, а також відокремленого майна, що ускладнює процес захисту порушених прав та превентивної охорони відповідних об'єктів і накладення відповідальності за такі порушення;
- у кібернетичному домені складно проконтролювати використання та розповсюдження об'єктів ІВ, так само як і довести факт ймовірного порушення, адже дані, що розміщуються, та інший контент легко видалити або модифікувати дуже швидко;
- не завжди існує можливість представити об'єкт ІВ у формі іншій, ніж цифрова, з подальшою необхідністю його розміщення або передачі через Інтернет, що полегшує завдання зловмисникам-цифровим піратам;
- транскордонний характер кібернетичного простору суттєво ускладнює реалізацію норм національного законодавства у цьому аспекті.

Отже, широке поширення та застосування цифрових технологій сьогодні, на нашу думку, вже змінює характер правозастосовної практики захисту інтелектуальних прав авторів та інших правовласників, також

відзначається вплив на збереження персональних даних учасників кібернетичного обороту інтелектуальної власності. Таким чином, можна зробити висновок про формування нового виду інтелектуальної власності - "кібернетичної власності" або "кібервласності".

Сьогодні перед інститутом ІВ виникли нові виклики та загрози у зв'язку з активною взаємодією суб'єктів відповідних прав у кіберпросторі. Так, все частіше з'являються нові інтелектуальні об'єкти, що потребують охорони відповідно, список "традиційних" об'єктів ІВ має бути розширений і гармонійно врегульований.

Єдиної стратегії досягнення балансу між бажаннями споживачів цифрового контенту та правовласниками ІВ не існує. Тому важливо підходити комплексно до вирішення цього завдання, з урахуванням не лише нормативних аспектів, а й доктринальних ідей, поглядів вчених, а також думки інформаційної кіберспільноти.

1.2. Дотримання права інтелектуальної власності у кіберпросторі як предмет наукового дослідження

Пошук сучасних підходів до розуміння інтелектуальної власності у кіберпросторі, аналіз наявних і розробка нових форм, моделей і способів забезпечення дотримання відповідних прав дійсно важливі для формування не тільки предмета та методології дослідження відповідних концептів та основ, але і для створення дієвих рекомендацій щодо поліпшення поточного регулювання відповідних відносин в Україні та навіть на міжнародному рівні. Ми сьогодні можемо спостерігати певний плюралізм підходів до поняття, що розглядається, і його суті, єдиного загальноприйнятого підходу досі не існує.

Зрозуміло, що такий стан речей має своїм результатом недостатність чи навіть відсутність дійсно адекватного регулювання та якісної правової політики, що відповідають сучасним реаліям та викликам сьогодення.

Тому важливо насамперед провести теоретико-методологічний аналіз наявних підходів до розуміння не лише самої інтелектуальної власності, а й кібернетичного простору як одного із найважливіших вимірів її використання, щоб пізніше обґрунтовано перейти до формування фундаменту забезпечення дотримання прав творців та правовласників у відповідному полі.

У зв'язку із вказаним зазначимо, що на рубежі нинішнього та минулого століть у соціальних науках з'явився та укорінився безпосередньо пов'язаний із кіберпростором термін «глобальний інформаційний простір», що було викликано, насамперед, вельми інтенсивним та масовим впровадженням новітніх досягнень інформаційно-технологічної революції по всій земній кулі. Дане поняття у зарубіжних джерелах використовується у вузькому сенсі як «глобальний кіберпростір» (англ. *global cyberspace*).

Отже, підходів до визначення та розуміння кіберпростору є декілька. Далі ми їх розглянемо разом із пов'язаними категоріями та термінами.

Сама назва такого поняття походить від англійського терміна *cyberspace*, що складається з двох частин: «*cyber*», тобто «цифровий» та «*space*» - «простір». Вперше термін «кіберпростір» з'являється 1984 року у книзі «Нейромант» У. Гібсона. І хоча сам автор критикував таку назву, вважаючи її "безглуздою", але її і зараз використовують по всьому світу для опису об'єктів і функцій, що стосуються всесвітньої глобальної мережі. У Гібсона кіберпростір сприймався як узгоджена ілюзія (галюцинація), яку щодня випробовується безліччю користувачів у світі. На відміну від нього, розробник Ч. Морнінгстар вважав кіберпростір середовищем для соціальної взаємодії, а не його технічним виконанням (реалізацією) [233, с. 31].

Відповідно до підходу Д. Холліса, під даним поняттям варто розуміти технічну архітектуру, яка забезпечує функціонування Інтернету як всесвітньої глобальної мережі [199]. Юридичний словник Дюема ототожнює кіберпростір із Інтернетом, називаючи його децентралізованою,

але при цьому взаємопов'язаною сукупністю даних та автономною телекомунікаційною мережею [154]. Аналогічно і юридичний словник Фарлекс, при спробі дізнатися сутність поняття "cyberspace," перенаправляє користувача на веб-сторінку, присвячену терміну "Інтернет", під яким розуміє всесвітню телекомунікаційну мережу, що складається із підключених до неї комп'ютерів бізнес- та урядових суб'єктів, а також персональних комп'ютерів [153].

Р. Джа впевнений, що кіберпростір варто розглядати як такий, що представлений використанням технічного обладнання та електромагнітності для обміну, зберігання та модифікації даних за допомогою скоординованих структур та пов'язаних із ними реальних органів та установ. Таким чином, кіберпростір і, особливо, Інтернет варто розглядати як взаємозв'язок фізичних осіб за допомогою комп'ютерів та засобів передачі даних, при цьому фактична географія великої ролі не грає [224].

Т. Фолсом визначає кібернетичний простір як мережу, що комутується, для переміщення інформаційного трафіку, яка характеризується різними рівнями доступу, інформаційної активності, навігації, довіри до неї. Вчений не ототожнює даний концепт із Інтернетом, який в його розумінні є спеціальним інструментом, що створює і відкриває ворота (шлюз) у кіберпростір. При цьому набір дій, що становлять кіберпростір з іншого боку шлюзу і сам шлюз у сукупності виявляють собою об'єктивний кіберпростір зі значеннями, які можуть виникати з його цілей [185, с. 80].

В.М. Фурашев визначає кіберпростір як форму співіснування особливого комплексу матеріальних та нематеріальних об'єктів і процесів, які націлені на взаємодію із інформацією - її створення, засвоєння, запам'ятовування, переробку та взаємообмін такими даними та відомостями [112, с. 164].

Таким чином, погодимося із думкою В. Кумар про те, що термін «кіберпростір» не має стандартизованого, уніфікованого або єдино вірного визначення. Натомість поняття просто використовується для опису систем, які поширюються та функціонують через глобальну мережу підключених комп'ютерів. Відповідно, кіберпростір — це інтерактивний домен, що складається із цифрових мереж, які використовується для зберігання, зміни, передачі та подібних дій із інформацією. І кіберпростір безпосередньо включає глобальну Інтернет-мережу [233, с. 4].

Відповідно до Д.В. Дубова та М.А. Ожевана, все ще зберігаються сумніви щодо можливості використання у суто практичній площині терміна «кіберпростір», і це з урахуванням множинності підходів до його розуміння у науковій літературі та закріплення у офіційних документах. Дослідники впевнені, що це спричинило те, що багато країн все ще використовують застаріле "традиційне" законодавство щодо боротьби із кіберзлочинами (наприклад, нормативно-правовий акт (далі - НПА) з порушення телекомунікаційних мереж, набуття несанкціонованого доступу до даних тощо) [25, с. 4].

Що стосується міжнародно-правових актів, то термін, що розглядається, фігурує в п. 8 Окінавської хартії глобального інформаційного суспільства, згідно з яким узгоджена активність зі створення не тільки безпечного, а й вільного від злочинності кіберпростору є тим, на що мають бути спрямовані зусилля міжнародної спільноти з метою розвитку Світового інформаційного суспільства [57].

Також згадка про кіберпростор є в Угоді про кібербезпеку між США та Китаєм 2015 (англ. *United States–China Cybersecurity Agreement*), у проекті Закону про електронну безпеку кіберпростору 1999 р. (*Cyberspace Electronic Security Act of 1999*, також відомий як *CESA*). Проект Закону про захист кіберпростору як національного надбання США S.3480 від 2010 р. (англ. *S.3480 - Protecting Cyberspace as a National Asset Act of 2010*) визначив

цей термін як взаємозалежну мережу інформаційної інфраструктури, елементами якої є телекомунікаційні мережі Інтернет, комп'ютерні системи та вбудовані процесори та контролери, що використовуються в критично важливих галузях [252]. Але цей документ також локальний, до того ж не набув чинності. Ще у 2018 р. Д. Трампом було підписано нову Національну кіберстратегію, в якій вказувалося на необхідність боротьби із вразливістю в кіберпросторі, якісного управління кібербезпекою шляхом ідентифікації інтернет-користувачів та захисту мереж, даних та виявлення кіберінцидент, спрямованих проти країни [135].

Окремо також розглянемо стандарти Національного інституту стандартів і технологій США (*The National Institute of Standards and Technology*, скорочено - NIST). Спільно з Американським національним інститутом стандартів (ANSI) даний суб'єкт розробляє стандарти та специфікації до програмних рішень. Так, згідно з NIST SP 800-30 Rev. 1, NIST SP 800-39 та NIST SP 800-53 Rev. 4, кіберпростір – це глобальна сфера (область) в інформаційному середовищі, до складу якої увійшла взаємозалежна мережа інфраструктур інформаційних систем, у т.ч. комп'ютерні системи, вбудовані процесори та контролери, а також телекомунікаційні мережі та Інтернет безпосередньо [201, с.53], [202, с.62], [272, с.86]. У другому томі NIST SP 800-160 дано дещо інше визначення, а саме: кібернетичний простір - це взаємозалежна мережа інфраструктур інформаційних технологій, що включає телекомунікаційні мережі разом із Інтернетом, комп'ютерні системи, вбудовані процесори, контролери у критично важливих галузях [295, с.59]. У NISTIR 8074 (том 2), де міститься додаткова інформація до міжвідомчого звіту про стратегічну участь уряду США в міжнародній стандартизації для досягнення цілей країни у галузі кібербезпеки, термін, що розглядається, визначений як специфічне середовище, яке не існує у фізичній формі, і виникло як результат взаємодії

людей, програмного забезпечення та інтернет-сервісів, що проводиться за допомогою технологічних пристроїв та підключених мереж [279, с.48].

У процесі визначення концепту кіберпростору було досліджено Інтернет, але варто все ж таки приділити розумінню його суті особливу увагу, адже він є ключовим елементом кібернетичного домену. Так, Словник Farlex визначає його як всесвітню телекомунікаційну мережу, що поєднує у собі ділові, урядові та комп'ютери для приватного використання. Всесвітня мережа, як ще називають Інтернет (або просто Мережа), була розроблена в 1969 для цілей Міністерства оборони Сполучених Штатів Америки. Далі Мережа почала використовуватися у дослідницьких колах і стала відома як ARPANET, у такому вигляді вона проіснувала до 1990 року. На зміну їй прийшла Мережа NSF (NSFNET), Інтернет став набувати рис відомого сьогодні нам. У середині останньої декади 20-го століття Всесвітня павутина, як стали називати Мережу (від англ. *World Wide Web*, *WWW*), вже набула цілком операбельного мультимедійного інтерфейсу, який дозволяв передавати текст, зображення, аудіо- та відеоматеріали [219].

Інтернет, давши нам свободу комунікації і забезпечивши простоту у здійсненні звичайних справ та навіть веденні бізнесу, тим не менш, став приводом для різних конфліктів. Одним із каменів спотикання стало право на свободу слова. Саме навколо нього багато дебатів точилося через можливість використання Інтернету дітьми, адже в Мережі нерідко зустрічається контент, який не підходить для неповнолітніх. Противники такого підходу наполягали на неадекватності зведення Мережі лише до тих даних, які є прийнятними для дітей.

Не менш важливим аспектом інтернет-існування став захист власників авторських та інших прав інтелектуальної власності від піратства, яке набуло надто великих масштабів за останні десятиліття. Також проблемною сферою в контексті Мережі вважається поширення небажаної реклами, так званого "спаму", вірусів та постійне зростання кіберзагроз.

Саме тому навіть противники *Internet Governance*, тобто управління Інтернетом, згодні з тим, що певне нормативне регулювання Мережі все ж таки потрібне. З розвитком Інтернету його середовище стає все більш стандартизованим, але все ще вимагає регламентації, про що йтиметься у наступних розділах даного дисертаційного дослідження.

Таким чином, можна говорити про те, що, з урахуванням деяких винятків у вигляді названих вище міжнародно-правових актів та декількох інших (Будапештська конвенція про кіберзлочинність 2001, ратифікована Україною 07.09.2005 та ще не введена в дію Конвенція Африканського союзу про кібербезпеку персональних даних), на даному етапі міжнародне право не має спеціальних норм і правил для регулювання взаємовідносин у кіберпросторі. Як зазначає Д. Холліс, питання про застосування діючого міжнародного права до кіберпростору деякий час залишалося відкритим, але сьогодні багато країн та деякі міжнародні організації, серед яких Перший комітет Генеральної Асамблеї ООН з роззброєння та міжнародної безпеки, Європейський союз, Асоціація держав Південно-Східної Азії (АСЕАН), Організація американських держав та G-20 (група двадцяти, англ. *The Group of Twenty*) вже підтвердили свій намір вважати норми чинного міжнародного права такими, що застосовуються щодо використання інформаційних та комунікаційних технологій по країнах. Таким чином, як вважає дослідник, сьогоднішня тенденція полягає не у вивченні можливості застосування міжнародного права, а в тому, як це відбувається [199].

Відмітимо, що саме нематеріальна природа кібернетичного простору істотно ускладнила визначення та обґрунтування його правових основ із подальшим їх нормативним закріпленням.

Національне українське законодавство з цього питання представлено насамперед Законом 2163-VIII Про основні засади забезпечення кібербезпеки України від 05 жовтня 2017 року. Цей НПА регулює основи

забезпечення захисту національних інтересів країни у кіберпросторі, а також життєво важливих інтересів основних суб'єктів відповідної взаємодії – людини та громадянина, суспільства та держави. До його відання також віднесено основні цілі та принципи держполітики, повноваження та принципи координації діяльності держорганів, установ та інших суб'єктів з метою забезпечення кібербезпеки. У п.11 статті 1 цього документу дано визначення кіберпростору як віртуального простору, середовища, створеного у результаті функціонування з'єднаних, сумісних комунікаційних систем та забезпечення електронних комунікацій із використанням глобальної інтернет-мережі або інших глобальних мереж передачі даних. І такий простір дає кожному можливість вести комунікацію та реалізовувати у ньому суспільні відносини [79].

Сьогодні можна сміливо сказати (посилаючись на міжнародну практику), що винахідники, письменники та інші творці можуть подавати заявки на визнання їхніх прав та реєстрацію відповідних інтелектуально-правових об'єктів завдяки законодавству про інтелектуальну власність у цифровому просторі. Ми все частіше маємо справу з інноваціями, і їхні творці прагнуть не лише прославити себе, а й монополізувати, а також отримати вигоду зі своїх творінь. Таким чином, права інтелектуальної власності проявляють себе аналогічно матеріальним активам, які ми можемо придбати, продати, ліцензувати і не тільки.

Інтелектуальна власність не має єдиного вичерпного переліку об'єктів, її складових. Найчастіше, коли йдеться про кібернетичний домен, мають на увазі об'єкти авторських та суміжних прав, патентів, доменні імена, товарні знаки та права на дизайн. Хоча, зрозуміло, і більш традиційні об'єкти можуть тією чи іншою мірою використовуватись чи іншим способом бути пов'язаними із кібернетичним виміром.

Так, авторське право в інформаційному кіберсередовищі зазвичай включає "твори в галузі науки, літератури та мистецтва", а саме літературні

письмові, музичні (з текстом і без), аудіовізуальні, ілюстраційні, фотографічні, їх переклади і похідні роботи, а також карти, ескізи, креслення тощо. Окреме місце в контексті "цифрової складової" посідають у цьому переліку комп'ютерні програми та бази даних. Крім зазначених, існують й інші об'єкти авторського права, згідно зі Статтею 2 Закону України № 3792-ХІІ про авторське право та суміжні права (від 23.12.1993) (драматичні твори, постановки, твори архітектури, образотворчого та прикладного мистецтва тощо) [67], але їх, в силу форми, дуже важко використовувати у кібернетичному аспекті.

Важливо уточнити, що п.3 зазначеної статті гарантує охорону саме формі вираження результату творчої діяльності, але ніяк не ідеям, методам, принципам, процедурам, способам тощо. При цьому, як зазначає І.Сопілко, авторське право на відповідний матеріальний інтелектуально-правовий об'єкт не завжди збігається із правом власності на матеріальний носій, у якому такий об'єкт знайшов своє вираження. Тому на такий носій можуть існувати окремі права власності та користування, при цьому авторського права тут не буде [102, с. 112].

Найчастіше у кіберпросторі авторські права порушуються шляхом нелегального завантаження відеоконтенту, музичних композицій та піратського програмного забезпечення. Нерідко зустрічається також передрук текстових матеріалів, розміщення чужих зображень на веб-ресурсах тощо. Подібні порушення легкоздійсненні, що викликано простотою:

- відтворення (тобто створення копій). Так, після публікації об'єкта в електронній, тобто цифровій формі, його можна скопіювати швидко, без особливих витрат і втрати якості. А з такого дубліката можна зробити нові копії;
- поширення. Використання інтернет-технологій дозволяє не тільки легко завантажити цифровий об'єкт у кіберпростір, але з такою ж

легкістю та швидкістю можна його поширити серед інших користувачів;

- зберігання. "Місце" для зберігання контенту у кібернетичному домені практично не обмежене.

Ш. Сінгх вважає, що головна проблема авторського права в кіберпросторі полягає у проведенні різниці між приватним та публічним використанням творів. Так, публічне використання має здійснюватися за згодою правовласника. Головна вимога за приватного використання - сумлінність користувача [275]. У зв'язку із зазначеним, К. Мантрі відзначає тенденцію сприймати виготовлення копій для особистого (приватного) використання цілком сумлінним та законним. Але такі копії легко "витікають" у Мережу під час обробки, а потім - дуже важко знайти особу, якій належить авторське право на такий об'єкт. Дослідник окремо вказує на проблеми, що виникають у зв'язку із створенням похідних об'єктів, тобто тих, що були засновані на наявному захищеному творі, наприклад, як у випадку з ПЗ, коли незалежні програмісти вносять до наявної програми виправлення чи оновлення. У цьому контексті К. Мантрі наводить приклад двох кейсів. Так, у справі *Midway Mfg. Co проти Artic Int'* судом було вирішено визнати модифікацію ПЗ несанкціонованою адаптацією твору. У той же час у справі *Lewis Galoob Toys Inc проти Nintendo of America* судовий орган при винесенні рішення посилався на те, що порушення авторських прав не було, адже не було створено нову програму [236].

Що стосується патентів та об'єктів інтелектуальної власності, що ними охороняються, в кіберпросторі, то важливо зазначити, що комп'ютерні програми та інше ПЗ, яке визнано об'єктом авторського права за законодавством України та країн-учасниць Бернської конвенції, не підлягає патентуванню. Цей факт суттєво обмежує можливості розробників ПЗ щодо захисту своїх об'єктів та їх монетизації.

Взагалі, патент - це "охоронний документ, що засвідчує пріоритет, авторство та права на винахід (корисну модель)", згідно зі статтею 1 Закону України № 3687-ХІІ Про охорону прав на винаходи та корисні моделі (від 15.12.1993). Стаття 6 цього НПА декларує 20-річний період чинності майнових прав ІВ на винахід [81]. Такий документ, по суті, наділяє винахідника або іншого правовласника правом забороняти третім особам виробляти, використовувати, продавати такий винахід протягом певного терміну з моменту подання заявки на видачу патенту. Патентну охорону зазвичай слід вимагати в кожній окремо взятій державі, де така охорона потрібна. Хоча з урахуванням дії особливих міжнародно-правових актів, наприклад, Договору про патентну кооперацію, процедура може бути суттєво спрощена. Патентування - відмінний стимул для новаторів творити, наділяючи їх винятковим правом на створені винаходи та даючи можливість монетизувати свою діяльність.

У цьому контексті варто також розглянути так звані Інтернет-патенти, які захищають певний спосіб ведення бізнесу у Всесвітній мережі. Також вони відомі як «патенти на методи ведення бізнесу». Одіозним прикладом таких можна назвати історію інтернет-магазину Priceline.com, який запатентував свою орієнтовану на покупця бізнес-модель «назви свою ціну» [207].

Не завжди природа нового методу ведення бізнесу чи нової ідеї може бути ефективно захищена саме патентом. Особливий тип захисту в даному випадку може забезпечити режим комерційної таємниці. Стаття 505 Цивільного кодексу України (в останній редакції від 22.06.2022 р.) такою вважає інформацію, яку слід вважати секретною з точки зору її невідомості (в повній мірі або в частині) особам, які зазвичай взаємодіють із даними такого типу. Саме тому така таємниця і наділена особливою комерційною цінністю, також щодо неї були попередньо проведені відповідні заходи з метою збереження її секретності. У п.2 зазначеної статті міститься перелік

типів відомостей, які можуть бути віднесені до комерційної таємниці, а саме "технічного, організаційного, комерційного, виробничого та іншого характеру", з цього списку виключено інформацію, яка згідно із законом не може набути статусу комерційної таємниці [116].

Таким чином, ми маємо справу із конфіденційними даними або певною приватною інформацією, що використовуються у бізнесовій діяльності. Така таємниця не просто має комерційну цінність, але і завдяки їй забезпечує своїм власникам конкурентну перевагу на ринку або у галузі. Зазвичай встановлення прав на комерційну таємницю відбувається шляхом підписання відповідної угоди, за якою всі сторони, що підписалися, зобов'язуються дотримуватися секретності (конфіденційності). Але не варто вважати, що угода про нерозголошення точно вбереже компанію від конкурентів, адже вони такий документ не підписували, а тому можуть почати самостійно розробляти конкуруючий продукт. Для цих цілей варто все ж таки подати заявку на видачу патенту.

Торгові марки (також - ТМ, товарні знаки, знаки для товарів та послуг) є відмітними позначеннями, які допомагають відрізнити товари та послуги одного виробника (постачальника) від однорідних товарів та послуг іншого. Важко уявити успішний бізнес без відповідної унікальної його ідентифікації. Найчастіше ТМ складається зі слів, фраз, символів, комбінації названого тощо. Таким чином, головна мета використання товарного знаку полягає в ідентифікації комерційного джерела, походження товару та послуги. Завдяки такій ідентифікації споживач будує свої очікування щодо певного продукту. Також ТМ - це символ для постачальників послуг, виробників товарів пропонувати дійсно якісні продукти з метою підтримки своєї ділової репутації.

Торговий знак - це також форма власності, і відповідні права можуть встановлюватись шляхом фактичного використання у комерційній діяльності або шляхом реєстрації знака у відомстві. Стаття 16 Закону

України №3689-ХІІ Про охорону прав на знаки для товарів та послуг (від 15.12.1993) у п.2 декларує право власника свідоцтва на ТМ використовувати її, при цьому у п.4 зазначено, що таким використанням, в т.ч., варто вважати застосування знака у мережі Інтернет [82]. Законодавство також уповноважує власника ТМ запобігати несанкціонованому її використанню.

З переходом торгівлі у цифрове середовище перед охороною товарних знаків виникло багато нових проблем. До них М. Тарін відносить гіпертекстові посилання, коли такі розміщені між веб-сторінками, але ведуть не на сайт заявленої торгової марки, а на електронний ресурс того, хто нечесно використовує таке позначення. Як приклад надана ситуація, коли користувач клікає за посиланням з логотипом Гуччі, а потрапляє не на офіційний сайт компанії, а на сайт з контрафактною продукцією, що імітує товари зазначеного бренду. Аналогічно працює і використання ключових слів із назвою брендів тими суб'єктами, які жодного відношення до таких брендів не мають. Це дозволяє збільшити трафік відвідувань на своєму ресурсі, заманивши юзерів туди обманним шляхом [282].

Не менш проблемним для кіберпростору є такий інтелектуально-правовий об'єкт як доменне ім'я. Відповідно до вищезазначеного Закону України №3689-ХІІ (Стаття 1), доменним варто вважати ім'я "що використовується для адресації комп'ютерів та ресурсів в Інтернеті" [82]. Простою мовою - це ім'я-адреса, яку користувачі Мережі використовують для того, щоб відвідати конкретний веб-сайт, тобто, це особливий ідентифікатор комп'ютера в Інтернеті, зазвичай у вигляді набору символів. Насправді такий набір, пов'язаний із IP-адресою пристрою (від англ. *Internet Protocol*, тобто «міжмережевий протокол») важко прочитати і складно запам'ятати. Тому замість нього для користувачів пропонуються цілком зрозумілі альтернативи - доменні імена, що складаються зі слів, цифр і символів, як, наприклад, <https://nau.edu.ua/>.

Важко зараз уявити більш-менш прибуткове підприємство, яке не має свого представництва в Інтернеті, тобто свого веб-сайту. Найчастіше постачальники товарів та послуг прагнуть зареєструвати доменне ім'я, яке б відповідало назві ТМ, бренду чи компанії. Забігаючи наперед, зазначимо, що, згідно із чинними в нашій країні Правилами домену .UA, якщо особа хоче зареєструвати доменне ім'я безпосередньо в зоні .UA, тобто те, що матиме вигляд "бренд.UA", то делегування такого позначення можливе лише після реєстрації відповідного товарного знака правовласниками [111, с. 196].

Таким чином, реєстрація доменного імені та його подальше використання найчастіше стикається з такими проблемами:

- *кіберсквотинг* (від англ. *Cyber-squatting*). Мається на увазі реєстрація доменного імені (далі - ДІ), що відповідає товарному знаку певної компанії, але ще не зареєстровано нею. Третя сторона з метою наживи здійснює реєстрацію на себе відповідного ДІ, а після - вимагає від компанії-жертви оплатити передачу їй такого за велику суму грошей. І доки зловмисник вважається власником даного ДІ, постраждала компанія не може стати власником доменного імені, що відповідає її бренду, відповідно, її право на реєстрацію порушується;
- *зворотний кіберсквотинг*. Ця ситуація передбачає висування хибних звинувачень реальними власниками ТМ з метою оволодіти доменним ім'ям особи, яка зареєструвала його добросовісно;
- *кібер-паразитизм*. У даному випадку дохід надходить порушнику за допомогою використання фактичного доменного імені, що включає схоже або неправильно написане ДІ, яке дуже схоже на ім'я відомої ТМ. Найчастіше під такими доменами-паразитами функціонує сайт з контрафактною продукцією, а недосвідчені користувачі купують її з повною впевненістю придбання на офіційному сайті.

Можна говорити, що ДІ - це засіб ідентифікації компанії, із функціями аналогічними ТМ. А в нинішніх реаліях, коли для багатьох віртуальний світ став не менш важливим, ніж світ реальний, саме доменні імена виходять на перший план у комерційній діяльності. А тому їхній захист потребує чималих зусиль і є вельми важливим.

Коли йдеться про ДІ та ТМ, при їх захисті власнику прав на такі об'єкти важливо мати можливість довести факт їхньої реєстрації, ступінь схожості з чужими об'єктами, факт загальновідомості тощо. І якщо товарні знаки вже давно стали об'єктом ІВ, а їхня охорона надається у відповідності не лише із локальним, а й з міжнародним законодавством, то доменні імена все ще досить часто стають об'єктами суперечок та судових розглядів.

Що стосується дизайну, наприклад веб-сайту, то найчастіше охорона йому надається в рамках авторського права. Це цілком логічно, адже ми маємо справу із графічним об'єктом. Але якщо йдеться не лише про сайт, чи окремі ярлики і зображення на ньому, а й, наприклад, про вмонтоване ПО, або продукт компанії, то найвигіднішим є отримання свідоцтва на промисловий зразок (англ. *industrial design*). Справа в тому, що дизайн часто стає "обличчям" компанії або бренду поряд із згаданим товарним знаком, а отже, і охорона йому потрібна максимальна. Відповідно до статті 1 Закону України № 3688-ХІІ Про охорону прав на промислові зразки (від 15.12.1993), відповідним зразком варто вважати "результат інтелектуальної, творчої діяльності людини у галузі художнього конструювання" [83].

Свідоцтво на промисловий зразок, особливо якщо воно отримане ще до виходу продукту на ринок, закріпить перевагу компанії, оскільки позбавить конкурентів можливості скопіювати її продукти, сайт (його окремі елементи або весь інтерфейс в цілому), а також інші об'єкти ІВ, в тому числі елементи інтерфейсу додатків (застосунків) та програм, шрифти. На практиці дизайн веб-сайтів найчастіше відноситься саме до фізичних характеристик продукту, відповідно виключається застосування до ПЗ як

такого. Натомість він застосовується до конкретного пристрою, де використовується таке ПЗ, але є й виключення.

Отже, інтелектуальна власність у кіберпросторі може існувати та використовуватися практично так само легко, як і у традиційних формах. І хоча кібер-складова сильно спростила користувачам життя, але і стала свого роду прокляттям для власників прав інтелектуальної власності. У Мережі щодня відбувається безліч кібер-порушень, і довести їх дуже непросто. Інформаційні та інші технології розвиваються семимильними кроками, а тому якісне регулювання відповідної сфери не завжди за ними встигає.

Так, законів про боротьбу з кіберпорушеннями багато в усьому світі, але вони далеко не завжди ефективні. Кібербезпека персональних комп'ютерів, організацій і навіть цілих країн нерідко опиняється під загрозою, адже кіберзловмисники володіють сучасними методиками та інструментарієм, який постійно розвивають та модернізують. Гібридні цифрові мережі та мультимедіа все частіше стикаються із новими проблемами в силу технологічного розвитку, а отже, нові закони для вирішення проблем у сфері забезпечення прав інтелектуальної власності у цифровому світі є особливо важливими.

Вказане нормативно-правове регулювання має врахувати специфіку кібернетичного простору, а також суть об'єктів інтелектуальної власності. Тому важливо пам'ятати про транскордонність кібердомена взагалі та Інтернету зокрема, так само як і про необхідність пошуку ідеального балансу між правами авторів, новаторів, творців та споживачів результатів їхньої інтелектуально-творчої праці у кібернетичному просторі. В іншому випадку, при нормативному закріпленні надто очевидного "перегину" на користь правовласників, у майбутньому нам доведеться забути про режим суспільного надбання для об'єктів ІВ, а також про безоплатне (або на лояльних умовах) використання деяких з них, що ще сильніше позначить

розрив між різними соціальними групами за матеріальною ознакою. Не останню роль у цьому відіграють створення та забезпечення ефективного управління майном, а також спеціальних механізмів захисту. Таким чином, важлива гармонія між правами приватної власності та суспільними інтересами. Власникам же прав варто також і самостійно використовувати різні методики та способи забезпечення безпеки й захисту контенту, щоб правопорушник не мав можливості здійснювати недобросовісні дії у кібернетичному середовищі.

Кіберпростір — це віртуальний світ, який технічно існує у комп'ютерних мережах, але водночас це інтерактивне середовище, в якому мільярди людей по всьому світу щодня взаємодіють. Відповідно, кібернетичний домен дуже вразливий, а з ним — і ми, його "жителі". Тому вкрай важливо зробити такий простір захищеним та максимально безпечним.

1.3. Принципи дотримання права інтелектуальної власності у кіберпросторі в Україні і світі: порівняльно-правовий аналіз

Раніше, у ході дослідження, стало зрозуміло, що власність взагалі та інтелектуальна власність — це два різні поняття. І якщо першу можна, наприклад, сховати в сейф або найняти спеціальну людину для її фізичної охорони, то з другої такі методи не спрацюють, особливо коли йдеться про кіберпростір. Але, як і матеріальні об'єкти, об'єкти ІВ потребує якісного захисту. Адже коли належна охорона надається "на ділі", то таке відчутно сприяє збільшенню кількості винаходів та об'єктів творчості, а з ними — й розвитку науково-дослідної діяльності, що, своєю чергою, каталізує технічний прогрес. Інноваційний розвиток, що дуже важливо, допомагає залучити інвестиції.

Нерідко охорону інтелектуальної власності ототожнюють із її захистом, хоча ці поняття варто розрізняти, адже у них різні завдання, також

їх здійснюють різні суб'єкти. Охорона, як набуття прав, що зазвичай підтверджується видачею охоронного документа (патент, сертифікат, свідоцтво тощо), надається відповідним реєстраційним органом. Захист об'єкту ІВ буде потрібний, якщо зазначені права будуть порушені, і здійснювати його будуть адміністративні та судові органи.

Дотримання прав інтелектуальної власності, а разом з ним - їх охорона та захист в своїй основі мають певні принципи. Таких є декілька груп, в залежності від цілей, задач, суб'єктного складу тощо. Про них піде мова далі.

Взагалі, принципами права, на думку О.Ф. Скаун, є об'єктивно властиві праву відправні засади, це так звані "позитивні зобов'язання", вимоги, що висуваються до сторін суспільних відносин. Їх дотримання допомагає врахувати інтереси всіх учасників - і окремо взятих осіб, і груп, і навіть суспільства в цілому. Отже дані принципи - це своєрідна система координат, у її межах розвивається право; вони формують його фундамент, відбивають його сутність та основні зв'язки. Вони увібрали в себе глобальний і цивілізаційний досвід розвитку права [96, с. 222].

Насамперед право інтелектуальної власності підпорядковується загальним принципам права. Такими, як вказують Б. Шрамм і М. Г. Коен, є основні правила з досить загальним змістом, іноді навіть абстрактним, але необхідні для самого функціонування правової системи. Зазвичай вони не були "встановлені" як закон чи договір, будучи при цьому частиною позитивного права. Найчастіше такі принципи було виведено із правових міркувань суб'єктів, уповноважених приймати юридичні рішення у процесі застосування НПА, наприклад, судів. Вони потрібні, щоб заповнити собою правові прогалини, як фактичні, так і потенційні. Посилаючись на формулювання п. 1(с) статті 38 Статуту Міжнародного Суду ООН, дослідники роблять висновок про походження загальних принципів права із внутрішніх правових систем, з подальшим застосуванням їх на

міжнародному рівні. Такими принципами названі автори вважають принцип відшкодування завданих збитків, принципи тлумачення правил або ті, які використовуються для вирішення правових колізій, а також деякі інші [229].

Точного переліку загальних принципів права немає. Справа в тому, що наразі виокремлюються три підходи щодо їх розуміння, а саме:

- загальні принципи права - це основні засади міжнародного права, в ході багаторазового застосування вони можуть стати частиною національного права [47, с. 45];
- це норми, що існують у національних системах права. В силу своєї ідентичності вони визнаються регуляторами у сфері міжнародних відносин [266, с. 513];
- з компромісної точки зору, такими принципами слід вважати правила, що виникають при взаємодії міжнародного та внутрішньодержавного права [134, с. 106-107].

Отже, конкретного переліку таких не існує. Але загальні принципи права можна знайти у нашому Основному Законі – у Конституції України, вони є обов'язковими для дотримання та торкаються всіх правових галузей. До таких засад віднесено принцип верховенства права, що декларує вищу силу Конституції та пряму дію її норм, загальну підпорядкованість праву (Стаття 8); принцип гарантування права і свободи людини і громадянина (Стаття 22); принцип забезпечення захисту прав усіх суб'єктів права власності та господарювання, а також їхньої рівності перед законом (Стаття 13) тощо. Важливим з погляду даного дисертаційного дослідження є принцип, висвітлений у Статті 41 Основного закону, а саме принцип володіння - "кожний має право володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності" [45]. Таким чином, принципи дотримання прав інтелектуальної власності

мають повністю відповідати загальним принципам права, що визнаються цивілізованими державами.

Як зазначає О. П. Світличний, вивченню принципів у юридичній літературі приділяється належна увага, але при цьому принципи права інтелектуальної власності все ще не надто досліджені. Хоча це необхідно для гарантії охорони та захисту особистих майнових та немайнових прав відповідних суб'єктів. Дослідник також наголошує на тому, що в чинному законодавстві немає визначення принципів права ІВ, вони можуть бути встановлені на підставі наукового узагальнення та аналізу чинних НПА [95, с. 18].

Тому варто пам'ятати, що принципи ІВ, чия роль нерозривно пов'язана із охороною та захистом суб'єктивних прав відповідних суб'єктів, повинні мати у своїй основі, по-перше, об'єктивні закони розвитку суспільства, а по-друге - закони спеціальні, які регулюють безпосередньо відносини, що стосується результатів творчо-інтелектуальної діяльності. Таким чином, ці правові засади повинні відповідати суспільним інтересам, принципам гуманізму, а також моралі, як і основним цілям та завданням нашої держави в особі відповідних органів публічної влади.

Далі розглянемо безпосередньо принципи дотримання прав ІВ, їх охорони та захисту. Так, О.Д. Соколов та інші зазначають чотири наступні принципи охорони об'єктів інтелектуальної власності:

1. принцип охороноздатності. І якщо у контексті АП ми говоримо про надання об'єкту матеріального вираження, то об'єкти права промислової власності повинні задовольняти певні законом вимоги, щоб здобути необхідну охорону. Наприклад, винахід повинен не тільки мати новизну, але і бути промислово придатним, а також мати винахідницький рівень;

2. принцип дотримання балансу інтересів правовласника та суспільства. Щоб виключити монополізм, наприклад, патент видається на розумний строк (20 років);
3. принцип дотримання прав усіх сторін. Важливо дотримуватись прав не лише правовласників, а й тих, хто створив творчо-інноваційний результат (винахідники, розробники, автори тощо);
4. принцип визнання виняткового права на об'єкт права ІВ за правовласником [44, с. 7].

Національне управління інтелектуальної власності Китаю (СНІРА) у рамках Всесвітньої організації інтелектуальної власності (ВОІВ) створило посібник з основ ІВ, де серед її характеристик названі нематеріальність її прав за природою, їх винятковість та обмеженість за територіальною ознакою і терміном дії. При цьому вказується, що не всім видам цих прав притаманні кожна із зазначених характеристик, наприклад, комерційна таємниця може бути не відкрита ніколи. Що ж до винятковості прав, цей принцип виявляє себе у тому, що ніхто не має права використовувати належну правовласнику інтелектуальну власність без його дозволу чи законного обґрунтування. Також не можуть існувати одночасно і декілька ідентичних прав, коли справа стосується патентів та товарних знаків. Територіальний принцип передбачає дійсність прав інтелектуальної власності безпосередньо тільки в тій державі, де відповідні права визнані або надаються. По суті, ці права діють тільки на території країни, де вони і були набуті за законом. Що стосується часового принципу, то ІВ, за загальним правилом, охороняється протягом певного терміну, після закінчення якого охорона припиняється, а сам результат творчої та інтелектуальної діяльності переходить до категорії суспільного надбання [205, с. 14-15].

Також варто розглянути інший регіональний документ – Принципи інтелектуальної власності для суб'єктів Співдружності (це офіційна назва

держави, від англ. *Commonwealth of Australia* – прим. автора), представлені Департаментом комунікацій та мистецтв Австралії. Вони мають забезпечити надійну політичну основу для управління інтелектуальною власністю суб'єктами Співдружності, яким урядом рекомендовано розробляти індивідуальні системи управління ІВ з урахуванням власних цілей та потреб. Усього документ налічує 15 пунктів, що містять основи управління ІВ у державі, серед яких:

- відповідальними за дієве та етичне управління ІВ є суб'єкти Співдружності (організації тощо). Також вони з певною періодичністю зобов'язані оцінювати загальну ефективність своїх практик, які застосовують для керування та використання ІВ; робиться це з урахуванням корисності для австралійського суспільства та інших цілей уряду;
- кожному такому суб'єкту слід мати політику управління ІВ, що відображає його цілі та дані Принципи, а також є підкріпленою планом управління, стратегією та різними рекомендаціями. Така політика визначає підхід організації до діяльності з придбання, розпорядження та публічного доступу до об'єктів інтелектуально-творчої діяльності, реєстрації прав власності та їх безпосереднього захисту;
- суб'єкти повинні вести реєстри та подібні системи для ідентифікації ІВ, а також впроваджувати процедури для зниження ризику порушення інтелектуальних прав інших осіб (навчання персоналу, аудит використання ІВ та ведення документації всередині організацій тощо);
- організації також мають використовувати гнучкий підхід при розгляді варіантів володіння, управління та використання відповідних об'єктів. Осібно стоїть підпункт щодо контрактів на постачання програмного забезпечення в галузі інформаційних та

комунікаційних технологій (далі - ІКТ), суб'єкти, за умовчанням, зобов'язані в цьому випадку зайняти позицію на користь постачальника ІКТ, який володіє ІВ у ПЗ;

- суб'єкти повинні сприяти публічному використанню та спрощенню доступу до матеріалів, які були опубліковані з метою інформування громадськості про державну політику та розвиток у неї розуміння своїх прав на державну допомогу. Так, інформація державного сектора ліцензується організаціями відповідно до стандарту Creative Commons BY;
- комерціалізація ІВ не повинна бути основною діяльністю суб'єкта, якщо така діяльність не потрібна як невід'ємна частина цілей організації тощо [208, с. 5-9].

Ці австралійські Принципи, на думку автора, були б дуже доречними при регулюванні діяльності комерційних суб'єктів в українському економічному сегменті, оскільки сприяли б креативно-інноваційній діяльності населення.

Британська правозахисна організація *Article 19*, чия назва походить від 19 статті Загальної декларації прав людини, що наділяє всіх людей правом на свободу переконань та їх вільне вираження, свою місію бачить у сприянні свободі вираження поглядів та інформації по всій земній кулі. Для таких цілей вона розробила Принципи свободи слова та авторського права в цифрову епоху (англ. *Principles on Freedom of Expression and Copyright in the Digital Age*), до яких віднесла:

1. Загальні принципи, викладені у Розділі I документа, до яких включено:
 - а. право на свободу вираження поглядів (Принцип 1). Сюди, крім права розповсюджувати будь-які дані, думки та ідеї через ЗМІ, включено право шукати та отримувати інформацію (п. 1.1). При цьому, як сказано в п. 1.2, всесвітня мережа Інтернет - це суспільне надбання, необхідне для ефективного здійснення

декларованого права на свободу вираження думок. П. 1.3 говорить про можливість обмежити це право тільки на підставі вимог міжнародного права, а п.1.4 декларує неможливість обмеження свободи слова з метою захисту прав третіх осіб, включаючи авторські права, якщо держава не доведе, що таке обмеження викликане необхідністю захисту інтересів демократичного суспільства за законом;

- b. авторські права (Принцип 2). У пп. 2.1-2.2 визначена суть авторського права, дано перелік відповідних прав, що набуваються у зв'язку із ним творцем на певний термін, а також зазначена вимога щодо оригінальності твору як вираження ідеї. У п.2.3 сказано про обмежений захист АП за міжнародним законодавством про права людини як частину права власності; п.2.4 наділяє держави знаною свободою дій у випадку обмеження права власності, якщо таке потрібно для здійснення соціальної, економічної та культурної політики;
- c. принципи інтерпретації (Принцип 3). П. 3.1 говорить про взаємодоповнення свободи слова та АП, оскільки мета останнього - це просування літературної, художньої, музичної творчості, так само як і збагачення культурної спадщини та поширення серед громадськості знань та інформаційних продуктів. У п. 3.2 зазначено 5 критеріїв, які враховуються при визначенні виправданості обмеження свободи вираження на підставі авторського права;

2. Захист суспільного надбання (Розділ II):

- a. загальні засади (Принцип 4). П. 4.1 дає визначення суспільному надбанню як сумі всіх відомостей та культурних цінностей, не захищених АП, які можуть використовуватись громадськістю

без обмежень. П. 4.2 вказує на необмеженість терміну перебування об'єкта АП у громадському надбанні;

- b. термін дії авторських прав (Принцип 5). Відповідно до п. 5.1 термін дії АП повинен бути не довшим за час, необхідний для досягнення мети АП без шкоди для права за Принципом 1. Цікаву вимогу висуває п. 5.2, називаючи охорону АП після смерті творця невиправданим обмеженням суспільного надбання та права за Принципом 1, а тому її слід скасувати;

3. Винятки з авторського права (Розділ II):

- a. добросовісність та похідні роботи (Принцип 6). П. 6.1 вимагає тлумачити обмеження та виключення з АП широко, особливо при сумлінному веденні справ, що забезпечить виконання Принципу 1. Похідні роботи на підставі оригінальних творів також повинні отримати повноцінну охорону відповідно до принципу добросовісності (п. 6.2);
- b. право на особисте користування культурними цінностями (Принцип 7). Пп. 7.1-7.2 декларують право кожного отримувати та поширювати відомості та ідеї, що також включає право читати, слухати, вивчати культурні цінності без обмежень АП, у тому числі у всесвітній мережі; а спільне використання таких культурних цінностей не повинне бути обмежено;

4. Свобода слова та захист авторських прав у цифровому середовищі (Розділ IV):

- a. відключення від доступу до Інтернету (Принцип 8). На підставі авторських прав таке завжди є непропорційним обмеженням права за Принципом 1;
- b. фільтрація та блокування контенту, захищеного авторськими правами (Принцип 9). Перелічені та інші технічні чи юридичні обмеження доступу до контенту - це серйозне обмеження

свободи вираження думок, єдине виправдання в цьому випадку - повна відповідність перевірці трискладовому тесту (англ. *three-part test*) відповідно до міжнародного права (п. 9.1). П. 9.2 вважає невідповідним обмеженню свободи вираження думок блокування веб-ресурсів на підставі захисту АП. П. 9.3 вимагає застосовувати блокування сайту (якщо таке дозволено згідно із законом) тільки судом або іншим незалежним судовим органом та з урахуванням 8 критеріїв, що перераховуються в цьому пункті (a-h). П. 9.4 вимагає передбачити процедури, що дозволяють зацікавленим суб'єктам втручатися у процедури судової заборони з зазначених питань, а п. 9.5 – накладати особливе покарання за свідоме звернення до суду із заявою про блокування контенту без АП;

с. відповідальність посередника та видалення контенту (Принцип 10). Пп. 10.1-10.3 говорять про важливу роль інтернет-посередників (тобто тих, хто надає послуги доступу до Інтернету, пошуку, передачі або кешування даних у ньому) та про те, що вони не повинні нести відповідальність за порушуючий АП контент, що поширюється третіми особами з використанням послуг таких посередників; від останніх також не вимагається контролювати свої послуги для запобігання порушенню зазначених прав. П. 10.4 наказує включати до НПА, які регулюють відповідальність посередників щодо нелегального контенту, процесуальні гарантії для захисту свободи вираження поглядів та права на недоторканність приватного життя. Таким чином, посередникам буде потрібно видалити спірний контент лише за розпорядженням суду чи іншого незалежного судового органу на підставі верховенства права. П. 10.5 вказує перелік факторів (вимог за Принципом 1),

які повинні враховуватися при видаленні посередниками спірного контенту. П. 10.7 вимагає транспарентно документувати запити на таке видалення та рішення щодо них, щоб не порушувати право громадськості на отримання інформації та окремих осіб - на самовираження; зазначені документи мають бути доступними для оскарження;

- d. цивільно-правова відповідальність за порушення авторських прав (Принцип 11). У разі понесення правовласником збитків, відшкодуватимуться лише фактично понесені, а передбачена законом компенсація за некомерційні порушення підлягає обмеженню з метою недопущення лімітування свободи вираження поглядів (п. 11.1). Інтерес викликає положення п. 11.3, згідно з яким образливі заяви про порушення АП в Інтернеті та погроза судовим розглядом щодо них повинні каратися, інакше вони спричинять стримуючий вплив на право на свободу вираження думок;
- e. кримінальна відповідальність (Принцип 12). Пп. 12.1-12.3 називають кримінальні санкції за некомерційне порушення АП невідповідним втручанням у право за Принципом 1, тому їх треба повністю скасувати із наступною заміною на цивільно-правову відповідальність. У країнах, де таке скасування не передбачено, важливо при накладенні кримінальної відповідальності за АП довести відповідність 3 критеріям, що перераховуються. Також визнається необґрунтованим обмеженням свободи вираження поглядів і вимагає скасування криміналізація обходу програмного забезпечення для управління цифровими правами;

5. Заходи, що сприяють доступу до знань та культури (Розділ V):

- а. сприяння доступу до знань та культури (Принцип 13). За ним країни обтяжені позитивним зобов'язанням щодо просування права на свободу вираження поглядів та доступу до інформації, а тому НПА по АП мають це відображати. Держави закликають активно впроваджувати Creative Commons та подібні заходи з метою забезпечення широкого доступу громадськості до культури. Бібліотеки та інші культурні громадські місця повинні наділятися правом оцифрувати та надавати онлайн безкоштовно або за невисокою вартістю великий обсяг контенту. Також слід заохочувати рівний доступ до знань для всіх без дискримінації за мовним критерієм та рівнем грамотності тощо;
- б. Прозорість і підзвітність розробки політики у сфері авторського права (Розділ VI). Зазначене має дотримуватися під час укладання міжнародних угод та розробки політики у сфері авторського права (Принципи 14-15) [289, с. 6-22].

Окремо слід висвітлити принципи міжнародної охорони інтелектуальної власності, перелічені у згаданому вище матеріалі СНІРА, а саме:

- принцип національного режиму. Відповідно до нього держава має забезпечити громадянам інших країн той самий ступінь правової охорони, який отримують його власні громадяни. Важливе уточнення: під "іншими країнами" розуміються не всі інші існуючі на земній кулі, а лише ті, хто приєднався до міжнародного договору, наприклад Бернської або Паризької конвенції;
- принцип режиму найбільшого сприяння. Його взято з Угоди про торговельні аспекти прав інтелектуальної власності (також - угода ТРІПС, від англ. *Agreement on Trade-Related Aspects of Intellectual Property Rights, TRIPS*). Він передбачає застосування всіх пільг та

послаблень, отриманих громадянами однієї з країн-учасниць, до громадян будь-якої іншої країни-учасниці негайно та безумовно. Він дуже схожий на попередній принцип і покликаний нівелювати відмінності в режимах, що застосовуються до іноземців;

- принцип незалежної охорони. Суть його полягає у тому, що набуття та охорона прав у певній державі визначаються виключно її законами та ніяк не пов'язані із законами інших країн. Так, наприклад, визнання недійсності патенту у Сполучених Штатах не робить його недійсним у Китаї тощо. Цей принцип втілив у собі національний суверенітет, адже конкретна держава самостійно надає права та визначає їх обсяг з урахуванням внутрішньодержавної ситуації та інтересів свого народу;
- принцип мінімальних стандартів охорони. За ним країни-учасниці міжнародного договору сприймають встановлені ним стандарти як мінімальний рівень охорони, нижче за який внутрішні закони не можуть встановлювати об'єм охорони відповідних прав. Але вони вільні встановлювати вищі стандарти, якщо це дозволяє, наприклад, економічний розвиток тощо;
- принцип пріоритету. Він - важлива ланка у системі подання заявок, видачі патентів та реєстрації торгових марок. Оскільки одночасне подання заявок на реєстрацію відповідних об'єктів у кількох країнах - завдання важке, Паризька конвенція встановила систему пріоритету. За нею заявник, який подає заявку в одній країні-учасниці, наділяється пріоритетом при подачі заявок на той самий результат інтелектуальної діяльності в інших державах-членах протягом певного терміну;
- принцип транспарентності. Також взятий з Угоди ТРІПС, він вимагає, щоб усі НПА, угоди, судові та адміністративні рішення були доведені до загального відома без шкоди для державних чи законних ділових

інтересів сторін, а також провадження правоохоронної діяльності. Ця засада допомагає забезпечити стабільність та передбачуваність торговельного середовища;

- принцип суспільних інтересів. У ньому втілено вимогу про дотримання балансу між інтересами правовласників та широкого загалу [205, с. 19-21].

Юрист П. Гордон розробив керівництво по принципам інтелектуальної власності у відповідності із категорією об'єкта, що охороняється:

- винаходи. Для отримання патенту об'єкт повинен бути новим, наділеним винахідницьким рівнем і мати можливість промислового застосування;
- дизайн (промисловий зразок). Щоб вважатися новим, загальне враження про дизайн має відрізнитись від будь-якого вже існуючого;
- авторські права. Вони виникають автоматично під час створення творіння;
- товарні знаки. Реєстрація ТМ наділяє власника винятковим правом використовувати її для своїх товарів та послуг. Інакше, якщо знак не був зареєстрований, а спір щодо нього виник, доведеться покладатися на позов про підміну, що ускладнює процедуру і робить її більш витратною [191].

Деякі вчені виділяють окремо авторсько-правові засади, серед яких:

- принцип всебічної охорони прав та інтересів автора. Під ним мається на увазі декларована статтею 11 Закону України № 3792-ХІІ презумпція авторства, тобто за відсутності доказів іншого, автором роботи буде вважатися особа, чиє ім'я зазначено на творі;
- принцип відсутності формальностей щодо виникнення охорони з моменту створення твору. Реєстрації результату творчої діяльності автора чи іншого спеціального оформлення прав та інших офіційних

процедур не потрібно. АП виникає у зв'язку зі створенням такого об'єкта (згідно зі ст. 11 ЗУ №3792-ХІІ);

- принцип поєднання суспільних інтересів та особистих інтересів творця. У національному законодавстві є норми (наприклад, статті 21-25 ЗУ №3792-ХІІ), що дозволяють вільне використання творів, що охороняються, при повному дотриманні особистих немайнових прав творця;
- принцип виключно договірною погодження із творцем способів використання його роботи. Відповідно до статті 15 ЗУ №3792-ХІІ, саме творець наділяється виключним правом використання, а також дозволу (заборони) таких дій третім особам щодо свого творіння [50, с. 27-29, 32].

Щодо суміжних прав, то головним принципом таких є здійснення своїх прав на засадах дотримання прав:

- авторів виконуваних творів та інших суб'єктів АП - для виконавців;
- суб'єктів АП і виконавців - для виробників відео- та фонограм
- суб'єктів АП, виконавців, виробників фоно- та відеограм - для організацій мовлення [50, с. 38].

Окремо слід наголосити на необхідності дотримання особистих немайнових прав суб'єктів суміжних прав, так само як і на забороні завдання шкоди нормальній експлуатації об'єктів суміжних прав [50, с. 43].

Найбільш точний, на нашу думку, перелік сучасних принципів ІВ наводить у своїй роботі О. П. Світличний. Це наступні засади:

- принцип забезпечення державою інноваційного розвитку інтелектуальної сфери. Вчений посилається на ч.2 ст. 3 Закону України «Про інноваційну діяльність» та перераховує засади державної інноваційної політики, а саме: інноваційно-спрямований шлях української економіки; розробка нормативно-правової бази у сегменті інноваційної діяльності; створення необхідних умов для

якісного існування вітчизняного науково-технічного та інноваційного потенціалу; ведення активностей з метою міжнародної науково-технологічної кооперації та виведення національного продукту на зовнішній ринок; всіляке сприяння розвитку інноваційної інфраструктури тощо. Реалізація зазначеного, на думку дослідника, можлива за допомогою спеціальних державних науково-технічних програм;

- принцип сумлінності (добросовісності) заявника під час реєстрації об'єкта права ІВ. Заявник реєструє відповідний об'єкт із сумлінними намірами щодо його використання. Якщо ж ця особа без поважних причин не використовує об'єкт, що розглядається, протягом 3 років від дати реєстрації, тоді інша особа має право зареєструвати права на нього на себе;
- принцип рівності прав і законних інтересів всіх суб'єктів прав ІВ під час здійснення підприємницької діяльності. Так, свобода підприємницької діяльності є закріпленим у статті 42 Основного закону нашої держави як один з найважливіших прав українських громадян. Відповідно, всі суб'єкти права ІВ рівні у зазначених правах без урахування національної приналежності, майнового статусу тощо;
- принцип відповідальності посадових осіб митних органів. Зазначені суб'єкти, якщо під час реєстрації інтелектуально-правового об'єкта в митному реєстрі правовласнику було завдано шкоди, несуть відповідальність, у тому числі персональну майнову, якщо орган порушить строки внесення змін до митного реєстру;
- принцип надзвичайної суспільної необхідності. Примусове ліцензування запатентованого об'єкта в Україні можливе у разі надзвичайної суспільної потреби та введення військового чи

надзвичайного стану. Така ліцензія видається Кабміном терміном до 4 років із виплатою компенсації правовласникам;

- принцип вартісної оцінки об'єктів права ІВ. Майнові права на інтелектуально-правові об'єкти підлягають експертній оцінці з визначенням вартості; дана процедура встановлюється відповідно до НПА [95, с. 21-23].

Таким чином, інтелектуальна власність - це актив, який, хоч нерідко і є "віртуальним", може мати велику матеріальну цінність для підприємницької діяльності та взагалі економічного благополуччя різних суб'єктів. Тому об'єкти, що охоплюються даним поняттям, та права на них повинні якісно та надійно охороняються, для чого й використовуються різні механізми захисту. Крім зазначеного, кожна галузь права має низку основних засад, відомих як принципи. У праві інтелектуальної власності немає єдиного уніфікованого їх переліку, проте шляхом аналізу доктринальних підходів та наявної правозастосовної практики було запропоновано загальні інтелектуально-правові принципи, яких, тією чи іншою мірою, дотримуються не лише в Україні, а й у різних країнах світу. Серед таких особливо виділяється право власності на інтелектуальну власність, що належить її творцю, або яке було передане їм іншому правовласнику. Не меншу роль відіграють і принципи примусового ліцензування, справедливої поведінки, балансу прав правовласника та громадськості тощо.

І все ж, основний принцип права ІВ завжди один, незалежно від класифікації об'єктів, що охороняються, методів правового захисту та охорони. Цей принцип одночасно є й метою права інтелектуальної власності - це гармонізація. Адже взаємне узгодження, встановлення єдиної системи, забезпечення взаємної відповідності НПА, стандартів та підходів позитивно впливатиме на охорону та захист прав та безпосередньо об'єктів інтелектуальної власності не лише в Україні, а й у всьому світі. Це,

безумовно, призведе до підйому творчо-інноваційного духу та створення ще більшого масиву якісно нових та суспільно корисних об'єктів.

1.4. Правові форми дотримання права інтелектуальної власності у кіберпросторі: сучасні наукові погляди до визначення і застосування

Правові норми, що містяться у законах та інших НПА, щоб виконувати своє соціальне призначення, мають втілюватися у життя. Така їх реалізація відбувається через свідомо-вольові дії суб'єктів відповідних правовідносин. Таким чином, прийняття НПА варто розуміти як попередній етап правового регулювання, для реальної правореалізації ж потрібне практичне здійснення тих заходів, які є нормою права. Саме реалізація цих норм увінчує процес правового регулювання. Питання реалізації правових норм, відповідно, має особливу практичну значимість, у тому числі, для сфери права інтелектуальної власності.

У юридичній науці сьогодні можна знайти кілька підходів до розуміння суті терміна "реалізація норм права". Так, на думку деяких дослідників, правореалізація є втіленням правових норм у діяльності правосуб'єктів у вигляді використання суб'єктивних прав, виконання обов'язків та дотримання заборон. Реалізація прав, відповідно, може стосуватися як вчинення правомірних дій, так і правомірного утримання від певних дій, тобто бездіяльності. Результатом правореалізації буде досягнення повної відповідності між вимогами правової норми та діями (бездіяльністю) суб'єктів [106, с. 56].

О.Ф. Скакун розглядає як поняття, що вивчається, і процес, і кінцевий результат, вважаючи, що правореалізацією є "втілення приписів правових норм у правомірній поведінці суб'єктів права, в їх практичній діяльності" [97, с. 386]. П.А. Недбайло також висловлює ідею того, що норми права втілюються у життя саме в практичній поведінці людей, їх груп, державних

установ, і в процесі цього реалізуються належні їм права, виконуються покладені на них зобов'язання тощо [56, с. 125].

Здійсненням приписів норми права у практичній діяльності чи бездіяльності суб'єктів трактує реалізацію норм права П.М. Рабінович. Він також зазначає, що соціальна сутність правореалізації полягає у задоволенні суб'єктами суспільного життя своїх потреб саме соціально допустимими способами та сформованими державою засобами [93, с. 129].

Таким чином, багато вчених єдині в думці про те, що саме фактичне виконання правових вимог (норм, розпоряджень) у поведінці правосуб'єктів - це і є реалізація норм права як результат (фактичний прояв) правового регулювання.

Таким чином, підсумовуючи вищевикладені визначення реалізації права, відзначимо, що її невід'ємним елементом є правомірна поведінка правосуб'єктів, тобто будь-які дії учасників суспільних відносин повинні відповідати вимогам правових розпоряджень або не бути таким, що ними забороняються. Пасивна поведінка, тобто правомірна бездіяльність також необхідна, адже дозволяє іншим суб'єктам права безперешкодно реалізовувати свої права та виконувати обов'язки. Останнє можна назвати другим аспектом (або стороною) правової реалізації. При цьому реалізація суб'єктом прав – це добровільний акт, виконання обов'язків – необхідність, підкріплена примусовою силою з боку держави. Можемо зробити висновок, що *реалізація права – це реальне, закріплюване на практиці втілення в життя формально-визначених правових розпоряджень шляхом правомірних дій (бездіяльності) суб'єктів суспільно-правових відносин, метою чого є задоволення основних потреб громадян, суспільства та всієї держави в цілому на підставі засобів та методів, встановлених державою в особі своїх органів.*

Для цілей даного дисертаційного дослідження важливо також знати способи та форми реалізації норм права, якими є наступні:

- за суб'єктами реалізації правових норм - індивідуальна (особа самостійно використовує свої права та виконує обов'язки) та колективна форми (кілька осіб спільними діями користуються правами, виконують обов'язки);
- за методом здійснення права - добровільна та примусова;
- за субординаційною ознакою - форми з формально рівними сторонами та з переважанням прав однієї зі сторін;
- за рівнем активності суб'єктів правовідносин - активна (права використовуються, обов'язки виконуються у зв'язку із безпосередніми активними діями) та пасивна (коли суб'єкти утримуються від дій, не діють);
- залежно від типу правових норм (уповноважуючі, забороняючі, зобов'язуючі) - виконання, дотримання та використання як безпосередні форми реалізації права [2].

Саме останні форми мають особливе значення для цього підрозділу дисертаційного дослідження. Їх і розглянемо далі.

Як зазначає О.Ф. Скакун, таке виділення форм реалізації норм права за характером поведінки, необхідного для реалізації права, обумовлено методом правового регулювання, що використовується у відповідній правовій нормі. На думку вченої:

- *виконання* вимагає активних дій, пов'язаних із виконанням суб'єктами обов'язків, які на них покладаються певними правовими нормами (як-от сплата податків на дохід);
- *дотримання* полягає у бездіяльності, коли суб'єкт поводить пасивно, утримується від деяких дій, заборонених до вчинення нормами права (як-от утримання від куріння цигарок у громадському місці);
- *використання* спрямоване на добровільне здійснення суб'єктом своїх суб'єктивних прав як у вигляді здійснення активних дій, так і у вигляді

утриманні від дій (прикладом першого можна вважати виборче право, останнього - право відмовитися від свідчення проти себе у суді) [97, с. 67].

Таким чином, дотримання вимагає від особи суворого дотримання законодавчо встановлених заборон у вигляді утримання від заборонених дій. У разі права інтелектуальної власності варто навести приклад норми статті 54 української Конституції, згідно з якою "кожний громадянин має право на результати своєї інтелектуальної, творчої діяльності; ніхто не може використовувати або поширювати їх без його згоди, за винятками, встановленими законом" [45]. У цьому розпорядженні чітко простежується вимога до громадянина про утримання від поширення результатів творчо-інтелектуальної діяльності іншого суб'єкта без згоди творця - тобто є необхідність пасивної поведінки. Можна сміливо сказати, що дотримання як форма правореалізації зазвичай відбувається саме собою, коли ми вчиняємо незаборонені дії чи легально бездіємо.

Щодо виконання правових норм, то з погляду термінології, воно схоже на дотримання. Проте, виконання передбачає як можливість пасивної, стримуваної поведінки, так й активної. У випадку із цією формою реалізації правових норм має місце втілення в життя правових відносин двох або більше суб'єктів, між якими простежується особливий правовий зв'язок на основі юридичного факту, який передбачений гіпотезою певної норми права.

Використання норм права також має певну схожість із попередніми формами реалізації права, проте від них воно відрізняється здійсненням саме суб'єктивних прав, а не обов'язків чи заборон. Отже, суб'єкт правовідносин сам вирішує, чи використовувати надані йому права.

Далі варто дослідити правові форми та особливості дотримання права інтелектуальної власності взагалі та у кіберпросторі зокрема.

Варто зазначити, що, згідно з даними ООН, на 2019 рік кількість інтернет-користувачів у всьому світі склала 4,1 мільярда [58]. Більшість країн працює над покращенням якості інтернет-з'єднання, а також створює умови для забезпечення його доступності, що, відповідно, благотворно впливає на зростання кількості інтернет-користувачів, яке триває щодня.

Генеральний секретар ООН А. Гутерреш у ході брифінгу для держав-членів серед важливих пріоритетів вказав на використання можливостей цифрових технологій, а також, що важливо, на необхідність одночасного забезпечення якісного захисту від проблем та небезпек, які такі технології несуть у собі. На його думку, для вирішення такої проблеми особливу важливість має забезпечення надійності використання даних користувачів, при цьому політик зазначив, що більша частина інформації у всесвітній мережі все ж таки захищена. Але користувачі ще не захищені повною мірою від використання їх даних урядовими структурами, що веде до дискримінації та інших порушень у галузі прав людини. У цьому, як зазначають Н.О. Шпак, М.Б. Найчук-Хрущ та В. М. Гавецька, важливо особливо пильну увагу приділити соціальним медіа, чий контент створюють користувачі, і який далі використовується у різних інтернет-системах, що дає нам можливість "соціально" взаємодіяти один з одним. Соціальні мережі на кшталт Фейсбуку, Інстаграму та інших – унікальні платформи для комунікації та інших видів взаємодії, але вони ж створюють великі можливості для порушення прав інтелектуальної власності. Особливо часто порушення в медіапросторі стосуються захищеного авторським правом цифрового контенту, а саме комп'ютерних ігор, відео- та музичних творів, програмного забезпечення, авторських текстів, які поширюються несумлінним учасниками кіберпростору у соціальних мережах та на інших веб-сайтах без згоди власників АП. У зв'язку із зазначеним, як вказують дослідники, лише у 2019 році Державне підприємство "Український інститут інтелектуальної власності"

(Укрпатент), який, згідно з розпорядженням КМУ від 13.10.2020 р. № 1267-р “Про Національний орган інтелектуальної власності”, виконує функції Національному органу інтелектуальної власності, розглянув 465 звернень. Так, не всі з них стосувалися саме цифрового інтернет-вмісту, але велика їх кількість [121, с. 257-259]. Таким чином, цим ще раз підкреслюється важливість захисту інтелектуальної власності та прав на неї в Інтернет-мережі.

Про створення ефективного комплексного механізму держрегулювання у сфері інноваційної діяльності (а це царина інтелектуальної власності - *прим. автора*) як особливо важливого науково-практичного завдання для країни взагалі та вітчизняної науки зокрема заявляє і Н.П. Дяченко. Саме створення та впровадження належного правового забезпечення інноваційної діяльності, на думку дослідниці, сприятиме формуванню процвітаючої національної інноваційної системи. У своїй роботі вона посилається на статистичні дані, згідно з якими кількість інноваційних підприємств зменшилася на 55,5% у 2019 році порівняно із 2012 р., відповідно, зменшився і сукупний обсяг видатків таких суб'єктів на інноваційну діяльність (більш ніж у 3 рази порівняно із 2011 р.) [26, с. 511-512]. Багато в чому скорочення фінансування інноваційної діяльності пов'язане із неможливістю забезпечення належної правової охорони та захисту результатам творчо-інтелектуальної діяльності відповідних суб'єктів, що ще раз наголошує на важливості ведення нормотворчої та правозастосовної діяльності у аналізованому полі.

Якщо повернутися до дотримання та інших форм реалізації прав у контексті інтелектуальної власності взагалі та у кіберпросторі зокрема, та захисту і охорони відповідних прав у разі їх недотримання, то слід, перш за все, згадати, що наша незалежна держава Україна обрала для себе європейський вектор розвитку, тим самим розпочавши інтеграційні процеси української правової системи у загальноєвропейську, що

торкнулося, безумовно, і права інтелектуальної власності. Вирішальною подією в даному випадку стало підписання Угоди про асоціацію між Україною та Європейським Союзом, Європейським співтовариством з атомної енергії та їх державами-членами, яка була ратифікована нашою державою 16.09.2014 р. ЗУ № 1678-VII, а набула чинності 01.09.2017 року. Ця подія стала каталізатором не лише зближення наших країн, а й поширення та впровадження європейських правових та соціальних стандартів в українській державі.

У згаданій Угоді про асоціацію від 27.06.2014 питанням інтелектуальної власності присвячено окрема Глава 9 під назвою «Інтелектуальна власність» (це майже 1/5 частина всього НПА), а безпосередньо питанням захисту відповідних прав - Частина 3 зазначеної Глави - «Захист права інтелектуальної власності». У цьому контексті слід зазначити, що у відповідності із українською Конституцією (Ст. 9, ч. 1) міжнародні договори, згода на обов'язковість яких надана ВРУ, є частиною національного законодавства [45]. Відповідно, норми згаданої Угоди, як і інших загальноєвропейських документів (зокрема Директив), також застосовуються на території України.

Стаття 157 Угоди про асоціацію формулює цілі Глави 9, а саме: "спрошення створення та комерційного використання інноваційних продуктів та продуктів творчої діяльності на території Сторін; та досягнення належного та ефективного рівня охорони та захисту прав інтелектуальної власності". Стаття 158 цього документа вимагає від Сторін забезпечити дієве виконання зобов'язань за міжнародними правовими актами (далі – МПА) у сфері ІВ, особливо за Угодою ТРІПС. Стаття 176, присвячена технічним засобам, наказує Сторонам забезпечити необхідну правову охорону від обходу технологічних заходів з метою порушення прав інтелектуальної власності, а також охорону від виробництва, ввезення, розповсюдження, реалізації тощо пристроїв і різних продуктів, націлених

на такий обхід. Стаття 230 також вимагає забезпечувати сумлінні та справедливі засоби захисту, додаткові заходи та процедури з метою забезпечення дотримання охорони прав, які не будуть складні в реалізації, надмірно затратні або спричинять необґрунтовані затримки, а також не створять перешкод у законній торгівлі. Стосовно процедур і способів захисту ІВ за статтею 236 судам дозволено накладати судову заборону з метою запобігання порушенню прав ІВ, арешту контрафактних товарів, можливо також зобов'язати порушника виплатити штраф, компенсацію. Важливим моментом є можливість накладання аналогічної заборони на посередника, чиї послуги використовуються порушником прав ІВ. Стаття 237 передбачає можливість вилучення з торгівлі, або знищення товарів, що порушують права ІВ, а також обладнання та засобів для їх виготовлення, що робиться за рахунок порушника.

Не менш важлива для цілей цього дисертаційного дослідження Стаття 244 Угоди про асоціацію щодо використання послуг посередників. Такими послугами нерідко користуються порушники, а тому, з метою вільного звернення інформаційних послуг та захисту прав ІВ у цифровому середовищі, сторонам необхідно забезпечити спеціальні заходи для зазначених суб'єктів. Звільнення їх від відповідальності можливе лише у випадку, коли їх діяльність є суто автоматично-пасивною, полягає у технічних операторських процесах та наданні доступу до ІКТ, відповідно сам постачальник не володіє належними уміннями, знаннями і не здійснює контроль за переданими даними. Статті 245-247 присвячені відповідальності різних типів посередників:

- просто посередник - надає послугу інформаційному суспільству, що полягає у передачі даних від одержувача послуги через комунікаційну мережу. При цьому він не вибирав одержувача, не є ініціатором такої передачі і не здійснює вибір та зміну даних, що передаються. Тоді відповідальності він не несе;

- кешування - відповідальність на постачальника не накладається при автоматичному тимчасовому та проміжному зберіганні спірних даних, якщо ця активність ведеться тільки з метою зробити більш ефективною подальшу передачу іншим одержувачам. Вимоги щодо нього в цьому випадку такі: не змінювати інформацію, виконувати умови доступу до неї та правила щодо її оновлення, не перешкоджати законному використанню технологій для отримання відомостей та використання такої інформації. Він також зобов'язаний оперативно обмежити доступ до даних, що зберігаються, як тільки дізнається про необхідність такого;
- хостинг - постачальник послуги не несе відповідальності за дані, що зберігаються на вимогу одержувача, якщо він де-факто не володіє інформацією про незаконність діяльності або даних, а у разі отримання відповідних відомостей - оперативно унеможливорює доступ до спірних даних [108].

Далі, з урахуванням інтеграційних спрямувань України, слід розглянути положення Директиви Європейського парламенту та Ради ЄС про забезпечення дотримання прав інтелектуальної власності (Директива № 2004/48/ЄС від 29.04.2004). Основною метою документу проголошується зближення законодавчих систем для забезпечення якісного та достатнього рівня захисту на внутрішньому ринку (п. 10 Преамбули) у рамках права Євросоюзу прав творців та інших учасників правовідносин у сфері ІВ. Також зазначений НПА спрямований на розвиток інтелектуальної власності як однієї із фундаментальних засад розвитку сучасної економіки в ЄС [167]. Вказане знайшло свій відбиток й у п. «а)» ст. 157 Угоди про асоціацію, де зазначено, що цілями цього розділу є, зокрема, спрощення створення та комерційного використання інноваційних продуктів та продуктів творчої діяльності на території сторін [108].

Також мета Директиви 2004/48/ЄС полягала у доповненні положень Угоди ТРІПС щодо правозастосування. Справа в тому, що остання містить кримінальні засоби покарання, а акт 2004 р. розповсюджується лише на цивільно-правові засоби захисту. Директива 2004/48/ЄС вимагає від держав-членів використання ефективних та пропорційних засобів правового захисту, а також санкцій щодо піратів та виробників контрафактної продукції [167]. Отже, можна говорити про спрямованість НПА на регулювання саме захисту прав ІВ, а не конкретно самих прав.

За Статтею 1 документу, його предметом є захист прав ІВ, який, відповідно, включає й промислову власність, а область його застосування, відповідно до Статті 2, включає заходи та засоби відновлення порушених прав, щодо яких висувається вимога про відповідність принципам справедливості, збалансованості, ефективності тощо [167].

Також Директива передбачає застосування запобіжних заходів типу повного вилучення й знищення контрафакту, окремо потерпілому має бути відшкодовано збитки та судові витрати. Слід наголосити й на так званому праві інформації, відповідно до якого правопорушник має надати відомості щодо походження контрафактних товарів, їх розповсюдження, вартості та кількості, а також щодо посередників. Але варто зауважити, що, відповідно до преамбули документу, вказане розповсюджується тільки на порушення з метою отримання комерційної (економічної) вигоди [167].

Серед цілей НПА також слід виокремити сприяння розвитку інноваційної діяльності, конкурентоспроможності, а також забезпеченню охорони прав споживачів, підтримці правопорядку у суспільстві, збереження трудової зайнятості, а разом з вказаним - і усіляке сприяння запобіганню податковим втратам. Окрім зазначеного, Директива встановила й додаткові дії задля захисту саме цифрових авторських прав, без зачіпання національного регулювання в інших сферах.

За Статтею 3(1) загальне зобов'язання за документом має бути засновано на принципах справедливості і рівноправності, пропорційності, стриманості, а також ні в якому разі не може проявляти себе як бар'єр у торговельних відносинах, себто бути складним чи занадто вартісним, або таким, що створює необґрунтовані обмеження чи затримки [167].

Документ викликав чималу критику, бо супротивники вважали його норми надто суворими. Тому перший проект акту зазнав великої кількості змін.

Якщо повернутися до змісту Директиви, то у її Розділі 2 декларовано і розкрито принцип роботи з доказами. Так, згідно Статті 6 зацікавлені особи мають право звертатися за доказами щодо наявності правопорушення, але такі мають обов'язково бути "розумно доступними, достатніми, щоб підтримати претензії" особи в суді. Якщо ж відповідне правопорушення вчинено у комерційному масштабі, то країни-учасниці мають вжити всіх доступних заходів задля надання фінансової і подібної документації. Також, згідно Статті 6(2), вони мають сприяти попередньому арешту власності винної у порушенні авторських та суміжних прав особи. Пр цьому обов'язково має бути забезпечено захист конфіденційних відомостей. Стаття 7, з метою забезпечення доказової бази, дозволяє застосовувати фізичний арешт і самого контрафакту, і матеріалів, що застосовуються при його виробництві та розповсюдженні. При цьому оповіщення порушника про відповідне не вимагається, особливо якщо існує ризик знищення доказів або нанесення шкоди правовласнику [167].

Одним з перших відомих кейсів щодо застосування Директиви ЄС/2004/48 слід вважати справу *Princo Corporation, Ltd v. Koninklijke Philips Electronics*, коли Philips (Нідерланди), що володіла патентами на технології CD-R звернулася з позовом до суду. Результатом розгляду стало рішення на користь позивача, відповідно до якого мало бути вчинено попереджувальне вилучення всього майна Princo, як рухомого, так і нерухомого, в тому числі

банківських рахунків, задля відшкодування завданих порушенням збитків [246, с. 642].

Отже, сьогодні чітко прослідковується необхідність модернізації механізмів забезпечення права ІВ, що, в першу чергу, має здійснюватися саме через узгодження інтересів усіх суб'єктів творчо-інноваційної сфери. Таке сприятиме не тільки забезпеченню її стійкості та ефективності, але й допоможе підвищити рівень довіри нашого суспільства державним органам та інститутам.

Як зазначено у даному розділі, нормативно-правове регулювання, що має безпосереднє соціальне призначення, реалізується шляхом свідомовольових вчинків суб'єктів відповідних правовідносин. Саме тому, прийняттю НПА у зазначеному полі відведено роль попереднього етапу правового регулювання, а саме для фактичної правореалізації вирішальне значення має практичне здійснення заходів, що і є нормою права. Реалізація останніх увінчує процес правового регулювання, а тому відповідне питання має особливу практичну значимість взагалі, та безпосередньо для сфери ПІВ.

Як вже було зазначено, невід'ємним елементом такої реалізації є правомірна поведінка учасників суспільних відносин, при чому як активна, так і пасивна. Сама ж реалізація, зазвичай, проявляється у трьох форма - виконання, дотримання, використання. Наразі в Україні можна спостерігати за втіленням в життя усіх зазначених форм. І, в першу чергу, слід відмітити створення та впровадження належного правового забезпечення інноваційної діяльності, що, відповідно, якнайліпше сказується на формуванні процвітаючої національної інноваційної системи. Україна, як відомо, обрала для себе європейський вектор розвитку, задля зближення наших країн, а також впровадження в свою правову систему європейських стандартів, в тому числі, і в царині ІВ.

З урахуванням вищевикладеного, зробимо висновок про важливе значення реалізації права для української держави. Адже саме через таке здійснюються права і обов'язки учасників суспільних відносин, бо останні інакше б не змогли втілити в життя правові норми. Відповідно, ці норми визначають специфіку відносин правового характеру, тим самим визначаючи поведінку учасників. У разі ж виникнення спору між такими суб'єктами, для його врегулювання до правозастосовчого процесу вступають спеціальні державні органи. Отже, створення ефективного комплексного механізму державного регулювання у галузі інноваційної діяльності, його постійне покращення та усіляке сприяння реалізації права (в тому числі ППВ) є важливим етапом у становленні України як держави, що відкрита для інновацій.

Висновки до Розділу 1

Сучасний світ безперестанно зазнає впливу глобалізаційних процесів, у рамках яких особливої актуальності набула потреба у переорієнтації економіки на інноваційну модель розвитку, адже як соціальний, так і економічний розвиток і окремої країн, і всієї земної кулі неможливі без активного розроблення та впровадження інновацій. Саме інноваційна діяльність є тим механізмом, який, залучаючи, можливість удосконалення діючих виробничих процесів, підвищення ефективності, впровадження нових моделей їх функціонування є діючою силою у досягненні конкурентних переваг кожної країни поміж інших. Для цього держава має не тільки розробляти власні (локальні) інноваційні активи, але й обмінюватися відповідними здобутками з іншим міжнародними й приватними суб'єктами. І велику роль у вказаному сьогодні відіграє саме інтелектуальна власність, особливо в аспекті її вкорстання у кібернетичному середовищі, яке характеризується транскордонністю. Тому й питання дослідження проблеми правового забезпечення дотримання

права інтелектуальної власності у кіберпросторі (його методологія) є досить актуальним.

Цифрові технології наразі отримали досить широке поширення та застосування, що, в свою чергу, помітно змінює й характер правозастосовної практики у царині захисту інтелектуальних прав власників відповідних об'єктів. Сьогодні вказані активи іноді навіть називають "кібернетичною власністю" у зазначеному аспекті.

З урахуванням здійсненого дослідження, якому присвячено даний розділ, авторка дисертації дійшла наступних висновків:

1. Україна, як незалежна суверенна держава з високим інноваційним потенціалом, щоденно стикається з новими викликами й загрозами через безперестанну взаємодію суб'єктів прав ІВ у кіберпросторі. Адже нові інтелектуальні об'єкти з'являються щодня, а діюче правове регулювання, якому все ще притаманна деяка консервативність і навіть закостенілість, не завжди здатне достойно відповідати вказаним викликам. Тому воно потребує удосконалення, в тому числі, шляхом запозичення норм та їх практичного втілення у держав ЄС та інших провідних країн світу.
2. Сьогодні все ще не впроваджено єдину стратегію досягнення балансу між бажаннями споживачів цифрового контенту та власниками творчо-інтелектуальних об'єктів. Саме тому вважається за необхідне застосовувати саме комплексний підхід до вирішення цього питання, беручи до уваги не тільки нормативні аспекти, але також і доктринальні ідеї, наробітки та погляди вчених-дослідників, не нехтуючи й думкою інформаційної кібернетичної спільноти.
3. Зазначено, що довести факт вчинення кібер-правопорушення складно, адже регулювання сфери інформації та інформаційних технологій не завжди встигає за їх розвитком. Автор вказує на те, що НПА щодо запобігання та боротьби із кіберпорушеннями існує

чимала кількість в усьому світі, але вони не завжди є достатніми та ефективними. Кіберпорушники постійно підвищують свій рівень, винаходять нові методики й інструменти для скоєння неправомірних дій, чим створюють загрози безпеці персональних комп'ютерів фізичних та юридичних осіб і навіть цілих країн. Саме тому вважається за необхідно розроблювати та вводити в дію нове якісне законодавство з метою вирішення проблем у сфері забезпечення прав інтелектуальної власності у цифровому просторі. В процесі такого законотворчі мають враховувати специфіку кіберпростору (наприклад, його транскордонність) й суть об'єктів ІВ.

4. Підкреслюється важливість пошуку балансу між правами авторів, новаторів, творців та споживачів результатів інтелектуально-творчої праці у кібердоміні. Адже при нормативному закріпленні надання переваги правовласникам через деякий час буде майже неможливо дотримуватися режиму суспільного надбання щодо інтелектуально-творчих об'єктів, чи надавати безоплатний доступ до них. Таке, в свою чергу, призведе до збільшення розриву між різними соціальними угрупованнями за матеріальною ознакою.

Правовласник дуже бажано самостійно вживати доступних заходів щодо забезпечення захисту свого контенту, тим самим унеможливлючи здійснення правопорушень у кібернетичному середовищі.

5. Зазначено, що інтелектуальна власність є хоч і "віртуальним", але активом, що може мати велику комерційну цінність, тому важливо використовувати всі доступні методи й засоби захисту прав на них. Важлива роль в цьому відведена принципам як основоположним засадами, а саме принцип права власності на ІВ, яке належить її творцю, чи таке, що передане ним іншому правовласникові, а також принципи примусового ліцензування, справедливої поведінки,

балансу прав правовласника та громадськості тощо. Головною ж засадою авторка вважає принцип, який є одночасно також і метою ПІВ - гармонізація. Саме взаємна узгодженість, встановлення єдиної системи та забезпечення взаємної відповідності нормативних актів і стандартів сприятиме охороні та захисту прав та безпосередньо об'єктів ІВ в усьому світі, тим самим стимулюючи творців до створення нових праць та інновацій.

6. Надано визначення реалізації права як реальному, закріпленому на практиці втіленню в життя формально-визначених правових розпоряджень шляхом правомірних дій (діяльності або бездіяльності) суб'єктів суспільно-правових відносин, метою чого є задоволення основних потреб громадян, суспільства та всієї держави в цілому на підставі засобів та методів, встановлених державою в особі своїх органів.
7. Підкреслюється вирішальне значення для фактичної правореалізації практичного здійснення заходів, що і є нормою права. Реалізація таких норм - це головний етап процесу правового регулювання, а тому цей аспект має особливу практичну значимість безпосередньо для сфери ПІВ. Невід'ємним елементом реалізації (яка проявляється у трьох формах - виконанні, дотриманні, використанні) є правомірна поведінка суб'єктів суспільних відносин, а також створення і впровадження належного правового забезпечення інноваційно-творчої діяльності. Саме через правореалізацію здійснюються права і обов'язки учасників правовідносин, інакше б ці суб'єкти не змогли втілити в життя правові норми, які в свою чергу і визначають їх поведінку. Спори між ними передбачають залучення до правозастосовчого процесу спеціальних державних органів для скорішого вирішення конфлікту.

Результати дослідження, викладені у Розділі 1, відображено у таких публікаціях автора: [328]; [339]; [151]; [153]; [161]; [166]; [168]; [422].

РОЗДІЛ 2. ТЕОРЕТИКО-ПРАВОВА ХАРАКТЕРИСТИКА КІБЕРПРОСТОРУ ЯК ОСНОВИ ІСНУВАННЯ ЦИФРОВОГО КОНТЕНТУ

2.1. Місце кіберпростору у інформаційному середовищі

Сьогодні можна спостерігати тенденцію до домінування в економіках найбільш розвинених держав секторів, пов'язаних із виробленням знань, їх подальшою обробкою та розповсюдженням. Кожен окремо взятий індивід як такий, що має інтелектуальний потенціал і є основною діючою одиницею постіндустріального суспільства, задає ритм економічного розвитку та науково-технічного прогресу. Сучасне суспільство отримало доступ до інформаційних потоків та усіляких знань, що й визначило форми та способи його навчання та культурного зростання, а також відкрило для нього можливість зберегти світ і швидше вийти із неблагополучного стану. Таким чином дані, відомості, інша інформація, будучи перетворені на нові знання, стали рушійною силою соціальної трансформації та основою змін у соціальній структурі суспільства.

Технологічна база для глобальної інтеграції була сформована саме завдяки постіндустріальній економіці, що ґрунтувалася на виробництві нових знань, а з ними – інновацій. Розвиток та подальше поліпшення сфери комунікаційних мереж сприяло впровадженню нових інформаційних технологій у повсякденне життя нашого суспільства та окремо взятих індивідів, і навіть спровокувало докорінні зміни у різних соціальних сферах.

У попередньому розділі було розглянуто особливості відносин у кіберпросторі та безпосередньо сам термін «кібернетичний простір», але пов'язані із ним категорії не були визначені повною мірою. У зв'язку із цим нагадаємо про те, що на в останні 30 років у соціальних науках особливе місце посів безпосередньо пов'язаний із кіберпростором термін

«глобальний інформаційний простір» (або «глобальний кіберпростір»), що викликано, в першу чергу, розвитком та використанням новітніх результатів інформаційно-технологічного прогресу. Нашу увагу в даному випадку привертає саме частка «інформаційний» у вказаному терміні.

У зв'язку із цим зазначимо, що кібернетичний простір відрізняється відсутністю географічної прив'язки і меж фізичного простору, він має транскордонний характер. У той же час він не існує сам по собі, а нерозривно пов'язаний із інформаційним середовищем. Останнє теж потребує надання йому визначення. Так, Закон № №537-V Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки від 09.01.2007 у Розділі I говорить про один із основних пріоритетів нашої держави - прагнення створити інформаційне суспільство, яке буде доступним для усіх та орієнтованим на інтереси та розвиток людини. У такому соціумі кожен з нас матиме можливість не тільки отримувати знання та іншу інформацію, а й створювати їх, користуватися ними, передавати іншим, безперешкодно отримувати доступ до них. Все це має на меті надати кожній людині можливість реалізувати свій потенціал повністю, тим самим покращуючи якість свого життя та сприяючи суспільному та особистому розвитку кожного [80].

У розділі IV цього НПА задекларовані організаційно-правові основи, необхідні для розвитку українського інформаційного суспільства. І, крім ресурсних та інституційних, зазначені також інтеграційні (п.3 Розділу IV). Так, вказується, що інтеграція української держави у глобальний інформаційний простір має ґрунтуватися на політиці міжнародного співробітництва та участі нашої країни у розвитку глобального інформаційного суспільства. При цьому основними засадами такої співпраці визнаються зменшення цифрової та інформаційної нерівності та реалізація універсального підходу до спільної активності. Задля досягнення згаданих цілей Закон № №537-V наказує розширювати співробітництво із

основними міжнародними організаціями на базисі міжнародних договорів, які є обов'язковими за згодою ВРУ. Також важливо у рамках таких міжнародних угод розвивати спільні проекти, спрямовані на забезпечення інтеграції нашої держави у глобальний інформаційний простір. Разом із зазначеним потрібно інтегрувати українські науки та культуру у глобальний науково-технічний та культурний інформаційний простір, а також всіляко сприяти укоріненню партнерських відносин між усіма секторами економіки з метою розвитку інформаційного суспільства, як того вимагає Декларація тисячоліття ООН [80]. Також у п.8 ч.1 статті 3 Закону № 2657-ХІІ "Про інформацію" від 02.10.1992 сприяння міжнародному співробітництву в інформаційній сфері та входження нашої країни у світовий інформаційний простір є одним із головних напрямів держполітики [76].

Якщо говорити про глобальний інформаційний простір, то можна розглядати його як невіддільний елемент соціального простору, який формує окреме самостійне явище, а саме соціально-інформаційний простір. Як зазначає О. Проскуріна, глобальний інформаційний простір, що вступає в союз із системою міждержавних відносин, варто досліджувати з двох ракурсів - як самостійну сферу зіткнення зовнішньополітичних інтересів країн і як об'єкт, засіб втілення зазначених інтересів у життя в системі міжнародних відносин [92, с.137].

Дослідниця зазначає, що в ході реалізації інформаційної стратегії України стратегічним її напрямом має бути участь у активностях міжнародних організацій та рухів, які націлені на політичне та правове регулювання глобального інформаційного простору. Для цього нашої державі також варто приєднатися до міжнародних договорів щодо порядку діяльності державних та недержавних органів в інформаційних мережах [92, с.141].

Сьогодні багато вчених, які вивчають роль і місце інформаційно-комунікаційних технологій у житті світової спільноти, виходять із того, що

глобальний інформаційний простір - це сукупність інформаційних ресурсів та інфраструктур, до складу яких включені міждержавні та державні комп'ютерні мережі, так само як і мережі загального користування, а також телекомунікаційні системи та інші транскордонні канали передачі інформаційних даних. При цьому під інформаційним ресурсом дослідники розуміють веб-сторінки, текстову документацію, зображення, програмне забезпечення, звуковий та графічний контент та бази даних. І такі ресурси через інформаційно-комунікаційну інфраструктуру формують собою єдиний інформаційний простір [193, с. 17].

Деякі вчені, наприклад, В. Горовий, використовують термін "загальноцивілізаційний (глобальний) інформаційний простір". Він формується із глобальних інформаційних ресурсів та засобів їх використання у всьому світі, а також прискорено розвивається та стимулює інші країни на перетворення в інформаційній сфері. Структуризація зазначених ресурсів, зумовлена суспільними потребами, провокує на їх основі розвиток загальноцивілізаційної інформаційної бази. І в процесі такої структуризації беруть участь спеціальні групи інформаційних ресурсів, які:

- мають загальноцивілізаційне значення;
- використовуються суб'єктами як продукти міжнародного ринку інформації;
- використовуються для поширення глобального впливу окремими міжнародними інформаційними суб'єктами;
- є джерелами інформаційного виробництва у зв'язку із глобальною інформатизацією;
- є компонентом інформаційних воєн та засобом їх нейтралізації;
- використовуються у кіберзлочинах та як засоби нейтралізації їх наслідків [13, с. 59-60].

Можна зробити висновок про те, що взагалі під інформаційним середовищем (інформаційною сферою) у широкому розумінні слова розуміють світ інформації (знань, даних) навколо кожного з нас та світ нашої інформаційної діяльності. У ще більш загальному сенсі вказаний термін зазвичай розглядається як позначення певної системи зовнішніх та внутрішніх організаційних потоків даних, які, відповідно, суттєво відрізняються між собою за такими характеристиками як зміст та наповнення, методи та інтенсивність обміну та інше.

У вузькому сенсі мова йде про сукупність інформаційних систем та інфраструктури, а також інших засобів, за допомогою яких забезпечується створення, обмін, обробка інформації, сюди віднесено також носії даних і саму інформацію як основу діяльності суб'єктів такої взаємодії [264, с. 7].

Згідно з іншим джерелом, існує чотири основні підходи, що визначають інформаційне середовище як:

- сферу діяльності суб'єкта, у якій створюються, споживаються, модифікуються дані;
- сферу суб'єктної активності у рамках суспільного життя, пов'язаного із зазначеною діяльністю щодо даних, а також їх збереженням, поширенням та обробкою;
- сукупність самих знань та відомостей, інформаційної інфраструктури та суб'єктів, які здійснюють інформаційну діяльність;
- симбіоз інформаційних ресурсів та системи взаємодії щодо інформації та інформаційної інфраструктури [109, с. 394].

Б. А. Корміч виходить із загального підходу про розуміння інформаційного простору з погляду потоків інформації, система яких і охоплює сферу суспільної діяльності [48, с. 38]. При цьому під інформаційним потоком варто розуміти комплекс відомостей, що переміщуються в інформаційному просторі через канали комунікації за

допомогою фізичного зв'язку між донором та реципієнтом даних, що матеріалізуються у такому інформаційному потоці [24, с. 22].

Деякі автори серед журналістів сприймають інформаційний простір лише з його інформаційної сторони як сукупність відомостей, знань і результатів комунікаційної діяльності соціуму в просторі, який певним чином організований. Так, якщо вивчається інформаційний простір певної країни, то маються на увазі дані, що функціонують у конкретних географічних межах. При цьому будь-яка комунікаційна активність, будь то спілкування, обробка інформації, творчість - все це веде до наповнення простору, що розглядається. І результат такої діяльності буде характерним для цього конкретного суспільства, цієї держави чи цього інформаційного простору [124].

Як зазначає О. О. Жидкова, інформаційне середовище варто розглядати як сукупність інформаційних умов існування суб'єкта, під якими розуміються наявні інформаційні ресурси та їх якість, а також розвиненість інформаційної інфраструктури. Таке середовище забезпечує умови, необхідні для розвитку суб'єктів інформаційного простору. Але, при цьому, те, наскільки вона буде сприятливою, залежить від внутрішніх характеристик суб'єктів, а саме від інформаційного потенціалу як сукупності інформованості, здатності до осмислення та рівня інформаційних потреб [31, с. 61]. Проаналізувавши підходи інших авторів, виділимо три найбільш часто вживані визначення аналізованого концепту, а саме:

- це інформаційні умови існування суб'єкта у своїй сукупності, тобто підхід аналогічний до підходу О. Жидкової [15];
- це сукупність системи формування, поширення та використання даних, інформаційної інфраструктури, а також інформаційних ресурсів [139, с. 376];

- це діяльність підприємств і організацій, що пов'язана із створенням, використанням, модифікацією інформації [6, с. 5].

К. О. Дубняк упевнений, що інформаційна сфера є сукупністю відомостей, інформаційних суб'єктів, інфраструктури та системи регулювання відповідних інформаційних суспільних відносин [24, с. 21].

А.В. Арістова та Т.А. Чернадчук використовували у своїй практиці також поняття "інтегративна інформаційна сфера", що об'єднало у собі всі сфери суспільного життя, включаючи інформаційну, з точки зору циркуляції інформації. При цьому кібернетичний простір - це свого роду провідник у інформаційних процесах і головна частина інформаційної сфери сучасного суспільства [125, с. 194-195].

Згідно з документом CNSSI 4009-2015 згаданого раніше Комітету із систем національної безпеки, інформаційне середовище є сукупністю окремих осіб, організацій та систем, які збирають, обробляють, поширюють дані або впливають на них [144, с. 63]. При цьому варто розуміти, що інформаційний простір не є статичним, це широке динамічне середовище. У ньому всі фізичні об'єкти зазвичай обмежені фізичними кордонами, а сам такий простір чітко структурований за допомогою інформаційних полів та потоків.

Також звернемо увагу на проект Концепції інформаційної безпеки України 2015 року, розміщений на офіційному сайті Організації з Безпеки та Співробітництва в Європі (далі – ОБСЄ). Цей документ у статті 2 містить термін "національний інформаційний простір", який інтерпретований як сукупність усіх доступних на території країни інформаційних потоків національного та зарубіжного походження. Далі в тій же статті надано визначення інформаційної сфери як сукупності ІТ, інформаційної інфраструктури, суб'єктів інформаційної діяльності, ресурсів, інформаційної продукції та послуг, а також системи регулювання суспільних інформаційних відносин [46, с. 4].

При формуванні термінологічної бази щодо інформаційного середовища (простору) варто також враховувати її основні функції, а саме:

- **комунікативну**, тобто впровадження особливого середовища комунікації для інформаційних суб'єктів, де вони можуть вільно обмінюватися інформацією на умовах транскордонності, мобільності, інтерактивності;
- **геополітичну**, тобто подальше створення якісно нової платформи, середовища для ведення геополітичних відносин і здійснення конкуренції на основі раніше сформованих власних ресурсів і трансформації вже існуючих традиційних;
- **інтегруючу**, тобто об'єднання різних видів діяльності, наприклад, соціальної та політичної, у комунікативно-соціокультурне середовище;
- **актуалізуючу**, тобто актуалізацію інтересів різних інформаційних суб'єктів у даному середовищі за допомогою реалізації ними інформаційно-політичних цілей [24, с. 22].

Не менш важливо також розуміти, із чого складається інформаційне середовище. Так, компонентний склад інформаційного простору, за деякими джерелами, представлений такими елементами:

- **інформаційні ресурси як "фізичні" (на фізичних носіях), так і "віртуальні" (розміщені на веб-сторінках).** Такий підхід щодо ресурсів дещо відрізняється від підходу К. О. Дубняка. Так, під зазначеним розуміються ресурси у власності будь-якого інформаційного суб'єкта, що відрізняються від інших видів ресурсів тим, що:
 - піддаються саме моральному зносу, а не фізичному;
 - не є матеріальними за своєю природою, відповідно вони не зводяться до втілення тільки на фізичних носіях;

- грають позитивну економічну роль, тому що їх використання дає можливість суттєво зменшити рівень споживання інших типів ресурсів;
- **інформаційна інфраструктура.** Мається на увазі таке середовище, яке дозволяє та сприяє взаємодії з інформаційними даними, а саме здійсненню збору, розповсюдженню, зберіганню, передачі та обробці даних автоматизованими засобами у соціумі.
- **методи та інструментарій прикладної математики.** Сюди входять різноманітні алгоритми та програмні ресурси, завдяки яким можлива робота апаратних систем;
- **правові норми** у вигляді національних інформаційних нормативно-правових актів, міжнародних договорів та інших юридично значущих інструментів;
- **ринок інформаційних технологій.** Сюди входять не лише безпосередньо інформаційні продукти та послуги, а й різноманітні засоби зв'язку, інформатизаційні та телекомунікаційні ресурси.
- організаційні заходи. Це ті, завдяки яким забезпечується адекватне функціонування елементів інформаційного середовища [36].

Варто зазначити, що для інформаційного середовища як суспільного простору, в якому успішно взаємодіють як окремі інформаційні суб'єкти, так і цілі соціальні групи, характерна відсутність меж та наявність об'єктивної віртуальної складової. Отже, ми маємо справу із інтеграційним механізмом організаційних структур.

Окремо варто зазначити характерні особливості інформаційного простору, а саме:

- універсальність його впливу на всі сфери життя як цілого суспільства, так і окремих його членів;
- структурованість та неоднорідність такого простору, основний акцент робиться саме на різних тематиках та соціальних групах, хоча

це середовище не має як відчутних географічних, так і фізичних вимірів;

- у кожній державі вона має свої особливості, оскільки формується на основі національно-культурних та національно-психологічних поглядів та підходів у суспільстві конкретної країни;
- особливий динамізм, що викликаний безперервними змінами у багатьох сферах життя окремих держав та всього світу загалом, а також новими векторами в інформаційній політиці;
- необхідність надання йому надійного захисту від негативного впливу інших міжнародних інформаційних суб'єктів [109, с. 341].

В.М. Фурашев упевнений, що інформаційний простір існував ще до появи людей, адже неживі природні об'єкти завжди були джерелами різної інформації. Але тоді не існувало суб'єктів споживання такої інформації та взаємодії з нею. Сьогодні людство живе в інформаційному просторі, і кожен з нас є інформаційною системою, а також джерелом і користувачем інформації. Відповідно, інформаційний простір є певною формою співіснування системи матеріальних і нематеріальних об'єктів і процесів, спрямованих на задоволення інформаційних потреб кожного жителя нашої планети [112, с. 165]. На підставі такого визначення можна виділити деякі відмінні риси інформаційного простору (середовища):

- до об'єктного складу поняття входять суб'єкти природного середовища та інформаційні відносини між ними, процеси та об'єкти матеріального та нематеріального світів, що функціонують для задоволення інформаційних потреб таких суб'єктів з метою забезпечення їх життєдіяльності;
- суб'єктний склад представляють живі істоти та їх об'єднання, групи, здатні не просто сприймати, обробляти та запам'ятовувати інформацію, а й обмінюватися нею [112, с. 166].

К. О. Дубняк також згадує про інформаційну інфраструктуру суспільства як складову частину технологічних та організаційних аспектів інформаційного простору. Таке середовище, на його думку, формується як єдине ціле, що складаються з інформаційних та телекомунікаційних мереж, засобів інформатизації, алгоритмів та програм для правильної роботи програмно-апаратних ресурсів, а також систем, що відповідають за створення та збереження інформоресурсів, за кадрову підготовку та проведення наукових досліджень і забезпечення доступу до систем інформації та телекомунікацій, мереж зв'язку тощо [24, с. 21-22].

Також важливо вказати на наявність особливого наукового підходу, згідно з яким існує так званий когнітивний кіберпростір (від англ. *cognitive cyberspace*), що класифікується, у свою чергу, на когнітивно-інформаційний кіберпростір (від англ. *cognitive information cyberspace*) і когнітивно-комунікаційний (від англ. *cognitive communications cyberspace*). Автор зазначеної концепції під двома останніми термінами має на увазі, відповідно, інформаційний (кібер) простір та комунікаційний (кібер) простір [228, с. 5]. І останній сприймається як інструмент зв'язку, неагрегативний, незалежний від фізичних об'єктів, але такий, що потребує людської участі, а також вливань капіталу, часу та інших ресурсів. Він націлений на сприяння соціальній та економічній поведінці учасників [228, с. 22].

Для інформаційного простору характерний розгляд його із географічної, семантичної та соціальної точок зору. Так, географічна має на увазі конкретні географічні (локаційні) дані (наприклад, використання віртуальних карт), семантична – використовує словоформи з фізичного світу для маніпуляції інформацією, тобто має певний просторовий фактор. Соціальна точка зору передбачає переміщення відомостей між користувачами та об'єктами, які такі суб'єкти створили у процесі взаємодії [228, с. 16].

Таким чином, з урахуванням всього вищевикладеного, стає зрозуміло, що терміни "кіберпростір" та "інформаційний простір" - не тотожні, і відрізняються вони насамперед за своєю спрямованістю. Так, кібернетичний простір - це саме невіддільний елемент інформаційного простору, він охоплює лише живих істот, які сприймають, обробляють, запам'ятовують дані, здійснюють обмін отриманими знаннями. А інформаційний простір (середовище) охоплює взагалі всі джерела інформації, не вимагаючи сприйняття, обміну, запам'ятовування чи переробки отриманих відомостей.

У цьому питанні В.М. Фурашев також відзначає властивості, характерні одночасно і для інформаційного, і для кібернетичного простору, а саме: реальність загально діючого впливу, так само як і симбіоз матеріального та нематеріального, дискретного та безперервного, абстрактного та реального [112, с. 166].

Але, як зазначено вище, ці терміни не однакові. На нашу думку, слід розуміти кіберпростір як елемент системи інформаційного середовища (сфери) на рівні із "класичним" або "бумажним" інформаційним простором. Але саме кібернетичний простір сьогодні є центральним сегментом інформаційної сфери, адже саме в ньому наразі сконцентровано глобальні потоки як економічно-політичної природи, так і соціальних взаємин.

Інформаційна сфера у наші дні стала двигуном прогресу та розвитку постіндустріального суспільства, яке в Україні прийнято розглядати як інформаційне. Саме вона чинить основний вплив на стан економічного, політичного, оборонного та інших елементів національної безпеки нашої держави. Тому особливо важливим нам вважається формування ефективного та стабільного українського інформаційного простору, що дозволить створити та розвивати не менш стабільний кібернетичний простір, де вільно існують швидкі та мобільні інформаційні потоки. Для цього важливо зробити наступне:

- на офіційному рівні визначити правовий статус та становище інформаційних ресурсів з урахуванням прав власності на них, рівня захисту та доступу до даних;
- забезпечити належний захист інформаційним об'єктам у сфері інтелектуальної власності, для чого важливо насамперед класифікувати їх на матеріальні та нематеріальні активи;
- створити єдину систему національних інформаційних ресурсів, а також всіляко сприяти та забезпечувати підвищення рівня інформаційної незалежності України;
- розвивати інфраструктуру створення, розвитку та надання інформаційних продуктів та послуг населенню країни;
- опрацювати і внести поправки в (або замінити застарілі) нормативно-правові акти, що регулюють інформаційну сферу в цілому та окремо кібернетичний простір, в т.ч. щодо прав та обов'язків інформаційних суб'єктів, а також інформаційного забезпечення держорганів тощо;
- підвищувати ефективність функціонування державного та самоврядування, ґрунтуючись на використанні раніше накопичених інформаційних ресурсів;
- просувати позитивний імідж нашої країни у Всесвітній Мережі як такої, що всіляко сприяє розвитку та забезпеченню безпеки інформаційного простору.

Українське суспільство - це суспільство інформаційне, як уже зазначалося раніше, але процес становлення його як такого все ще не завершено, а тому влада нашої країни не повинна зупинятися на досягнутому у відношенні формування інформаційного простору. Не менш важливо врахувати наявний світовий досвід і тенденції, що панують в умовах глобалізації. Також необхідним є підвищення рівня інформаційної культури населення, прищеплення йому розуміння основ кібергігієни, оскільки серед населення існує інформаційний голод.

І лише досягнувши зазначених цілей, наша держава Україна зможе увійти у світовий інформаційний простір та безпосередньо кіберпростір як рівноцінний та незалежний суб'єкт.

2.2. Якість правового забезпечення функціонування кіберпростору в Україні

Інформаційні та комунікаційні технології сьогодні стали обов'язковим елементом як систем управління майже в кожній галузі економіки, так повсякденного життя більшості українців. Свобода доступу до глобальних мереж суттєво розширила можливості для комунікації, трудової діяльності та ведення різних активностей. І, одночасно з такими благами, з'явилася "велика ложка дьогтю" у вигляді нових викликів і загроз кібернетичній безпеці простору, що розглядається. Тому охорона та забезпечення такої безпеки стали для нашої держави одним із пріоритетних завдань.

У попередньому розділі було дано посилання на основний український нормативно-правовий документ, що прямо опікується питаннями сфери кіберпростору, а саме на Закон № 2163-VIII “Про основні засади забезпечення кібербезпеки України” від 05 жовтня 2017 року. Окрім визначення суті кібернетичного простору, цей акт також розкриває поняття безпосередньо кібербезпеки. Так, згідно п. 5 Статті 1, вона являє собою захищеність життєво важливих інтересів України, українського соціуму та безпосередньо кожного окремо взятого жителя території нашої країни як людини та громадянина при використанні кібернетичного простору. І саме в такому стані забезпечується як сталий розвиток українського інформаційного суспільства, так і цифрового комунікативного середовища, так само як і виявлення, попередження та усунення ймовірних чи реальних загроз національній безпеці нашої держави у кіберпросторі [79].

Вищезгадана національна безпека у загальному сенсі зазвичай розуміється як стан захищеності держави від загроз, як внутрішніх, і зовнішніх. У політології національну безпеку розглядають як особливого типу стабільність, стійкість, що забезпечується протягом досить тривалого періоду, у вигляді особливого стану розумної динамічної захищеності від найсерйозніших загроз та інших вразливостей. Сюди вчені-політологи відносять також здатність суб'єкта до розпізнавання подібних загроз та їх своєчасне відбиття, нейтралізацію [271]. Щодо нашого національного законодавства, то у п. 9 статті 1 Закону 21.06.2018 № 2469-VIII «Про національну безпеку України» сказано про те, що нацбезпеку слід розуміти як захищеність від реальних чи передбачуваних загроз та ризиків державного суверенітету, територіальної цілісності держави, демократичних конституційних засад, а також інших її національних інтересів [78].

До складу цієї категорії багато авторів відносять воєнну, соціальну, економічну та інформаційну безпеку [203, с. 336-341]. На нашу думку, особливе місце у системі національної безпеки займає саме інформаційна, що підтверджується положеннями відповідних нормативно-правових актів. Так, стаття 17 Конституції України прямо вказує на те, що головними функціями державної влади та справою усіх українців є захист суверенітету та територіальної цілісності нашої країни, так само як забезпечення її економічної та інформаційної безпеки [45]. Зазначимо, що Закон № 2469-VIII "Про національну безпеку України" у п.4 статті 3 також прямо вказує на те, що держполітика у сфері нацбезпеки та оборони націлена на забезпечення зовнішньополітичної, державної, воєнної, економічної, екологічної, кібернетичної та інформаційної безпеки [78].

У зв'язку із тематикою цього дисертаційного дослідження останній концепт цікавить нас як особливе "поле", елементом якого є кібернетична безпека. Так, інформаційна безпека (від англ. *Information security*,

скорочено - *InfoSec*) як соціальна та правова категорія, може бути розглянута з кількох точок зору.

Згідно з Л. Ірвіном, це те, як індивіди та цілі компанії захищають свої цінні активи інформаційного характеру, серед яких можуть бути ділові записи та документи, особисті дані, так само як і результати інтелектуальної творчої діяльності. Вказані відомості зберігаються на різних пристроях та в різній формі, наприклад, на серверах, флеш-накопичувачах, хмарних платформах або особистих пристроях) [222]. При цьому форма, в якій міститься інформація, може бути цифрова, і "паперова". Також можна класифікувати її на матеріальну (документацію) чи нематеріальну (знання). Це узагальнене поняття *InfoSec*.

У соціологічній сфері, на думку Є. Архипової, щодо інформаційної безпеки існує певна невизначеність понять і положень, що викликано відсутністю загальноприйнятої термінології, а також складністю та багатоаспектністю інформаційної безпеки. У свою чергу, таке вилилося у дисциплінарну роздробленість наявних знань та їхню суперечність зі складним характером завдань забезпечення безпеки. Як результат, дослідниця дійшла розуміння інформаційної безпеки як стану захищеності інформаційних активів від ненавмисних чи навмисних дій природного чи штучного характеру, результатом яких може стати заподіяння неприйнятної шкоди інформаційним суб'єктам, наприклад, власникам та користувачам таких даних [3, с. 28-30].

Що стосується технічного підходу, то варто звернутися до праці Дж. Фрулінгера, згідно з якою термін, що розглядається, являє собою сукупність методів, які використовуються з метою захистити дані від несанкціонованого доступу або внесення в них змін як при зберіганні, так і при використанні та подальшій передачі їх з одного гаджета чи платформи на інші. Цей фахівець вказує також, що нерідко Information security ототожнюють із безпекою даних (від англ. *data security*) [187].

У Розділі 2 українського Закону від 09.01.2007 № 537-V "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" серед ключових стратегічних цілей розвитку українського суспільства як інформаційного вказується, крім іншого, удосконалення законодавства щодо регулювання інформаційних відносин, а також покращення стану інформаційної безпеки у зв'язку із використанням сучасних інформаційно-комунікаційних технологій. Зазначене, своєю чергою, допоможе підвищити конкурентоспроможність України, у т.ч. у високоінтелектуальних сферах праці та покращити якість життя нашого народу завдяки економічному розвитку, повноцінному забезпеченню прав і свободи кожного з нас, а також наданню якісного, а головне рівного доступу до інформації. У Розділі 3 також вказуються принципи, на підставі яких має будуватися та функціонувати національна політика розвитку інформаційного суспільства у нашій державі. Серед іншого зазначаються принципи пріоритетності науково-технічного та інноваційного розвитку країни (що неможливо, на нашу думку, без детального врегулювання правових засад забезпечення охорони прав на об'єкти інтелектуальної власності), а також принцип повсюдного впровадження інформаційно-комунікаційних технологій (далі - ІКТ) у науково-освітню та культурну сфери, в охорону здоров'я та навколишнього середовища, так само як і принцип забезпечення інформаційної безпеки [80].

Пункт 13 зазначеного Розділу НПА присвячено конкретно інформаційній безпеці в інформаційному суспільстві, під якою Закон розуміє такий особливий стан захищеності життєво важливих інтересів України, всіх та кожного українця, при досягненні якого не допускається заподіяння шкоди у зв'язку із несвоєчасністю надання, невірогідністю чи неповнотою інформації. Також у такому разі має бути недопущений негативний інформаційний вплив, а з ним - і негативні наслідки застосування ІКТ. Не оминув Закон й "тріаду інформаційної безпеки", тобто

стан зазначеної захищеності окремо дозволяє не допустити порушення цілісності, конфіденційності даних, їх доступності, а також нелегальне поширення та використання таких відомостей. Щоб реалізувати зазначене в реальності, цей НПА пропонує такі варіанти дій:

- розробка якісної національної інформаційної інфраструктури та забезпечення захисту її особливо важливих елементів;
- створення та розвиток Національної системи конфіденційного зв'язку для передачі даних конфіденційного типу;
- підвищення рівня ознайомленості та координація активностей державних органів щодо виявлення, аналізу, прогнозування ймовірних загроз інформаційній безпеці, запобігання їм та своєчасної ліквідації наслідків, у тому числі і шляхом міжнаціональної колаборації;
- перегляд та покращення нормативно-правового регулювання забезпечення інформаційної безпеки [80].

Також окремо хотілося б відзначити таке поняття як "забезпечення інформаційної безпеки", під яким згаданий раніше проект Стратегії інформаційної безпеки 2015 року розуміє діяльність, націлену на своєчасне виявлення, запобігання та припинення загроз (як ймовірних, так і цілком реальних) інформаційній безпеці нашої країни [46, с. 4].

З урахуванням вищевикладеного, можна зробити висновок про схожість понять "інформаційна безпека" і "кібербезпека". Адже обидві категорії, що розглядаються, своєю метою ставлять захист даних і попередження загроз у комп'ютерних та мережевих системах. Але повністю ототожнювати їх не можна. Як зазначає І.М. Сопілко, кожна з них має різну націленість. Так, якщо кібербезпека має на меті захистити кіберпростір від кібернетичних атак, то інформаційна безпека поширює захист на цілісність, доступність та конфіденційність інформації, не беручи до уваги її форму. При цьому обидві досліджувані категорії використовують способи та

методи, спрямовані на безпеку та захист комп'ютерних систем та мереж від зловмисних дій, витоку даних та інших незаконних дій. Для обох категорій важлива цінність інформації, що ними охороняється [101, с. 112].

Вказане дає нам можливість зробити висновок про те, що кібербезпека – це один із важливих елементів структури інформаційної безпеки, яка, у свою чергу, є ключовим сегментом національної безпеки. Тому важливо забезпечити належний рівень захисту кожної із зазначених сфер, відповідно, необхідно розробляти нові та покращувати наявні методи протидії порушенням у них, що логічно призведе до захисту кіберпростору.

Таким чином, кібербезпека у відповідному просторі – не лише базовий елемент успішного бізнесу, а й державної політики. Але сучасні кіберзлочинці досягли суттєвого успіху у подоланні систем кібернетичного захисту на різних рівнях, постійно вдосконалюючи використовувані для цього методи та інструменти, а таке, у свою чергу, неминуче породжує зростання кількості кіберзагроз. Тому, у світлі вищевикладеного важливо також визначити поняття та суть цих загроз як негативних для кібернетичного простору факторів. Той самий Закон № 2163-VIII у п. 6 статті 1 визначає їх як можливі або наявні явища та обставини, що несуть небезпеку національним інтересам нашої держави у кіберпросторі, і які підривають її кібербезпеку, а також негативно впливають на кіберзахист її об'єктів [79]. Зазначимо, що суб'єктами, які створюють кібернетичні загрози, можуть бути різні індивіди (нерідко це "ображені" співробітники) або цілі групи, наприклад, терористичної спрямованості, як і вороже настроєні держави.

Інтелектуальна власність досить часто стає об'єктом подібних зловмисних дій, так само як і персональні дані клієнтів відомих комерційних підприємств, зазвичай таке має на меті фінансову наживу або "обхід" конкурентів. Найчастіше загрози кібербезпеці проявляються у формі комп'ютерних вірусів, троянів, зловмисних дій та витоку даних, DoS-атаках та

подібних діях. До перелічених форм варто також додати отримання несанкціонованого доступу, так само як і знищення, пошкодження, крадіжку інформаційних активів, інтелектуальної власності або будь-якої іншої форми даних, які розуміються як конфіденційні. Зазвичай кіберзагрози залежно від джерела походження умовно поділяють на такі, що походять від довірених користувачів та ті, що походять із віддалених місць від невідомих суб'єктів. Таким чином, можна зробити висновок про те, що **кіберзагроза (або загроза кібербезпеці)** є зловмисною дією, мета якої полягає в пошкодженні електронної інформації, крадіжці даних або порушення цифрового життя в цілому.

Поняття кіберзагрози як небажаного фактору у кіберпросторі тісно пов'язане із такими ймовірними наслідками як інцидент кібербезпеки та кібератака. Перший із зазначених концептів, також відомий як кіберінцидент, згідно із п. 3 Статті 1 Закону № 2163-VIII є певною несприятливою ненавмисно подією або рядом таких, або такою, яка має ознаки можливої кібератаки і становить загрозу кібернетичній безпеці. У цьому ненавмисним вважається випадок помилки, чи природного, технічного, технологічного характеру. На противагу кіберінциденту існує поняття кібератаки (п. 4 Статті 1), а саме навмисної дії у кібернетичному просторі, яку зловмисники здійснюють із використанням спеціальних електронно-комунікативних засобів. У цьому випадку метою такої зловмисної дії зазвичай є порушення "тріади інформаційної безпеки", тобто конфіденційності, цілісності, доступності електронних інформаційних ресурсів, а також отримання несанкціонованого доступу до них. У перелік навмисних дій у вигляді кібератаки також можна включити порушення стійкого, надійного, штатного режиму функціонування комунікаційно-технологічних систем, використання їх ресурсів для здійснення атак на інші об'єктів кібернетичного захисту [79].

Крім зазначеного Закону про кібербезпеку, питання, пов'язані із правовим забезпеченням функціонування кіберпростору в Україні, регулюються також наступними нормативно-правовими актами:

- Конституцією як Основним Законом нашої держави;
- Законами "Про національну безпеку України" (від 21.06.2018 № 2469-VIII), "Про засади внутрішньої та зовнішньої політики" (від 01.07.2010 № 2411-VI), "Про інформацію" (від 02.10.1992 № 2657-XII), "Про основні засади забезпечення кібербезпеки України" (від 05.10.2017 № 2163-VIII), "Про електронні комунікації" (від 16.12.2020 № 1089-IX) та іншими;
- міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України, у т.ч. Конвенцією про кіберзлочинність;
- указами Президента України,
- актами КМУ;
- іншими українськими нормативно-правовими актами.

Відповідно до статті 107 української Конституції, координаційним органом з національної безпеки та оборони при Верховному головнокомандувачі країни визнано Раду національної безпеки та оборони України (далі – РНБО). Цей орган здійснює контроль та координацію діяльності держорганів з питань безпеки та оборони. Президент нашої держави формує склад РНБО (куди входять також Голова СБУ, Прем'єр-міністр, міністри оборони, внутрішніх та закордонних справ), а також є її головою. Саме його указами вводяться у дію рішення Ради [45].

Так, одним із таких рішень є акт № 685/2021 від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки". Така Стратегія буде реалізована у період до 2025 року. Вона визначає актуальні загрози та виклики української нацбезпеки в інформаційній сфері, а також перелічує головні цілі та завдання у боротьбі із такими загрозами та ті, що спрямовані на забезпечення належного рівня захисту прав громадян на інформацію і

захист їх персональних даних. Головний курс Стратегією взято на посилення можливостей забезпечення державної інформаційної безпеки та функціонування інформаційного простору, так само як і на надання підтримки інформаційними засобами та заходами політичній, соціальній стабільності держави. Не менш важливою метою акту є якісне забезпечення надійного захисту державного суверенітету, територіальної цілісності країни, її демократичного конституційного устрою, а також забезпечення прав та свобод кожного українця [88].

Щодо Стратегії кібербезпеки, то Указом Президента № 447/2021 "Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" така затверджена та введена в дію. Цим документом у п. 1 вказується на пріоритетність у системі нацбезпеки забезпечення кібербезпеки, реалізація чого запланована за рахунок посилення можливостей національної системи кібербезпеки для протидії кібернетичним загрозам у сучасному середовищі безпеки. Стратегія підкреслює, що кіберпростір нарівні із фізичними просторами розглядається як можливе поле для ведення військових дій. Також вказується на тенденцію до використання сил кібервійськ, до завдань яких, крім іншого, належить ведення превентивних наступальних акцій у кіберпросторі, у т.ч. і з можливістю виведення з ладу критично важливих об'єктів інфраструктури вороже настроєного опонента через знищення інформаційних систем, що управляють ними. Ще документ гарантує українцям безпечне функціонування національного сегменту кіберпростору та націлений на досягнення нашою державою належного рівня соціально-економічного розвитку у цифровому світі, для чого їй і потрібно бути здатною ефективно стримувати деструктивні дії у кіберпросторі [87].

Стратегія у частині п. 3 присвячена викликам і кіберзагрозам національному кіберпростору. До перших віднесено:

- застосування кібернетичних засобів із метою ведення конкуренції між країнами;
- змагальна націленість розвитку засобів кібербезпеки;
- мілітаризація кіберпростору та розвиток кібернетичної зброї з метою кібернападів та розвідувально-підривної активності у цифровій сфері;
- вплив пандемії коронавірусу (COVID-19) на економіку і соціальну сферу у вигляді повсюдного використання дистанційного режиму взаємодії та інше.

Серед загроз, названих Стратегією, варто згадати, наступні:

- гібридну агресію проти України у кіберпросторі;
- кіберзлочинність, адже така суттєво зменшує довіру людей до інформаційних технологій, цим результуючи у відчутні матеріальні втрати;
- тривалі приховані кібератаки під проводом зарубіжних урядів із метою викрадення важливих даних та здійснення розвідувально-підривної діяльності;
- кібертероризм у кібернетичному просторі та його підтримка [87].

Пункт 5 Стратегії присвячений пріоритетам забезпечення кібербезпеки є нашої країні, а саме:

- безпеці кібернетичного простору для захисту суверенітету та розвитку українського соціуму;
- захисту прав та свобод українців у такому просторі;
- європейській та євроатлантичній інтеграції у сфері кібернетичної безпеки.

Також зазначається, що для досягнення зазначеного важливо визначити та встановити зрозумілі стратегічні цілі, перелік яких зазначений у цій Стратегії [87]. Щодо указаного зазначимо Рішення РНБО п0087525-21 "Про План реалізації Стратегії кібербезпеки України" від 30.12.2021 (введено в дію президентським наказом № 37/2022 від 1 лютого 2022 року).

Його метою є розробка системи індикаторів стану кібернетичної безпеки, в яку будуть включені базові індикатори розвитку національної системи кібербезпеки та її безпосереднього стану, а також стану кіберзахисту критичної інформаційної інфраструктури, національних інформаційних ресурсів та даних, які захищені у відповідності до нашого законодавства. Також окремі розділи документа присвячені наступним цілям:

- **забезпечення ефективної кібернетичної оборони.** Для досягнення цієї мети, крім іншого, у країні будуть створені та отримають свій розвиток особливі підрозділи, наділені повноваженнями вести збройне протистояння у кіберпросторі ("кібервійська"). Також буде забезпечено ефективну взаємодію головних суб'єктів національної системи кібербезпеки та сил оборони в ході різноманітних заходів із кібероборони, буде проведено їх якісне навчання та надано необхідне фінансове забезпечення;
- **ефективна протидія кіберзлочинності.** За допомогою аналізу практик США та країн Європи щодо електронних доказів, імплементації норм Конвенції про кіберзлочинність, розробки концептуальних підходів до реалізації державної політики у сфері забезпечення прав українців у кіберпросторі держава планує забезпечити набуття своїми органом можливостей для мінімізації загроз кіберзлочинності та розслідування таких. З цією метою також заплановано створення та впровадження методик збору кіберстатистики, проведення щорічних соціологічних досліджень з кіберзагроз, комунікації між державою та суспільством у відношенні протидії кібернетичним атакам та інцидентам; механізмів ідентифікації суб'єктів електронної комерції у кібернетичному просторі; а також забезпечення регламентації правового статусу криптовалют тощо;

- **ефективна протидія розвідувально-підривної діяльності у кіберпросторі та кібертероризму.** Держава вживає необхідних заходів для безперервного ведення контррозвідки з метою виявити, обмежити, попередити розвідувально-підривну активність агресивно налаштованих держав, кібершпигунів, кібертерористів, для чого передбачається створення загальнодержавної системи виявлення кібератак і протидії терористичним та актам шпигунства в кіберпросторі та щодо об'єктів критичної інформаційної інфраструктури. Також будуть створені особливі можливості для автовиявлення кібератак у режимі реального часу, переглянуто та вдосконалено нормативно-правове забезпечення у цій сфері та інше;
- **розвиток асиметричних інструментів стримування.** У країні буде створено належні умови для успішного стримування антиукраїнської агресії у кіберпросторі на основі особливих заходів у сфері економіки, дипломатії, розвідки та залучення спеціалістів із приватного сектору. Для цього передбачається посилення забезпечувальних заходів щодо кібербезпеки інформаційної інфраструктури та інформаційних ресурсів закордонних українських дипломатичних установ та об'єктів державної власності. Також буде запроваджено особливий підхід щодо застосування санкцій, гармонізований з євроатлантичною спільнотою та налаштований безперервний обмін з партнерами інформацією про деструктивну діяльність у кіберпросторі;
- **національна кіберготовність та надійний кіберзахист.** З метою забезпечити економічний добробут і захистити права і свободи українців, держава посилить та забезпечить режим постійної готовності до кіберзагроз, для чого буде розроблено план реагування на надзвичайні ситуації в кібернетичному просторі, створено національну систему управління інцидентами, забезпечено безперервний моніторинг національних електронних комунікаційних

систем, розроблено мінімальні вимоги та рекомендації щодо забезпечення кібербезпеки. Окремо буде створено національний сервіс доменних імен;

- **безпечні цифрові послуги.** Для забезпечення таких буде розроблено спеціальні національні стандарти, вимоги щодо безпеки додатків, гаджетів, мереж, серверів, клауд-платформ тощо. Також буде створено необхідні умови, у т.ч. на законодавчому рівні, для перевірки автентичності інтернет-користувачів;
- **зміцнення системи координації.** Передбачається створити умови, що сприяють ефективній взаємодії суб'єктів забезпечення кібербезпеки під час роботи національної системи кібербезпеки, для чого необхідно розробити та впровадити порядок проведення огляду такої системи. Також будуть запроваджені механізми заохочення приватного сектору, представників академічних кіл, громадських організацій та окремих українців для участі у реалізації активностей із забезпечення кібербезпеки;
- **науково-технічне забезпечення кібербезпеки та становлення кіберобізнаного суспільства.** Фундаментальна реформа системи підготовки та підвищення кваліфікації спеціалістів з кібербезпеки, підвищення кіберпроінформованості населення про сучасні кіберзагрози та протидію їм забезпечуватимуться шляхом координації та стимуляції наукової спільноти при проведенні досліджень та розробок у галузі кібернетичної безпеки, а також запровадження Загальнонаціональної програми кіберграмотності. Також почнуть діяти спеціальні центри з обміну досвідом у відповідних питаннях;
- **формування нової моделі відносин у сфері кібербезпеки.** Буде введена сервісна модель держучасті у заходах з кіберзахисту, де Україна виступатиме саме як партнер, а не вказівник. З цією метою

планується розробити законопроект щодо врегулювання питань державно-приватного партнерства у відповідному правовому полі та залучати на регулярній основі вчених та незалежних кіберекспертів до створення інших проектів у цій сфері;

- **прагматичне міжнародне співробітництво.** Будуть покращені відносини з міжнародними партнерами у галузі спільної відповіді на кібератаки, обміну інформацією про інциденти, ведення спільних кібероперацій. Для цього планується забезпечити участь нашої країни у міжнародних заходах ООН з питань кіберпростору та доопрацюванні Другого додаткового протоколу до Конвенції про кіберзлочинність. Буде вестися діалог з міжнародними партнерами з метою отримання доступу до системи Інтерполу 1-24/7 та поглиблено співпрацю з Міжнародним союзом електрозв'язку у сферах кібербезпеки та електронних комунікацій тощо [85].

У п. 7 Стратегії кібербезпеки зазначено напрями зовнішньополітичної діяльності держави у відповідній сфері. До таких, крім іншого, відноситься співпраця із міжнародними партнерами та різними зацікавленими сторонами, у яких з Україною збігається бачення майбутнього кіберпростору щодо його глобальності, відкритості, стабільності, заснованості на дотриманні прав людини та демократичних цінностей. Також українська держава й надалі активно вестиме міжнародний діалог щодо поведінки суб'єктів у кіберпросторі. Що стосується регулювання Інтернету, важливо, щоб він залишався глобальним і відкритим, орієнтованим на дотримання прав і свобод людей, підтримки конфіденційності у кібернетичному просторі. Також наша держава буде діяти особливо активно у дискусіях ООН та інших міжнародних форумах для розвитку інституту кібербезпеки з метою зниження небезпеки милітаризації кіберпростору [87].

Відповідно до п. 8 Стратегії, її реалізація покладена на органи нацбезпеки, українське МЗС, Мінцифри, МОН та інші суб'єкти, діяльність яких пов'язана із забезпеченням кібербезпеки. А координувати таку реалізацію має Національний координаційний центр кібербезпеки при РНБО, який зобов'язаний публічно звітувати про стан реалізації Стратегії [87].

Норми щодо стратегії кібербезпеки України містяться і в Законі № 2469-VIII про нацбезпеку, а саме в статті 31. У відповідності до неї, Стратегія кібербезпеки нашої держави є документом довгострокового планування, де визначено пріоритети національних інтересів країни щодо кібербезпеки, кіберзагрози інтересам кіберсуб'єктів у кіберпросторі, підходи та напрямки у реалізації державної політики по забезпеченню функціонування кіберпростору. Також у п. 3 зазначеної статті вказано, що саме така Стратегія має бути основою для держпрограм та НПА у галузі кібербезпеки нашої держави. Її реалізація має ґрунтуватися на основних типах потенціалу (оборонного, економічного, інтелектуального тощо) із залученням механізмів державно-приватного партнерства і міжнародної допомоги [78].

Отже, правове забезпечення функціонування кіберпростору в Україні представлено програмними та регулюючими документами, які містять завдання та індикатори вирішення таких завдань для досягнення належного рівня захищеності кібернетичного простору нашої держави. Крім нормативно-правового регулювання варто також запропонувати набір принципів, без яких, на нашу думку, буде дуже складно досягти зазначених цілей за допомогою тільки застосування норм чинних НПА. Таким є:

- *принцип поваги права і свободи людини.* Усі дії влади в кіберпросторі повинні бути націлені на забезпечення дотримання таких прав та інтересів, а будь-які обмеження, що вводяться, не повинні порушувати такі права;

- *принцип відповідальності.* Кожен окремо взятий учасник відносин у кіберпросторі повинен нести відповідальність за збереження стабільності у ньому;
- *принцип розумності та усвідомленості.* Кожен суб'єкт повинен думати перш ніж вчинити дію, внаслідок якої може бути поставлена під удар стабільність кіберпростору;
- *принцип необхідного втручання.* У разі недотримання попереднього принципу, необхідні відповідні дії з боку суб'єктів забезпечення функціонування кібернетичного простору в Україні.

Не менш важливим ми вважаємо розробку та впровадження принципів та стандартів, спрямованих на недопущення та запобігання дестабілізуючим діям, а також на стимуляцію ведення заходів щодо зміцнення стабільності кібернетичного простору.

2.3. Цифровізація як елемент кіберпростору у науці та законодавстві

Вище було досліджено суть кібернетичного простору, дано його визначення, яке, звичайно, не є остаточним і потребує регулярного перегляду, оновлення, адже такий домен є досить динамічним, він постійно трансформується, адже щоденно з'являються нові види взаємин у ньому, зростає кількість суб'єктів (акторів), формуються модернізовані кіберзагрози. У зв'язку із цим важливо також розглянути такий елемент кібернетичного домену, як цифровізація або діджиталізація (від англ. *digitalization*).

Як і у випадку із попередніми концептами та категоріями, єдиного визначення цифровізації немає. У широкому сенсі під нею розуміється використання цифрових технологій для отримання певних благ, створення нових активів. Це особлива тенденція розвитку людської цивілізації, що формує більш інклюзивне суспільство та якісніші механізми управління, як

вказує К. Маркевич. На її думку, цифровізація - це спосіб розширення доступу до освітньої, медичної, сфери держпослуг та продовольчої сфери. У цьому діджиталізація не обмежується лише використанням технологій, а передбачає також культурні зміни у всіх робочих сферах [51].

Цікаву думку висловлюють вчені про зміну парадигми нашого мислення, дій, спілкування із навколишнім світом та іншими індивідами як основи цифровізації, при цьому технологи не є тут певною метою, а є саме інструментом. Розглянуте поняття сприймається як пов'язане із культурними змінами та переробкою традиційних моделей взаємодії [61, с. 84, 88]. У цьому чітко простежується неможливість оцифровки, тобто повної цифровізації всієї доступної інформації.

Розуміння аналізованого концепту як цифрового способу зв'язку, передачі, запису інформації у вигляді використання цифрових пристроїв притаманно для деяких словників [119]. Під час пошуку терміну цифровізації у Вікіпедії, веб-сайт перенаправляє на сторінку про цифрову трансформацію (англ. *digital transformation*), під якою розуміє трансформацію управлінської системи через перегляд моделей, операцій, стратегії, виробленого продукту та подібного із використанням цифрових технологій. Мета феномена у цьому випадку - це прискорення продажу та зростання як комерційних підприємств, так і організацій, функціонуючих без мети отримання прибутку [118].

У зв'язку із цим варто детальніше вивчити різницю у термінологічному апараті, а саме між поняттями "цифровізація", "діджітізація" (від англ. *digitization*), "автоматизація", "оцифрування" та "цифрова трансформація". Дослідження відмінностей має особливу цінність, оскільки терміни часто плутають і використовують як синоніми, що ускладнює, зокрема, правове забезпечення цих процесів.

Так, під автоматизацією прийнято розуміти один із шляхів науково-технічного прогресу, який реалізується через використання

саморегулюючих технічних засобів та математичних методів. Метою такого є мінімізація обсягу участі людини у отриманні та використанні ресурсів, у тому числі інформаційних. При цьому, як зазначає А. Клевець, цифровізацією варто вважати використання цифрових технологій для того, щоб змінити бізнес-модель, розвинути нові можливості для отримання прибутку, тобто йдеться про процес переходу до цифрового ведення комерційної активності. І цей концепт часто плутають із оцифровкою, хоча обидва є по суті щаблями однієї піраміди, вершина якої – цифрова трансформація. Так, оцифровка передбачає переведення інформації із паперової чи іншої фізичної форми у форму цифровою. Це перший рівень згаданої піраміди, другим буде безпосередньо цифровізація. У розумінні О. Клевець йдеться про використання цифрових технологій з метою отримання прибутку та покращення цифрової культури. Цифрова трансформація вінчає цю піраміду [40].

Як вказує всесвітньо відомий технологічний гігант I-scoop, діджиталізація – це процедура створення цифрової версії аналогових чи фізичних речей. Таким чином, має місце переведення в байти та біти паперових документів, фото та іншого контенту [160]. Відповідно, можна дійти логічного висновку у тому, що діджиталізація - це оцифровка, яка вже згадувалася вище. При цьому оцифровка не означає автоматичної заміни оригінального документа, останній або зберігається, або знищується.

Діджиталізація ж може бути розглянута з точки зору таких трьох підходів:

- *діловий*. Він передбачає використання інформаційних технологій для покращення, перетворення бізнес-моделей, операцій та функцій з урахуванням певної вигоди;
- *сферовий*. Передбачає не просто оцифрування документів, а й роботу із використанням цифрових інструментів на кшталт різних гаджетів

та соціальних платформ для спільної роботи, тобто “цифровим способом”

- *інноваційний*. Він передбачає безперервне впровадження цифрових технологій у всі доступні види та сфери суспільної діяльності [160].

Цифрова трансформація, на думку М.С. Гупта, є трансформацією бізнесу, яку забезпечує цифровізація. При цьому він вказує на неточність у використанні терміна «цифрова», оскільки природа цифрової трансформації передбачає зміну бізнес-процесів, що зумовлено технологіями цифровізації. Як приклад використовується перехід від локального управління фізичними процесами до віддаленого моніторингу та менеджменту тими самими процесами. Також дослідником пропонується у зв'язку із вказаним такий термін як "індустрія 4.0", під яким він розуміє європейський підхід щодо симбіозу цифрової трансформації та цифровізації [195].

Таким чином, цифровізація використовує оцифровку, щоб зробити ділові, соціальні, економічні, правові та інші процеси ефективнішими та продуктивнішими. Можна запропонувати такі приклади діджиталізації:

- використання хмарних платформ для збереження та розповсюдження документації;
- централізація інформації про суб'єктів, наприклад, клієнтів. Відповідні дані можуть включати контактну інформацію осіб, історію операцій тощо;
- розробка та впровадження автоматизованих робочих процесів, наприклад, якщо йдеться про інтернет-магазин, то після розміщення відповідного замовлення на сайті фірми, буде створено автоматично рахунок-фактуру та надіслано на пошту покупцю тощо.

Саме хмарні платформи та сервіси стали одним із основних каталізаторів цифровізації у світі, так як завдяки їх використанню можна істотно знизити рівень витрат, підвищивши при цьому ефективність робіт.

Дані платформи забезпечують простоту доступу до своїх сервісів, полегшують ведення робочих процесів та консолідацію локальних і веб-додатків. Сьогодні практично кожна державна структура як в Україні, так і в більшості країн світу має своє віртуальне "представництво" у вигляді веб-сайтів, так само як і більшість користувачів досить вміло використовують цифрові технології.

Компанії, інституції та інші організації обирають цифрову трансформацію, щоб краще орієнтуватися у вимогах та потребах користувачів. Завдяки такому феномену, суб'єкти зможуть не тільки краще зрозуміти потреби споживачів своїх послуг, а й залучити більше методів і способів взаємодії із ними. Також досягається більш якісна та широка інтеграція між декількома робочими процесами.

Варто вказати на нелінійність процесу цифрової трансформації, адже він, як уже вказувалося вище, відбувається певними стадіями - від оцифрування до цифровізації, і лише потім може бути досягнуто цифрової трансформації. При цьому вона включає всі аспекти діяльності організації, незалежно від галузі, в якій та функціонує, і рівня цифровізації в ній.

Повертаючись до різниці між поняттями, зазначимо думку П. Богущ, згідно з якою оцифровка допомагає розкодувати (або навпаки) дані, у той час як цифровізація покращує робочі процеси. А цифрова трансформація відповідає за створення бізнесу (справи, проекту) за допомогою цифрових технологій за рахунок використання сучасних інноваційних продуктів та технологій на кшталт Інтернету речей та штучного інтелекту. Фахівець порівняла всі три поняття за певними критеріями та дійшла наступних результатів:

- Ціль. У оцифровки – кодування інформації, у цифровізації – її обробка, у цифрової трансформації – використання отриманих знань та відомостей;

- Завдання. Перетворення контенту з аналогового у цифровий формат; автоматизація існуючих операційних та бізнес-процесів; зміна організаційної культури на підприємстві, в інституції, з метою впровадження та надання нових послуг і корисних продуктів (відповідно);
- Діяльність. Процедура перетворення паперових документів, аналогових носіїв та іншого контенту на цифровий формат; створення та впровадження наскрізних робочих процесів у цифровому форматі; інтеграція різних процесів запровадження інформаційних цифрових технологій на підприємстві, в інституції (відповідно);
- Інструментарій. Комп'ютерна техніка та інше обладнання для кодування та оцифрування; інформаційно-технологічні системи, послуги та додатки; інноваційні технології (відповідно);
- Можливі перешкоди. Великий обсяг контенту; фінансові витрати та висока вартість впровадження; небажання працівників та інших індивідів сприяти трансформації (відповідно) [138].

Таким чином, можемо підсумувати, що оцифрування (диджитизація) – це процес створення цифрової об'єктивної форми фізичних об'єктів. При цьому цифровізація, тобто диджиталізація, є забезпечення або поліпшення ділових та інших процесів шляхом використання цифрових технологій та диджитизованої інформації. І третій ступінь, цифрова трансформація – це безпосередньо трансформація бізнесу, що забезпечується диджиталізацією.

Варто також відзначити, що 29 жовтня до Верховної Ради України було внесено законопроект №6241 про Національну програму інформатизації, який містить, в тому числі, визначення останньої як процесу впровадження цифрових технологій в усі сфери життя українського суспільства (п.18 Статті 1) [91].

Цифровізація сьогодні - це важливий аспект державної політики, особливо в часи пандемії та інформаційної війни, що ведеться в рамках

гібридної війни проти України. Діджиталізація - це той інструмент, завдяки якому ми можемо працювати і комунікувати, перебуваючи практично у будь-якій точці земної кулі. Вона дозволила нам проводити наради та зустрічі у форматі відеоконференцій, полегшила нам доступ до освіти, дозволивши отримувати знання дистанційно, купляти товари та послуги не виходячи з дому, вирішила багато наших соціальних проблем, наприклад, у відношенні охорони здоров'я, дозволивши нам записувати до лікарів через електронні черги та замовляти ліки в онлайн-аптеках, підвищила ефективність надання держпослуг, наприклад, через додаток Дія тощо.

Для цифровізації характерними є наступні позитивні риси:

- мінімізація витратної частини, адже дані тепер існують у електронному вигляді, а не у "матеріальному", що, в свою чергу, призводить до оптимізації основних робочих процесів;
- перехід на більш "екологічний" рівень, що впливає із попередньої тези, адже обсяг споживання "паперу" істотно скорочується;
- розподіл виробництва товарів та послуг, що здатне істотно підвищити продуктивність на підприємстві;
- підвищення культури та цифрової грамотності, краще розуміння особливостей та функціонування пристроїв;
- забезпечення швидкого реагування на виникаючі проблеми та виклики;
- спрощення та поліпшення комунікації із кінцевим споживачем товарів та послуг.

У державному секторі нашої країни цифрові технології стали одним із ключових аспектів (напрямів) у реформуванні держуправління, що зробить його не лише ефективним, а й досить сучасним і таким, що легко пристосовується до нових викликів і тенденцій. Таким чином, діджиталізацію варто розглядати не як основну мету, а саме як інструмент розвитку інформаційного суспільства, без чого неможлива сучасна

демократія. Цифровізація - це також й каталізатор економічного зростання, викликаного, зокрема, підвищенням робочої продуктивності. У свою чергу, зазначене позитивно відбивається на підвищенні якості життя українців.

Як зазначає К. Маркевич, цифровізація, окрім позитивних аспектів, має і негативні результати, а саме:

- повсюдна автоматизація, залучення до роботи робототехніки тощо завдає удару та порушує ринок праці, а, отже, має місце високий ризик безробіття та нерівності доходів;
- зростають ризики безпеки та можливості для порушення конфіденційності;
- спостерігається погіршення рівня культури та деградація, а з ними - розвиток та укорінення соціальної відчуженості;
- так званий "цифровий розрив", що формується внаслідок недовіри цифровим технологіям та невміння ними користуватися [51].

В Україні з грудня 2014 року діяв спеціально створений Комітет Верховної Ради України з питань інформатизації та зв'язку із 9 депутатами у своєму складі. У його віданні перебувало 12 напрямів, зокрема розвиток інформаційного суспільства, телекомунікації та індустрія програм, криптографічний захист даних, електронні цифрові підписи, документообіг та управління, кібернетична безпека, програма національної інформатизації та інше. У 2019 році на зміну даному органу прийшов Комітет Верховної Ради України з питань цифрової трансформації, до складу якого увійшли 8 депутатів. Відповідно до Постанови Верховної Ради України № 19-ІХ від 29 серпня 2019 року, до відання органу, крім держпрограми інформатизації, віднесено такі питання як:

- кібербезпека, технічний та криптографічний захист інформації;
- електронні демократія, довірчі послуги та цифрова ідентифікація, комерція, документообіг, а також управління та публічні послуги;

- законодавчі засади та принципи цифровізації, цифрового суспільства, адміністрування, функціонування та використання Інтернету в українській державі;
- розвиток екосистеми стартапів та інновації у галузі цифрового підприємництва;
- державні інформаційні ресурси, інформаційно-аналітичні системи, електронні бази та реєстри;
- дослідні центри у сфері цифрових технологій;
- смартінфраструктура, цифрова промисловість, телекомунікації, розвиток цифрових компетентностей;
- віртуальні активи, а також блокчейн та токенизація;
- цифрові права та розвиток сегмента «відкритих даних» (від англ. *open data*);
- програми цифрового співробітництва, зокрема "Єдиний цифровий ринок" та інше [84].

Крім того, КМУ, у процесі оптимізації системи центральних органів виконавчої влади, своєю постановою №829 від 02 вересня 2019 року створив Міністерство цифрової трансформації України, а постановою №856 від 18 вересня 2019 року затвердив Положення про нього. Сьогодні це Міністерство, скорочено зване "Мінцифри", є основним засвідчувальним органом виконавчої влади у сфері електронних довірчих послуг та ідентифікації, воно забезпечує розвиток інформаційного суспільства, а також формування та реалізацію держполітики у таких галузях та сферах як:

- цифровізація, цифрові розвиток, економіка, технології та інновації;
- електронні демократії, управління, бізнес, документообіг;
- цифрова грамотність населення;
- розвиток національних електронних інформаційних ресурсів (далі – ЕІР), інфраструктури широкопasmового доступу до Світової мережі;

- правовий режим Дія Сіті тощо (відповідно до п. 3 Положення) [60].

Також Мінцифри наділено функціями генерального держзамовника Національної програми інформатизації й інших програм цифровізації державного значення, серед яких варто відзначити здійснення моніторингу у сфері інформатизації та погодження і координацію проектів щодо неї; забезпечення нормативно-правової, інформаційної та інших видів підтримки активностей з виконання Національної програми інформатизації (П. 5 Положення). Також Міністерство погоджує призначення голови з питань цифрового розвитку, цифрових трансформацій або цифровізації (CDTO), відповідно до п. 7 Положення [60].

Варто вказати і на Постанову КМУ №606 від 08 вересня 2016 року, якою була введена в дію система електронної взаємодії державних ЕІР при зверненні суб'єктів для отримання адміністративних послуг та затверджено інші положення щодо електронної взаємодії відповідно до вимог ЄС [16]. Також щодо цифровізації діють такі закони як №2155-VIII «Про електронні довірчі послуги» від 05.10.2017, що регулює розробку цифрової інфраструктури довіри як ключового елемента цифрової економіки [72], та 2297-VI "Про захист персональних даних" від 01.06.2010, спрямований на захист основних прав і свобод громадян у зв'язку із обробкою їх персональних даних [75].

Раніше було вказано на негативні аспекти цифровізації. Також існує низка проблем, які потребують усунення для подальшого розвитку та досягнення диджиталізаційних цілей, для чого необхідно:

- активно боротися зі зростанням кіберзлочинності з огляду на те, що зловмисники в умовах збільшення кількості інформаційних систем істотно розширили арсенал своїх навичок та умінь, особливо при порушенні конфіденційності інформації та зломах персональних даних;

- розробити та впровадити особливий механізм (процедуру) підтвердження ідентифікаційних даних, адже відсутність такого відіграє на користь вищезгаданих кіберзлочинців, а потім - забезпечити захист обміну такою інформацією у відношенні фізичних та юридичних осіб, що підлягає обробці у різних державних та приватних інформаційних системах;
- переробити та внести відповідні зміни до механізмів використання систем реєстрації та контролю доступу до інформсистем, оскільки на даному етапі часто використовуються технологічно несумісні алгоритми та протоколи електронної ідентифікації.

Також варто відзначити рекомендації К. Маркевич, провідної експертки економічних та соціальних програм, щодо подолання викликів у галузі цифровізації. Так вона наполягає на потребі:

- забезпечення усілякого сприяння формуванню цифрової сумісності між світовими державами. Для цього потрібно розробити пакет глобальних основ (правил) з урахуванням відмінностей між такими суб'єктами щодо культурних, економічних та політичних поглядів. Дане зведення правил передбачало б, крім іншого, розробку уніфікованого глобального акта, в якому були б представлені принципи і пріоритети поширення цифрових технологій, які вже отримали своє визнання у більшості країн світу, і чия ефективність підтверджена міжнародною практикою. Це забезпечило б інтероперабельність у цифровій сфері всього світу, викорінення фрагментації глобального простору, а також формування цифрових «островів»;
- запровадження міжнародної платформи, яка допомагатиме боротися із негативним впливом цифрових технологій та долати ризики та виклики щодо порушень конфіденційності та проблем із безпекою;

- підвищення рівня якості роботи статистичних систем, що необхідно для безперервного та повноцінного моніторингу процесів впровадження діджитал-технологій та їх соціально-економічних результатів у динаміці. У цьому передбачається удосконалення статистичного нагляду на мікрорівні, тобто саме на рівні ФОПів, домогосподарства тощо;
- викорінення цифрового розриву між людьми та іншими інформаційними суб'єктами через посилення цифрового розвитку. Влада держав має спільними зусиллями скорочувати цифровий розрив не лише між країнами з різним рівнем розвитку, а й між різними соціальними спільнотами у будь-якій державі;
- створення надійних та ефективних технологій для кожного. Цифрові технології повинні забезпечувати велике охоплення користувачів, суттєво зменшувати затратну частину та підвищувати ефективність. Насамперед вказане особливо важливе для представників малого та середнього бізнесу. Аспект надійності технологій проявляється у забезпеченні належного рівня захисту конфіденційності інформації, функціонуванні перевірених систем онлайн-спорів та алгоритмів, заснованих на принципі недискримінації користувачів. Як зазначає К. Маркевич, у цьому особливу роль відіграє розвиток та забезпечення державно-приватного партнерства при людиноцентричному підході;
- заснування особливого фонду підтримки, фінансові кошти від якого підуть на цілі розвитку цифрової інфраструктури та поширення технічної та цифрової освіти у менш розвинених державах, що, знову ж таки, дозволить суттєво скоротити цифровий розрив [51].

Варто зазначити, що Україна активно працює у напрямі підвищення рівня цифрової, кібернетичної та інформаційної грамотності свого населення. Так, за часів пандемії коронавірусу для українців стали доступні безкоштовні онлайн-курси, у т.ч. "Оплата комуналки онлайн", "Цифрова

грамотність державних службовців" та інші. Як зазначає Н.С. Чередніченко, до 2022 року, українська влада анонсувала залучення близько 6 млн. громадян у програму розвитку цифрових навичок, віковий ценз респондентів, які проживають у регіонах, при цьому становить від 35 до 65 років і більше. Також уряд планує у найближчі три роки зробити "цифровими" близько 100 державних послуг [120].

Під час написання даного розділу дисертаційного дослідження Україна була атакована Російською Федерацією, війна йде по всіх основних фронтах, у тому числі, інформаційному. Мінцифри закликав українців взяти до рук цифрову зброю, тим самим скориставшись благами цифровізації. І такою зброєю названо смартфони та доступ до всесвітньої мережі. Так, з їх допомогою можна:

- написати у телеграм-чатбот «Ворог», щоб надіслати повідомлення збройним силам нашої держави про місце перебування ворожих військ на нашій території, а також долучити до свого допису відповідні фотоматеріали;
- стати частиною так званої ІТ-армії України, в лавах якої українці можуть атакувати (наприклад, через DDoS-атакування) веб-портали країни-агресора, тим самим не даючи їм вести інформаційну пропаганду;
- вступити до лав Інтернет Військ України і нести правду по всьому світу та, відповідно, боротися із російською пропагандою онлайн [41].

Таким чином, цифровізація - це дієвий засіб боротьби із окупантами та протидії агресивним діям країни-агресора.

Можна зробити висновок і про те, що цифровізація – це один із дієвих способів подолати корупцію. Адже державні послуги надаватимуться "онлайн", що виключає спілкування з чиновниками наживо. Так, наприклад, через додаток (онлайн-застосунок) «Дія», що є елементом проекту «Цифрова держава», можна звернутися за отриманням державних

послуг, завантажити свої документи, які матимуть статус офіційних електронних копій, пройти корисні курси з цифрової грамотності та подібні, отримати фінансову допомогу в рамках держпідтримки тощо. Загалом проект «Цифрова держава» включає наступні елементи та напрямки взаємодії:

- електронне управління, тобто здійснення внутрішніх процесів управління країни за допомогою інформаційних технологій. У цьому випадку кожен українець отримає доступ до будь-яких даних про державу, тим самим буде дотримано принципу прозорості. Для владних структур це також корисно, адже вони матимуть доступ до правдивої інформації та зможуть приймати ефективні рішення;
- електронна демократія полягає у можливості для кожного громадянина за допомогою інформаційних технологій брати участь у різних аспектах життя України. Мається на увазі, що референдуми, опитування, громадські бюджети тощо. будуть проводитись в електронній (цифровій) формі;
- електронний суд із повністю цифровізованим документообігом, в рамках якого подання процесуальних документів та обмін такими між установами та учасниками слухань здійснюватиметься онлайн;
- електронна охорона здоров'я, при якій у кожного пацієнта буде власна медична карта в цифровому форматі, у кожній лікарні - повністю цифрова інфраструктура, у кожного лікаря - безперебійний доступ до спеціалізованих онлайн-платформ;
- електронна освіта. Воно включає як забезпечення відповідним обладнанням педагогів, так і доступ до електронних журналів успішності для батьків, та заміну паперових джерел на цифровий контент для учнів;

- електронна транспортна система, з впровадженням електронних квитків, мобільного паркування, наданням доступу до Інтернету на транспортних об'єктах та моніторингом трафіку;
- електронний бізнес з роботою тільки за безготівковим розрахунком та за допомогою ведення електронного документообігом, що суттєво прискорить та зробить більш ефективним розвиток компанії;
- розумні міста, які працюють за допомогою інтегрованих інформаційних систем, з доступними планами забудови та можливістю для кожного мешканця розуміти, що робиться для міста;
- кібербезпека, що включає в себе діяльність відповідних органів щодо забезпечення захисту державної та приватної інформації від несанкціонованого доступу та подальшого використання та інше [117].

Отже, діджиталізація здатна забезпечити фундамент для сталого добробуту нашої держави, саме вона провокує трансформації у багатьох сферах людської взаємодії, а також каталізує творчість як рушійну силу інновацій та активності щодо створення об'єктів інтелектуальної власності. Також, як зазначив у своїй доповіді М. Федоров, міністр цифрової трансформації нашої держави, цифровізація здатна забезпечити ріст економіки в країні на 10-12% на рік, а це дійсно вражаюча цифра.

Висновки до Розділу 2

У даному розділі дисертаційного дослідження на основі порівняльного аналізу та загальнонаукових методів пізнання було обґрунтовано місце кіберпростору у інформаційному середовищі, вказано на якість правового забезпечення його функціонування в Україні та на роль цифровізації як елементу кібернетичного простору у житті держави та її громадян. Вказане дало можливість дійти наступних висновків:

1. При визначенні місця кібернетичного простору (як інтерактивного домену, що складається із цифрових мереж, які використовується для зберігання, зміни, передачі та подібних дій із інформацією) в інформаційному середовищі перший концепт було охарактеризовано як елемент системи інформаційного середовища (сфери) на рівні із традиційним інформаційним простором. При цьому саме кіберпростір слід визнати центральним сегментом інформаційної сфери, оскільки у ньому сконцентровані глобальні потоки економічно-політичної природи та соціальних взаємин.
2. Українське суспільство як інформаційне ґрунтується на існуванні інформаційної сфери взаємодії, тому формування ефективного та стабільного українського інформаційного простору сьогодні є пріоритетним завданням для держави, адже таке дозволить створити і надалі розвинути стійкий кіберпростір. Для цілей зазначеного пропонується на офіційному рівні визначити правовий статус та становище інформаційних ресурсів з урахуванням права власності на них, рівнів захисту та доступу до інформації; внести поправки в існуючі нормативно-правові акти, що регулюють інформаційну сферу і безпосередньо кіберпростір, або розробити та запровадити нові, зокрема у відношенні прав й обов'язків інформаційних суб'єктів та інформаційного забезпечення органів державної влади.
3. Вважається за необхідне підкріпити нормативно-правове забезпечення функціонування кіберпростору, представлене у нашій державі програмними та регулюючими документами, системою принципів, серед яких: принцип поваги прав і свободи людини, коли вся активність владних органів у кіберпросторі націлена на забезпечення дотримання зазначених прав; принцип відповідальності, що передбачає відповідальність всіх учасників кібервідносин за збереження стабільності у кіберпросторі;

взаємопов'язані принципи розумності та усвідомленості, а також потрібного втручання, коли кожен користувач кібернетичного простору повинен насамперед осмислювати всі свої дії, які можуть спричинити порушення стабільності в ньому, і якщо принцип дотриманий не був, органами забезпечення функціонування українського кіберпростору будуть вчинені спеціальні дії.

4. Визначено, що "оцифрування" – це процес створення цифрової об'єктивної форми фізичних об'єктів; "цифровізація (діджиталізація) - це забезпечення або поліпшенням ділових та інших процесів шляхом використання цифрових технологій та діджитизованої інформації; "цифрова трансформація" - це безпосередньо трансформація бізнесу, що забезпечується діджиталізацією. Зазначено, що цифровізація може мати негативні результати у вигляді проблем з безпекою порушення конфіденційності, погіршення культурного рівня громадян, поглиблення їх соціальної відчуженості. Водночас підкреслюються позитивні характеристики цифровізації як важливого елемента кіберпростору: мінімізація витрат та оптимізація основних робочих процесів у зв'язку із відмовою від матеріальних форм зберігання даних, і, відповідно, перехід на більш "екологічний" рівень; підвищення культури та цифрової грамотності населення; забезпечення швидкого реагування на виникаючі кіберпроблеми та виклики; надання сприятливих умов для спрощеної та легкої комунікації із кінцевим споживачем товарів та послуг.
5. Запропоновано, з метою подолання викликів у галузі цифровізації та посилення наших сильних сторін на різних рівнях, наступне: сприяти формуванню цифрової сумісності між країнами світу із обов'язковою розробкою та впровадженням набору глобальних правил з урахуванням їх економічних, політичних та культурних відмінностей; забезпечити цифровий розвиток нації з метою

нівелювати цифровий розрив між різними соціальними групами; розробити та впровадити надійні технології для всіх громадян з одночасним зниженням рівня неефективності та витрат; створити та інтегрувати міжнародну платформу, яка використовуватиметься для вирішення проблем, спричинених негативним впливом цифрових технологій; створити фонд підтримки, кошти якого мають спрямовуватися на розвиток цифрової інфраструктури та цифровізацію в державі.

Результати дослідження, викладені у Розділі 2, відображено у таких публікаціях автора: [\[144\]](#); [\[338\]](#); [\[151\]](#); [\[153\]](#); [\[161\]](#); [\[166\]](#); [\[168\]](#); [\[358\]](#).

РОЗДІЛ 3. АКТУАЛЬНІ ПИТАННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ВІДНОСИН ЩОДО ДОТРИМАННЯ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ У КІБЕРПРОСТОРИ

3.1. Структура відносин щодо дотримання права інтелектуальної власності у кіберпросторі: юридична характеристика

Слово "структура" відоме майже кожному з нас. Походить воно від латинського слова *structura*, тобто "з'єднання, будівля". Як зазначає Оксфордський словник, це особливе розташування частин чогось або безпосередньо спосіб, у який частини чогось поєднані між собою, розташовані чи організовані [278]. Словник Британіка під терміном, що розглядається, також розуміє якість (особливість) чогось, що є ретельно спланованим, організованим та контрольованим [277]. Тобто можна зробити висновок, що під структурою загалом мається на увазі певна організація чи розташування елементів, що пов'язані між собою, у матеріальному об'єкті чи системі.

Доктринальні юридичні джерела зазвичай використовують термін "структура", у розумінні "склад", наприклад, при визначенні побудови правовідносин. Як зазначають деякі вчені, використовуючи термін "склад", основну увагу приділяють саме елементам правових відносин, в той час як поняття "структура" не тільки окреслює такі елементи, але й вказує на логічний зв'язок між ними. Таким чином, структуру правовідносин дослідники визначають як основні елементи відносин правового характеру, а також як спосіб юридичного зв'язку між ними у контексті соціальних благ та інтересів. Саме через структуру можна досягнути систему, тобто організованість цих відносин [105].

Слід вказати на те, що саме термін "структура", й на думку О.Ф. Скакун, є більш відповідним стану правовідносин, адже слово "склад" фіксує їх елементи, не вказуючи при цьому на логічну пов'язаність між

ними. Вона також зазначає, що відносини правового характеру - це логічно пов'язана конструкція всіх елементів, серед яких основне місце займають суб'єкти, якими суб'єктивні юридичні права і обов'язки реалізуються, і які несуть суб'єктивну юридичну відповідальність з метою досягнення результатів таких зв'язків цього зв'язку [97, с. 401].

Важливо також згадати, у контексті даного Розділу дисертаційного дослідження, що предметом ПІВ є відносини інтелектуальної власності у, так званому, вузькому розумінні, тобто особисті немайнові та майнові стосунки щодо володіння, використання, розпорядження результатами людської творчо-інтелектуальної активності. Як зазначає О.І. Харитонова, взаємини, що врегульовані законодавством про ІВ, бувають кількох видів (поділяються на групи):

- відносини ІВ у вузькому сенсі, є предметом цивільного права; вони виникають на підставі створення благ в результаті інтелектуально-творчої діяльності, або використання таких благ для власних потреб;
- особисті немайнові та майнові відносини, які формуються за фактом легалізації результатів вказаної діяльності - патентування винаходу, реєстрація авторських прав тощо;
- особисті та майнові відносини, що виникають у зв'язку із реалізацією своїх прав ІВ іншим особам - використання по договору, ліцензування тощо. Це так звані пов'язані зі сферою ІВ правові відносини [113, с. 87].

Відносини ІВ є фактичною передумовою реалізації норм ПІВ, а правові відносини ІВ є наслідком реалізації зазначених норм права. А тому, як підкреслює зазначена дослідниця, правовідносини ІВ являють собою правовий результат реалізації норм права, тобто законодавства про ІВ. Вона також дає і наступне визначення цьому концепту як "врегульованих юридичними нормами... ідеологічних суспільних відносин, які

виражаються у взаємних юридичних правах і обов'язках суб'єктів права" [113, с. 87-88].

Щодо кібернетичного простору як наскрізного елементу даного дисертаційного дослідження, то важливо вказати, що на кожному з інфраструктурних рівнів Інтернету (як відповідного втілення кіберпростору), за визначенням М.Б. Касьонової, формуються певні правовідносини, учасниками яких є різні правові суб'єкти, а також відповідні відносини виникають щодо вельми специфічних об'єктів правового регулювання. Отже, правовідносини у Всесвітній мережі - це суспільні відносини, що врегульовані нормами міжнародного та національного права, і які формуються щодо матеріальних й нематеріальних об'єктів-елементів структури побудови, інформаційного наповнення та функціонування Інтернету [90, с. 180-181].

Отже, розуміючи природу як відносин, так і правовідносин інтелектуальної власності, слід дослідити їх структуру. Так, щодо структури правовідносин загалом, то до неї включають наступні елементи:

- об'єкт правовідносин;
- їх суб'єкти;
- їх зміст [8, с. 86].

Деякі ж вчені до цього переліка також включають юридичні факти. І саме останні є підставою виникнення, зміни чи припинення правовідношення [105].

Щодо першого зазначеного елементу, то *об'єктом правовідносин* є все те, з приводу чого вони виникають і розвиваються, а також реалізуються суб'єктивні юридичні права та обов'язки безпосередніх учасників таких відносин. Тобто об'єкт вказує, на що спрямовані відносини та на що спричиняють вплив права та обов'язки суб'єктів. Серед наукової спільноти сформувалося два підходи до розуміння категорії об'єкта правових відносин:

1. *плюралістичний*, зя якого явища навколишнього світу і є об'єктами правовідносин. До них віднесено матеріальні, нематеріальні соціальні блага для задоволенню суб'єктивних потреб та інтересів. Саме щодо таких благ у суб'єктів виникають юридичні зв'язки. Матеріальними благами в даному випадку вважатимуться майно та цінності тощо, а нематеріальними - життя і здоров'я, честь і гідність тощо. Також до об'єктів правовідносин за цього підходу відносять продукти духовної діяльності як от об'єкти ПІВ - твори мистецтва, літератури, комп'ютерні програми й інші результати інтелектуальної діяльності, що захищаються законом, а також цінні папери і документи аналогічного змісту, політичні блага й результати дій учасників правовідносин [97, с. 408]. Деякі науковці сюди включають також послуги виробничого та невиробничого характеру, а саме безпосереднє виконання певних робіт за договором (контрактом) [104];

2. *моністичний*, за якого тільки вчинки суб'єктів слід вважати об'єктом правовідносин, бо тільки люди як їх учасники можуть реагувати на дію права та на безпосередній вплив таких відносин. Це поведінка їх учасників, реальні суспільні відносини. Іноді у правовідносин може бути й матеріальний (спеціальний) об'єкт (предмет), тобто блага , щодо яких вони виникають. Саме цей підхід більшість науковців вважає найбільш обґрунтованим [97, с. 408].

Зазначимо, що людина об'єктом правовідносин не є, вона може стати тільки їх суб'єктом. Важливо також розрізняти об'єкт правовідносин і об'єкт права - під останнім мається на увазі предмет правового регулювання, тобто саме соціальна сфера, на яку вчиняється правовий вплив [105].

Що стосується другого елементу, *суб'єктів*, то ними є учасники правовідносин, що несуть взаємні суб'єктивні права і обов'язки [105].

Суб'єктами, за О. Скакун, є сукупність осіб, що приймають участь у правових відносинах, їх має бути мінімум двоє - правомочний (управлений) і зобов'язаний [5].

Головними критеріями суб'єктів правовідносин є їх правоздатність та дієздатність, а також деліктоздатність - всі вони об'єднані під єдиною властивістю - **правосуб'єктністю**. Нею вважається передбачена нормами права здатність бути учасником правовідносин [8, с. 95].

Кожен із нас, як людина, відповідно до Статті 6 Загальної декларації прав людини, де б не перебувала, наділена правом на визнання своєї правосуб'єктності іншими [33]. Аналогічну норму містить і Стаття 16 Міжнародного пакту про громадянські і політичні права [54].

Правосуб'єктність буває трьох видів:

- *загальна* - можливість людини бути суб'єктом права взагалі - нею наділяється кожен учасник, за виключенням тих, чия правосуб'єктність залежить від незмінних чи необоротних обставин;
- *галузєва* - можливість людини бути суб'єктом певних правових галузей;
- *спеціальна* - можливість людини бути суб'єктом окремої групи суспільних відносин в рамках певної правової галузі [8, с. 96].

При цьому всі суб'єкти як правовідносин наділені першим зазначеним видом, за винятком тих, чий права й обов'язки обмежені обставинами або незмінними (наприклад, стать) або необоротними (наприклад, вік).

Що ж стосується шаблів правосуб'єктності, то, як вже було зазначено, ними є:

- правоздатність - здатність людини як особи мати права і нести обов'язки;
- дієздатність - здатність людини за власним розсудом, самостійно здійснювати свої права і обов'язки;

- деліктоздатність - здатність понести відповідальність, що передбачено законодавством, у разі скоєння правопорушення [18].

В.В. Шуба зазначає, що на правоздатність не мають впливу вікові критерії, фізичний чи психічний стани особи, це її стійкий громадянський стан, адже вона здатна набувати суб'єктивні права і мати їх. Всі громадяни за даним критерієм є рівними, незважаючи на гендерну, расову, національну приналежність, релігійні вірування, матеріальний стан тощо. Тобто правоздатність наділена характеристикою загальності, адже держава одночасно із створенням правових норм як основ публічних правовідносин, надає кожній особі таку загальну рису як юридично закріплену здатність нести відповідні суб'єктивні права та обов'язки [123, с. 117].

На думку даного дослідника, дієздатність загальною бути не може, бо на неї впливає і вік особи, і її фізично-психічний стан, і належність до конкретної галузі права тощо. І якщо правоздатність надається суб'єкту з моменту народження і втрачається з його смертю, то дієздатність в поній мірі настає із повноліттям. Вона, у певних випадках, може бути обмежена за рішенням суду, а також людина може бути абсолютно позбавлена дієздатності, наприклад, через слабоумство чи іншу душевну хворобу, про що має бути відповідне рішення судового органу. Що ж стосується деліктоздатності, то за В.В. Шубою, її обов'язковою передумовою вважається осудність як здатність усвідомлювати свої дії і керувати такими під час скоєння діяння, що є суспільно небезпечним [123, с. 117].

Зазвичай до суб'єктів правовідносин належать як окремі люди, тобто фізичні особи (до них відносяться громадяни конкретної держави, іноземні громадяни, особи з подвійним громадянством чи взагалі без нього), юридичні особи, їх також називають колективними суб'єктами (організації, підприємства, різні установи, органи держави та місцевого самоврядування тощо), а також соціальні спільноти (нація, населення конкретної адміністративно-територіальної одиниці, наприклад, міста [104].

Зміст правовідносин складають безпосередньо суб'єктивні права та юридичні обов'язки вищевказаних суб'єктів. Суб'єктивне юридичне право, як зазначають О.П. та І.О. Віхрови, є встановленою в об'єктивному праві здатністю використовувати різні соціальні блага - це міра допустимої поведінки управненого суб'єкта у конкретних правовідносинах, яку він використовує для задоволення своїх інтересів, і яка забезпечується покладенням обов'язків на інших суб'єктів [8, с. 96].

Істотними елементами таких суб'єктивних прав, на думку науковців, є наступні правомочності:

- правовикористання - право на позитивну поведінку управненого (правомочного) суб'єкта, який, таким чином, наділений можливістю вчиняти фактично та юридичне значущі дії (до таких правомочностей можна віднести право звертатися до суду із позовом за захистом своїх порушених прав, розпоряджатися своїм майном, голосувати тощо). Також правовикористання у науковій літературі ще називають "правомочністю на власні позитивні дії";
- правовиконання - право вимагати певної поведінки від правозобов'язаного суб'єкта, тобто виконання ним покладених обов'язків (прикладом такого слід вважати вимогу сплатити борг, передати речі тощо). Також даний елемент ще називають "правомочність на чужі дії";
- правозахист - право на отримання змоги звернутися за захистом чи підтримкою до своєї держави, якщо правозобов'язаний суб'єкт порушує суб'єктивні права правомочного. У випадку вказаного державою буде застосовано особливий апарат - державний примус, якщо правозобов'язана особа не виконуватиме покладені на неї обов'язки (прикладом подібного буде стягнення заборгованості у примусовому порядку, відновлення незаконно звільненого

працівника на роботі тощо). Інша назва даного елемента - "правомочність домагання" [104].

Видами суб'єктивних прав є:

- громадянські, зазначені у статтях 27, 29-35 нашої Конституції, також їх називають особисті: право на життя, свободу, недоторканість особисту та свого житла, таємність листування та повідомлень, захист приватного життя особи, користування рідною мовою, свободу пересування і совісті, визначення національності тощо;
- соціально-економічні, визначені у статтях 13-14, 41-42 та 43-49 Конституції, тобто такі, що потрібні для забезпечення різних матеріальних та соціально-значущих потреб-інтересів людини. Завдяки їх забезпеченню, держава може вважатися дійсно соціальною, тобто такою, що забезпечує належний рівень життя своїм громадянам;
- культурні, які визначено статтями 53 та 54 Основного Закону: право на освіту, а також "свободу літературної, художньої, наукової і технічної творчості, на результати своєї інтелектуальної, творчої діяльності";
- політичні, зазначені у конституційних статтях 36 та 38-40, які належать тільки громадянину держави, на відміну від особистих прав. Завдяки ним особа приймає участь у політичному житті свого суспільства та в управлінні країною;
- права-гарантії, що визначені статтями 55-57, 59 та 64 Конституції: право на судовий захист та правову допомогу, відшкодування, у разі необхідності, матеріальної та (або) моральної шкоди, заборону обмеження конституційних прав і свобод тощо [105].

На протипагу суб'єктивному праву існує й юридичний обов'язок. Під таким розуміють встановлену необхідність певної поведінки, що забезпечує можливість для іншого суб'єкта скористатися соціальними благами. Інакше

кажучи, це міра належної поведінки, якої має дотримуватися зобов'язана особа у правовідносинах задля задоволення визнаних законом інтересів правомочного суб'єкта; і останній вправі вимагати від першого виконання конкретного обов'язку, інакше до нього буде застосовано державний примус [8, с. 97].

Слід розуміти, що за бажанням особа може не використовувати свої суб'єктивні права, а от юридичний обов'язок вона має виконувати, без можливості відмовитися від такого виконання.

Юридичний обов'язок має наступну структуру у вигляді елементів-зобов'язань:

- дією, адже суб'єкт має вчинити певну дію (дії);
- *необхідною поведінкою*, так як правозобов'язаний не має чинити перешкоди правомочному у користуванні ним благами, щодо яких відповідне право і виникло;
- *виконанням*, бо зобов'язана особа має відреагувати на законні вимоги контрагента;
- *позбавленням*, у разі невиконання чи не сумлінного виконання обов'язків відповідна особа понесе юридичну відповідальність [105].

Цю теорію підтримують й інші дослідники, вважаючи структуру суб'єктивного юридичного обов'язку зворотною стороною суб'єктивного юридичного права, що акумулює такі елементи у вигляді необхідності:

- для особи вчинити або навпаки утриматися від певних дій;
- зобов'язаної особи відреагувати на законні вимоги оппонента;
- понести юридичну відповідальність, а саме зазнати позбавлення певних прав при нехтуванні виконанням юридичних обов'язків [104].

На думку деяких вчених, у юридичного обов'язку є 3 форми:

- певна активність, вчинення дії, тобто активна поведінка;
- утримання від активності, що заборонена, тобто пасивна поведінка;

- встановлення обмежень щодо прав особи майнового, особистого чи організаційного характеру, тобто мають місце заходи юридичної відповідальності [8, с. 98].

Як наголошують дослідники, структура змісту правовідносин формує собою не зв'язок своїх змістовних елементів, а саме правовий зв'язок, що з'являється на їх підґрунті щодо домагання чогось. Тобто має місце особливе юридичне взаємне становище осіб-суб'єктів відносин, і саме таке становище й визначає їхню поведінку через права і обов'язки, які відповідають одне одному, задля задоволення потреб та інтересів таких учасників правовідносин [104].

Суб'єктивне право і корелюючий йому обов'язок разом складають юридичний зв'язок між зобов'язаним та правомочним суб'єктами правовідносин. Так, користування суб'єктивним правом неможливе без виконання відповідного йому обов'язку іншої особи.

Вказані правові зв'язки поділяються на відносні (вони виникають між окремими правовими суб'єктами та абсолютні (ті, що формуються між суб'єктом та суспільством [105]. А сама структура змісту правовідношення буває простою та складною [104].

Як зазначають О.П. та І.О. Віхрови, іноді у правовідношенні окрім вказаного юридичного, також виокремлюють матеріальний, тобто фактичний зміст. Його трактують як відповідне суспільне відношення, позбавлене юридичної форми - фактичну поведінку, яку правомочний суб'єкт може здійснити, а зобов'язаний суб'єкт - має (тобто повинен) виконати. І такі дії реально втілюються в життя учасниками відповідних правовідносин, задля реалізації їх прав та обов'язків. Однак дана наукова позиція, на думку зазначених авторів, не надто отримала схвалення, адже правові відносини як особливий тип суспільних, не ототожнюються з реальною правовою поведінкою учасників, і самі фактичні дії не входять у межі правовідносини, а тому і не є елементом їх змісту [8, с. 96].

Отже, можемо визначити *структуру правовідносин* як симбіоз суб'єктів та доцільного способу зв'язку між ними з основою на суб'єктивних юридичних правах та обов'язках по відношенню до певних соціальних благ чи інтересів. Далі слід розібрати структуру відносин саме щодо дотримання права інтелектуальної власності у кіберпросторі. Отже, виходячи із попереднього визначення, можна говорити, що структура вказаних відносин у кіберпросторі є симбіозом суб'єктів, що вступають у правовідносини з приводу інтелектуальної власності, і доцільного способу зв'язку між ними з основою на суб'єктивних юридичних правах та обов'язках по відношенню до певних соціальних благ чи інтересів у кіберпросторі.

Щодо відносини, які виникають у зв'язку з використанням Інтернету (як одного із втілень кіберпростору), то Г.О. Ульянова, О.І. Харитонova та інші вказують на притаманну їм специфіку, чия суть полягає у суб'єктному складі, об'єктах та змісті відповідних правовідносин. Зазначені відносини щодо використання Інтернету зазвичай характеризується інформаційним наповненням, адже формуються у зв'язку із фактом розміщення у Всесвітній мережі інформації і даних, а ще можуть врегульовуються шляхом застосування методів як приватного, так і публічного права, а також обома ним одночасно. Так як такі інтернет-правовідносини є складною правовою категорією, то і містять в собі традиційно-обов'язкові елементи - суб'єкти, об'єкти й зміст [90, с. 180].

Загалом структура відносин ІВ, які формуються між творцями інтелектуального продукту і суб'єктами господарювання щодо належних їм правомочностей, на думку вчених, складається з відносин:

- користування - адже вони знаходяться у тісному зв'язку із привласненням корисних якостей та результатів використання об'єкту ІВ у різних сферах промисловості та іншої діяльності;

- комерціалізації - бо вони формуються на основі введення об'єкта ІВ у господарський оборот задля його подальшого перетворення у інтелектуальний капітал, а з ним - і отримання доходів;
- розпорядження - адже вони в майбутньому і вирішать долю такого об'єкта, наприклад, щодо передачі прав на нього іншим суб'єктам господарювання на певних умовах;
- володіння - суб'єкт отримує абсолютне панування над об'єктом ІВ, яке не є пов'язаним із його використанням [7, с. 5].

Також деякі дослідники додають до вказаного переліку й відносин привласнення, адже суб'єкт ІВ отримує права власності на об'єкт як результат творчої активності у спосіб, що законодавчо закріплено на рівні держави і санкціоновано суспільством [4, с. 144].

Такі види відносин ІВ можуть по-різному комбінувати у процесі господарської діяльності суб'єктів. І поєднання таких різних за змістом правомочностей роблять інтелектуальну власність універсальним та гнучким явищем, що благодатно сказується на визначенні переліку прав авторів інтелектуальних продуктів.

Щодо видів правовідносин в мережі Інтернет, то є декілька варіантів поділу, що виокремлюються науковцями. Так, залежно від об'єкту регулювання виділяють відносини, які виникають з приводу:

- створення контенту та його використання, а також надання різноманітних інформаційних послуг;
- використання адресного простору сегменту Мережі та розподілу IP-адрес;
- створення та адміністрування доменних імен;
- надання послуг хостингу тощо [90, с. 180-181].

Особливістю відносин в Інтернеті або з його використанням є їх неоднорідність. Так, деякими дослідниками виділено особливий тип правовідносин, пов'язаних із функціонуванням Всесвітньої мережі, до

регулювання яких входять наступні питання: регулювання інформаційного наповнення Інтернет-ресурсів (тобто регулювання контенту), захист конфіденційних та персональних даних, захист прав ІВ, протидія кіберзлочинам; електронна комерція, захист прав споживачів тощо [29, с. 15].

За галузевою приналежністю виділяють цивільно-правові відносини в мережі Інтернет, адміністративні, господарські та інші. За економічним змістом існує розподіл відповідних правовідносин на майнові (щодо матеріальних благ, наприклад, об'єктів фізичної інфраструктури Всесвітньої мережі) та немайнові (щодо нематеріальних благ типу інформаційних прав і свобод, прав ІВ тощо. Також можуть мати місце ускладнені «іноземним елементом» відносини (наприклад, має місце нелегальна публікація контенту на території іншої держави) та неускладнені ним, які не виходять за межі української юрисдикції [90, с. 180-181].

Що ж стосується безпосередньо структури правовідносин інтелектуальної власності, то, як зазначає О. І. Харитонова, вона тотожна відповідній структурі правовідносин загалом, і складається з суб'єктів та об'єкту правовідносин, а також їх змісту, що включає в себе права уповноважених й обов'язки зобов'язаних учасників цих відносин [114, с. 330].

Науковиця підкреслює, під поняттям «суб'єкт права» слід розуміти саме суб'єкта «об'єктивного (позитивного)» права, а тому ними є особи та організації, наділені властивістю правосуб'єктності, що і дає їм змогу приймати участь у правовідносинах. А отже в об'єктивному розумінні, як вказує О. І. Харитонова, суб'єктами ПІВ вважаються ті особи, які абстрактно можуть володіти правами користування та володіння, розпорядження, легітимації та безпосереднього захисту прав на результати творчо-інтелектуальної активності. І тому суб'єктами відповідних

правовідносин інтелектуальної власності (у суб'єктивному розумінні) слід вважати тих осіб, яким вже належать вказані правомочності [114, с. 330-331].

Суб'єктами правовідносин інтелектуальної власності, за Статтею 421 ЦКУ, є творці об'єктів ПІВ та інші особи, яким за законом належать особисті майнові та/чи немайнові права ІВ. Зазначена норма Кодексу не містить обмежень щодо тих осіб, які можуть створювати об'єкти інтелектуальної власності, а також щодо їх віку, стану здоров'я, чи навіть дієздатності [116]. А, отже, можна зробити висновок про можливість стати творцем для будь-кого, в тому числі ним може бути й особа неповнолітня, а також повністю недієздатна, або така, що наділена частковою або обмеженою дієздатністю. Але у процесі здійснення своїх прав ІВ на розпорядження об'єктом тощо такий творець потребуватиме допомоги інших осіб, як от піклувальників, батьків тощо, тобто тих, на кого законом покладене відповідне зобов'язання про піклування.

Зазначеними у Статті 421 ЦКУ іншими особами як суб'єктами ПІВ, яким належать права інтелектуальної власності, зазвичай є правонаступники, спадкоємці, роботодавці, інвестори тощо. Відповідно, тут уже мова не йде безпосередньо про творця, тобто того, хто своєю творчо-інтелектуальною працею створив об'єкт ІВ, а тому вказаними особами можуть бути як фізичні, так і юридичні. Права відповідних суб'єктів щодо об'єктів ІВ виникають на основі діючих нормативно-правових актів, договорів, в тому числі трудових.

Специфіка правовідносин у кібернетичному просторі, і безпосередньо в Інтернеті розкривається через факт того, що для уповноважених суб'єктів виникають права, тобто у них з'являються можливість вчиняти певні дії у віртуальному кіберпросторі (така можливість надання їм міжнародними договорами, судовими рішеннями, правовими нормами та забезпечується різними державами). Також разом з

вказаними правами суб'єкти отримують і обов'язки, відповідно до яких поведінка учасників відносин має відповідати передбаченій джерелами інтернет-права і забезпечуватися доброю волею цих суб'єктів або державним примусом [90, с. 181].

Досліджуючи питання суб'єктів правовідносин ІВ також варто вказати на певні властивості таких відносин, а саме:

1) *загальні:*

- a) їх суб'єкти є юридично рівними;
- b) регулювання суспільних відносин здійснюється переважно нормами цивільного законодавства;
- c) учасники відповідних цивільних відносин наділяються цивільними правами та обов'язками;

2) *специфічні:*

- a) відповідні відносини виникають на особливій підставі - створення об'єкту, що має охоронятися правовими нормами НПА по інтелектуальній власності;
- b) можливе поєднання у правових відносинах речових та зобов'язальних елементів;
- c) визначення прав та обов'язків суб'єктів таких відносин здійснюється на основі поєднання імперативного та диспозитивного елементів;
- d) даним правовим взаєминам притаманний цільовий характер, що проявляється у забезпеченні використання відповідних об'єктів та їх охорони [113, с. 88].

Як вже зазначалося вище, суб'єкти відносин ІВ можуть вступати у них на основі трудового договору. Так, згідно Статті 429 ЦКУ, особисті немайнові права ІВ на об'єкти, що були створені у зв'язку із виконанням трудового договору, належать працівникові-творцю такого результату творчо-інтелектуальної активності. А саме майнові права на вказаний об'єкт

будуть належати спільно (якщо інше не передбачено законодавством чи договором) авторові, і роботодавцю. Останнім може бути як фізична, так і юридична особа. Окремо слід вказати на ч. 2 Статті 1107, згідно якої договір щодо розпоряджання майновими правами ІВ має бути укладено у письмовій формі. Якщо ж відповідна форма не буде дотримана, то і договір вважатиметься нікчемним [116].

Деякі особливості має відповідна норма ЗУ Про авторське право і суміжні права. Так, Стаття 14 у п.2 вказує на перехід майнових прав на службовий твір до роботодавця з моменту створення відповідного твору повністю (якщо інше не передбачено відповідними НПА, контрактом чи договором). Але при переході таких прав працівник-творець має право на винагороду [167]. Отже, Стаття 429 ЦК є більш лояльною саме до прав працівника-автора результату творчо-інтелектуальної діяльності.

Варто звернути увагу і на норму Статті 430, що стосується об'єктів ІВ, створених на замовлення. Так, особисті немайнові права, як заведено, належать у такому випадку творцю результату творчо-інноваційної діяльності, хоча окремі з них і можуть (за законом) належати замовникові. Щодо майнових прав, то, як і у випадку із службовим твором, їми спільно володіють автор результату та замовник, якщо інше не передбачене діючими НПА чи договором між суб'єктами [116].

Стаття 15 Закону про Авторське право також вказує на належність немайнових прав саме авторові, без будь-яких вказівок на можливість передачі окремих з них. Майнові ж переходять на користь замовника, якщо про інше не було домовлено у відповідному договорі замовлення, а творець може претендувати на винагороду. Але є тут окреме зауваження щодо відповідних правомочностей на результат творчої діяльності в образотворчому мистецтві. Так, якщо він не був розроблений спеціально як елемент комп'ютерної програми, то і матеріальні права на нього належать творцю за відсутності інших домовленостей у договорі чи вказівок у

законодавстві. У замовника, якщо інше не передбачено, є право вносити зміни до об'єкту, створеного за замовленням [67].

О.І. Харитонова окремо звертає увагу на цей нюанс, що при так званій «трудовій функції» завдання на створення об'єкта може стосуватися лише об'єктів авторського права і споріднених з ними, наприклад, промислових зразків. Що ж стосується винаходів та корисних моделей, то такі відповідна особа створює саме у процесі виконання службового завдання, виданого роботодавцем, а не за його безпосереднім завданням. Справа в тому, що сам термін «службове завдання» передбачає виконання завдання, що покладено на працівника в межах його трудової функції. А сам творчий результат, який автор отримує, виконують відповідні функції (без окремого завдання від керівництва) не має, зазвичай, статусу службового результату. Винятки з вказаного можуть бути передбачені відповідним трудовим договором із виконавцем на здійснення творчих видів діяльності [114, с. 332].

Окремо відзначимо, що суб'єктний склад відносин щодо використання Інтернету має певні особливості. Справа в тому, що юзер заходить в кіберпростір завдяки діяльності самотійної особи-надавача відповідних послуг — провайдера. Також є нюанс і з доменними іменами, адже їх реєструють самотійні треті особи — реєстратори, при цьому такою самотійною особою виступає і власник веб-адреси, при цьому він може і не бути власником відповідного електронного ресурсу [90, с. 181].

Отже, підсумовуючи вищенаведене, до суб'єктів відносин ІВ можна віднести безпосередньо самих творців, власників прав інтелектуальної власності, правонаступників та інших осіб, чия діяльність пов'язана із використанням, захистом результатів творчо-інноваційної діяльності. Відповідно і суб'єктами відносин у кіберпросторі будуть ті ж самі особи, а також ті, хто вступає у такі відносини в процесі діяльності у кібернетичному

просторі та безпосередньо Інтернеті - провайдери, оператори зв'язу, реєстратори, інтернет-реєстри тощо.

Окремо слід вказати на суб'єктну структуру ІВ у запропонованій В. В. Вірченком та іншими архітектоніці інтелектуальної власності. Так, до неї включають:

- творців інтелектуального продукту, тобто тих фізичних осіб, які безпосередньо приймають участь у його створенні в процесі своєї літературно-мистецької чи науково-технічної активності. Відповідно до вказаної групи суб'єктів відносять авторів творів, винахідників, авторів промислових зразків тощо;
- первинних правонабувачів, які отримують відповідні права ІВ у результаті їх реєстрації або за нормами діючого законодавства. До таких належать виробники фоно- та відеограм й організації мовлення, а також власники прав на засоби індивідуалізації учасників у цивільному обороті та на комерційну таємницю;
- роботодавців, адже ті отримують майнові права на результати творчої-інноваційної діяльності, що були створені їх працівниками у порядку виконання службових обов'язків. Серед таких осіб ті, кому належать майнові права на службові твори, об'єкти патентного права, компонування мікросхем;
- правонаступників, які набули майнові права у зв'язку з їх переходом від попереднього власника відповідних прав на певних підставах. Таким правонаступником можна стати за законом, договором чи заповітом;
- посередників і довірених осіб, тобто тих суб'єктів, які ведуть діяльність із надання іншим суб'єктам інтелектуальної власності різних послуг консультативного, оціночного, право-трансферного, фідучіарного характеру тощо. До даного кола осіб належать патентні

повірені, ОКУП (тобто організації колективного управління правами), оцінювачі, спеціалісти з трансферу технологій;

- регуляторів, які, відповідно до закону, здійснюють повноваження у сфері регулювання відносин ІВ та охорони прав їх учасників. Це різні держоргани, держустанови й організації [7, с. 5, 8].

Щодо правовідносин в мережі Інтернет, то, залежно від суб'єктного складу, вирізняють ті, які виникають між:

- юзерами, тобто користувачами;
- провайдером, тобто постачальником мережевих послуг і інтернет-юзерами;
- провайдерами та уповноваженими державними органами [90, с. 181].

Як відомо, суб'єкти ІВ вступають у відповідні відносини з приводу певного *об'єкту*. Як зазначає О.І. Харитонова, об'єкти цивільних прав і об'єкти цивільних правовідносин є тотожними поняттями, і в контексті такого відповідними об'єктами є матеріальні або нематеріальні блага, щодо яких і склалися цивільні правовідносини. А тому, такими благами з точки зору цивільних правовідносин ІВ будуть вважатися результати інтелектуально-творчої діяльності, яким за діючим законодавством має бути надана охорона [114, с. 333].

Розглянемо далі відповідні переліки об'єктів вказаних відносин у нормативно-правових джерелах. Так, за п. VIII Статті 2 Конвенції про заснування ВОІВ (також - Стокгольмська конвенція) права ІВ розповсюджуються на такі об'єкти як: літературні, художні і наукові твори; промислові зразки, наукові відкриття, винаходи, виконання артистів, звукозаписи, теле- і радіопередачі, ТЗ, знаки обслуговування, комерційні позначення та фірмові найменування, а також захист від недобросовісної конкуренції. Також вказане стосується й інших прав щодо інтелектуальної діяльності у художній, літературній, виробничій й науковій галузях [42].

Відмітимо, що вказівки, подібної останній зазначеній, в українському законодавстві немає.

Тим не менш, зазначимо, що ні в міжнародному праві, ні в національному не передбачено норм щодо чітких критеріїв класифікації об'єктів відносин ІВ. Якщо поглянути у наші НПА, то побачимо, що вони надають лише безпосередньо перелік таких об'єктів (згадаємо статті 420 ЦКУ, 8 ЗУ про авторське право і суміжні права тощо). Аналогічно і Стаття 2 Конвенції про заснування ВОІВ 1967 року містить саме перелік об'єктів ІВ, а не критерії їх класифікації як таких [10].

Так, перелік об'єктів ІВ за нашим вітчизняним законодавством міститься у Статті 420 ЦКУ. Сюди, як вже зазначалося у минулих розділах дисертаційного дослідження, віднесені літературні й художні твори, фоно- й відеограми, виконання артистів, програми організацій мовлення, об'єкти патентного права, комп'ютерні програми та бази даних, наукові відкриття, компонування напівпровідникових виробів, раціоналізаторські пропозиції, сорти рослин й породи тварин; а також засоби індивідуалізації учасників у цивільному обороті як то фірмові найменування, ТМ, й географічні зазначення, а також комерційні таємниці [116].

З відповідним переліком погоджуються й вчені. Так, наприклад, В. Вірченко та інші в контексті архітекtonіки ІВ до об'єктної структури відносять безпосередньо вже зазначені об'єкти, групуючи їх наступним чином: об'єкти авторського права; суміжних прав; патентного права; засоби індивідуалізації та нетрадиційні об'єкти [7, с. 5].

Як вже було зазначено, критеріїв поділу об'єктів правовідносин ІВ немає, а тому з'явилося різноманіття підходів щодо такого їх структурування. Так, в роботі П.П. Крайнева простежується розділення об'єктів ІВ на об'єкти авторського і суміжних прав, промислової власності, комерційні таємниці і захист від недобросовісної конкуренції [49, с. 25]. В.Д. Базилевич окрім об'єктів АП і суміжних прав виділяє об'єкти

промислової власності, засоби індивідуалізації і нетрадиційні об'єкти ІВ [4, с. 155].

За К.В. Єфремовою, основними об'єктами, щодо яких формуються інформаційні відносини в інтернет-мережі, є, крім іншого, сама інформація, інформаційні системи й інформаційно-телекомунікаційні технології, інформаційні ресурси і продукти, доменні імена тощо [30, с.8]. Ознайомившись із вказаним переліком, розуміємо, що більшість названих об'єктів можуть бути віднесені до відання ППВ.

В.В. Вірченко та інші взяли за основу останній зазначений підхід і дещо удосконалили його з урахуванням сьогодення і тенденцій щодо розвитку економічних відносин у сфері привласнення результатів ІВ. Це дало змогу взяти до уваги найбільш значущі ознаки відповідних об'єктів, як от зміст і структуру прав ІВ на результати відповідної діяльності; особливості охорони та реалізації суб'єктивних прав на них, а також умови набуття і закінчення прав ІВ. Так, вказані дослідники виділяють чотири основні групи відповідних об'єктів, а саме: об'єкти АП, об'єкти суміжних прав, об'єкти промислової власності, яка включає в себе дві підгрупи - об'єкти патентного права і засоби індивідуалізації, й нетрадиційні об'єкти, розподілені додатково на інкорпоральні та уречевлені. Даному підходу притаманні три наступні особливості:

- нетипове розділення об'єктів авторського права і суміжних прав на дві окремі групи через значні відмінності в умовах набуття та механізмі реалізації прав власності на них. при цьому вони мають і спільні риси, як от вимоги щодо матеріального втілення результату творчої діяльності, умов охороноздатності щодо оригінальності і наявності творчості, а також надання охорони незалежно від змісту та художньої цінності результатів;
- розподіл об'єктів промислової власності на об'єкти патентного права та засоби індивідуалізації, які мають різне функціональне

призначення, але при цьому реалізувати виключні майнові права на них можна тільки у сфері господарського обороту;

- розділення нетрадиційних об'єктів ІВ на інкорпоральні та уречевлені, що робиться з урахуванням їх форми вираження і особливостей набуття (припинення) прав на них. В цю групу віднесені наукові відкриття, комерційні таємниці та ноу-хау, раціоналізаторські пропозиції (інкорпоральні), а також компонування інтегральних мікросхем й сорти рослин і породи тварин (уречевлені). Останні дещо схожі із об'єктами патентного права щодо особливостей свого створення, реалізації, структури виключних прав. Інкорпоральні ж об'єкти мають унікальні особливості й становлять знання у чистому вигляді без необхідності набуття уречевленої форми [7, с. 6].

Тим не менш, для досягнення мети даного дисертаційного дослідження авторка вважає найбільш вдалим підхід до групування об'єктів відносно ІВ, наданий В.В. Вірченком та іншими, а перелік відповідних об'єктів - зазначені у статті 420 ЦКУ. Також окремо слід вказати на те, що даний перелік не є виключним, що видно із слів зазначеної норми “До об'єктів права інтелектуальної власності, **зокрема**, належать...” [116]. Тобто саме слово “зокрема” вказує на невиключність даного списку, що й зрозуміло, адже творчо-інноваційна діяльність людини знаходиться у постійному русі, а з тим і з'являються нові об'єкти ПІВ.

Останнім елементом в структурі правовідносин інтелектуальної власності є *зміст*.

Сучасному українському праву, як зазначає О.І. Харитонova, притаманне розуміння ПІВ щодо особи у двох розуміннях: як елементу правосуб'єктності та як суб'єктивного права. Вона вказує на те, що право фізичної особи визнаватися творцем відповідного об'єкта є елементом її правосуб'єктності. В даному випадку мова не про юридичне право, а саме про абстрактну можливість набувати такого права. При цьому

правомочність на перешкоджання посягання на відповідні права, яке здатне нанести шкоду честі або репутації автора об'єкта ПІВ, а також інші особисті немайнові права є суб'єктивними цивільними правами, адже, як зазначає науковиця, вони виникають відносно конкретних об'єктів й між конкретними суб'єктами. А, отже, вказані права є елементом змісту правовідносин ІВ [15, с. 89-90].

Відповідно до Статті 422 Цивільного кодексу, право ІВ виникає з підстав, встановлених даним Кодексом, іншими законодавчими актами або договором. Статті 423-424 поділяють права суб'єктів ІВ на особисті немайнові та майнові. Так, до немайнових віднесено права на визнання фізичної особи творцем об'єкта ПІВ, на перешкоджання посягання на ПІВ, яке може нанести шкоду честі чи репутації такого творця та інші особисті немайнові права ІВ за законодавством. І вказані права є невідчужуваними, а також не залежать від майнових прав суб'єктів ІВ. Права на використання об'єкта, на надання дозволу використовувати такі об'єкти, на перешкоджання неправомірному їх використанню - це права майнового характеру [116].

Щодо немайнових прав ІВ в контексті використання кіберсередовища та пов'язаних із тим труднощів, деякі дослідники наголошують на необхідності відмовитись від концепції відповідних прав щодо розміщених у Мережі результатів творчо-інтелектуальної діяльності. Але б тоді твори в Інтернеті розповсюджувались без урахування авторства, що нині є протиправним діянням [90, с. 190-191].

За Статтею 440 ЦКУ, окрім вже зазначених вище майнових прав (використовувати, дозволяти (забороняти) використання творів також додані "інші майнові права інтелектуальної власності, встановлені законом". Також зазначається, що відповідні права належать автору, якщо інше не було передбачено у договорі чи законодавством. Але такі права на об'єкт, що створено в рамках виконання трудового договору або контракту

мають передаватися роботодавцю такого працівника (може бути як фізично, так і юридичною особою), а на результат, створений за замовленням - замовникові з моменту створення у повномуобсязі [116].

Стаття 15 ЗУ про авторське право до виключних майнових прав творця відносить вже зазначені у ЦК України право використання, дозволу (заборони) використання та вказує на можливість передачі таких прав іншим особам. При цьому виключне право на використання дозволяє відповідній особі користуватися об'єктів ПІВ у будь-якій формі чи будь-яким способом. Ч.3 зазначеної статті вказує на варіанти використання твору у межах включних майнових прав, їми є: відтворення твору (тобто створення копій такого) з можливістю подальшого імпорту відповідних примірників, його публічне виконання чи сповіщення, а також демонстрація і показ, як і доведення до загального публічного відома у такий спосіб, що відповідна публіка зможе отримати доступ до твору з будь-якого місця і у бажаний час. Також до вказаних правомочностей віднесено повторне оприлюднення творчого об'єкту іншою організацією, його переробка, переклад, адаптація чи подібні модифікації, включення такого результату творчо-інноваційної діяльності як складової частини до збірників, антологій і подібних об'єктів, а також розповсюдження творів шляхом першого продажу, або відчуження іншим способом, здавання в майновий найм і (або) комерційний прокат після першого продажу тощо. Як завжди відповідний перелік не є вичерпним [67].

Як зазначають дослідники, змісту відносин щодо інтелектуальної власності в мережі Інтернет також притаманні певні особливості. По-перше, це структура суб'єктивного юридичного права і суб'єктивного юридичного обов'язку. Так, структура першого виражається у зв'язку юридичних можливостей тобто правомочностей, якими наділений суб'єкт відносини, як її елементів. Істотними складовими суб'єктивного права є правовикористання, правовиконання та правозахист. Відповідно, у

віртуальному просторі суб'єктивне право проявляється у вигляді права-користування, -вимоги, -поведінки, -претензії [90, с. 182].

По-друге, суб'єктивні права учасників правовідносини у кіберпросторі взагалі, та у Інтернеті безпосередньо розкриваються саме через власні дії юзерів, адже вони провокують виникнення, зміну та навіть припинення прав і обов'язків інших учасників взаємодії у Мережі, а не просто через обов'язки третіх осіб [28, с. 14].

Структура суб'єктивного юридичного обов'язку включає в себе три складові:

- активний (зобов'язаний учасник має вчинити певну дію) та пасивний обов'язок (утримання від дії);
- обов'язок зобов'язаного відреагувати на законні вимоги правомочного;
- обов'язок понести юридичну відповідальність у разі небажання або несумлінного виконання, чи невиконання юридичного обов'язку.

Вказані суб'єктивні права і обов'язки взаємозалежні одне від одного. Саме через них і виникають правовідносини як зв'язок між суб'єктами, що одночасно виступають носіями таких прав й обов'язків [90, с. 182].

Отже, *суб'єктивне право в Інтернеті та у кіберпросторі загалом - це гарантовані правовими нормами вид та об'єм можливої або дозволеної поведінки учасників таких відносин, а обов'язок - це вид або міра вказаної поведінки (належної чи необхідної)* [90, с. 183].

Слід підкреслити, що, як зазначають О.І. Харитонова, Г.О. Ульянова та інші в контексті кіберправовідносин ІВ (у розрізі Інтернету), додаткових елементів, окрім об'єктів, суб'єктів та змісту у даних специфічних відносин немає. Так, є спроби додати до вказаної структури також інформацію та технічні засоби як її елементи, але зазначене, як вказують дослідники, є саме об'єктом даного правовідношення [90, с. 180].

Отже, структура відносин щодо дотримання права інтелектуальної власності у кіберпросторі включає в себе традиційні для будь-яких правовідносин елементи - суб'єкти, об'єкти та зміст. При цьому не кожен результат творчої діяльності вважається об'єктом ПІВ, а лише такий, що відповідає вимогам законодавства. І якщо до об'єктів суміжних прав та авторського права вимоги є досить простими, як от наявність творчості, відсутність плагіату, вираження у матеріальній формі тощо, то для науково-технічних результатів, щоб вони отримали відповідний захист, необхідно попередньо пройти кваліфікацію в державному органі, після чого на відповідний об'єкт буде видано правоохоронний документ. Але, як вже було зазначено, ні в міжнародному праві, ані в національному не передбачено конкретні норми щодо чітких критеріїв класифікації об'єктів відносин інтелектуальної власності.

Щодо суб'єктів відповідних відносин, то окрім традиційних для ПІВ творців, правонаступників, роботодавців тощо у випадку із кіберпростором сюди слід включати тих осіб, що вступають у відносини в процесі оперування у кібернетичному просторі, наприклад, провайдерів, операторів зв'язку, реєстраторів тощо. Зміст таких правовідносин, елементом якого є суб'єктивні права та суб'єктивні юридичні обов'язки, також має особливості. Так, суб'єктивні права учасників правових відносин у кіберпросторі розкриваються через власні дії користувачів такого середовища, а не через обов'язки третіх осіб, бо вони є каталізатором виникнення, зміни, припинення прав і обов'язків інших користувачів кібердомену.

Кіберпростір сьогодні - це середовище, в якому щодня з'являються нові об'єкти права інтелектуальної власності, і їх правовий режим потребує відповідного регулювання, яке не завжди розробляється вчасно, з урахуванням постійної динаміки кібердомену. Суб'єкти, об'єкти та зміст відповідних правовідносин мають певну специфіку, а тому потребують

якісного дослідження уже сьогодні. Адже кількість правопорушень прав ІВ у Всесвітній мережі росте щодня.

Визначення і правова кваліфікація досліджуваних елементів структури відносин щодо дотримання права інтелектуальної власності у кіберпросторі, на нашу думку, допоможе проаналізувати наявне законодавство та віднайти у ньому "слабкі" місця, і на їх основі - визначити тенденції подальшого удосконалення відповідних НПА, розробки нових, а також шляхи розвитку у відповідній галузі. Зауважимо, що питання виявлення суб'єктів правопорушення щодо ІВ у кіберпросторі наразі стоїть досить гостро, адже діюче законодавство не дає чіткого розуміння щодо визначення відповідних осіб.

3.2. Генеза правового регулювання функціонування окремих інститутів інтелектуальної власності у кіберпросторі

Сьогодні поліпшення вже існуючого або розробка нового досконалішого правового регулювання функціонування інститутів інтелектуальної власності взагалі та безпосередньо у кіберпросторі вбачається практично неможливим без попереднього вивчення його генези. Відповідно до визначення, наданого словником української мови, *генеза* (або *генезис*) - це походження, виникнення, становлення [100]. Отже, даний підрозділ дисертації буде присвячено дослідженню особливостей виникнення та становлення правового регулювання функціонування окремих інститутів інтелектуальної власності у цифровому середовищі - кібернетичному домені.

Як вже було зазначено у Розділі 1.1. даного дисертаційного дослідження, свої витоки правове регулювання інтелектуальної власності загалом бере ще у 1624 р. із появою Статуту про монополії, за яким послідував Британський статут Анни (1710 р.). Ці два правові акти започаткували регулювання відносин щодо патентного та авторського

права, а разом з тим - і укорінення концепції інтелектуальної власності. Далі було декілька відповідних подій, серед яких надання королівських грантів Єлизавети I на монополні привілеї у 1558–1603 рр. тощо. Наступними знаковими роками стали 1883 і 1886, що відзначилися появою Паризької конвенції з охорони промислової власності та Бернської конвенції про охорону літературних та художніх творів відповідно. Із заснуванням у 1967 р. ВОІВ інтелектуальна власність як соціальна і правова категорія отримує загальнозживане розуміння та переходить у глобальний режим.

Точно сказати, коли з'явився кіберпростір, не вбачається нам можливим. Тим не менш, про появу Інтернету як його невіддільного елементу, є відповідні згадки. Так, у 1950 рр. вже існували локальні мережі, а також зароджуються перші концепції мережі глобальної. І такі глобальні мережі зі складною структурою і основою на кількох локальних мережах з'являються вже у 60-і роки ХХ століття. У 1967 р. Д. Девіс показав світу інноваційну модель пакетної комутації, що стала основою проекту ARPANET, який і став прообразом того, що зараз ми називаємо Всесвітньою мережею Інтернет [37].

У 70-і роки також створюються інші мережі пакетної комутації, як от NPL и Telenet, Cyclades, Tymnet тощо. Тоді ж Вінтон Ґрей Серф (нині відомий як "батько Інтернета" - прим. автора) разо з Робертом Елліотом Каном створюють стек протоколів TCP/IP на базі ARPANET та Cyclades. У наступну декаду, з ініціативи NSF, впроваджуються перші обчислювальні центри в американських закладах вищої освіти, а вже у 1986 р. їх об'єднали в масштабну мережу NSFNET, після чого почали з'являтися й перші інтернет-провайдери. Тобто в цей період і з'явилася зрозуміла нам глобальна мережа (на основі розробок Т. Бернеса-Лі, який об'єднав велику кількість гіпертекстових документів у єдину систему, підключення до якої вже було можливе з будь-якого комп'ютеру, підключеного до загальної мережі. У 1990 проект ARPANET було закрито, що спровокувало появу у

США окремих приватних фірм-надавачів підключення до Інтернет-мережі. За 5 років було закрито NSFNET, що й дало початок становленню Інтернету як включно комерційного феномену. В свою чергу таке дало змогу пересічним людям стат юзерами, тобто користувачами Мережі [37]. З тих пір Інтернет знаходиться у постійному розвитку.

З урахуванням подій останньої декади ХХ століття стає зрозумілим, чому у грудні 1996 р. була скликана Дипломатична конференція, в рамках якої прийнято так звані "інтернет-договори ВОІВ" з авторського права та з виконань та фонограм. Вони, хоча й не надто конкретно врегулювали відповідні відносини, але стали відправною точкою у формуванні нормативно-правового масиву саме з питань ІВ у кібернетичному домені.

Як зазначив Л. Гао, інтернет-договори ВОІВ містили чотири основоположні принципи, а саме:

1. авторам, виконавцям та виробникам фоно- та відеозапису надано право створювати та зберігати свої твори у цифровій ("діджитал") формі, приблизно у той же спосіб як вони роблять відтворення традиційних творів;
2. зазначені суб'єкти можуть поширювати цифрові творчо-інтелектуальні об'єкти серед громадськості у спосіб, такі твори були легко доступні в Інтернет-мережі;
3. легкість копіювання оцифрованого об'єкту вимагає забезпечення дієвих засобів правового захисту проти обходу наявних технологічних заходів;
4. необхідно також забезпечити захист управлінської інформації у електронній формі [188, с. 590-591].

Вказані принципи та загалом норми інтернет-договорів ВОІВ стали для їх підписантів основою для розробки національних НПА у сфері захисту ІВ у цифровому середовищі. І одним із таких став прийнятий Сенатом США 14 травня 1998 р. Закон про авторське право в цифрову (англ. *Digital*

Millennium Copyright Act, DMCA). Окрема увага вказаному документу буде присвячена у Розділі 4.1. даного дисертаційного дослідження. Але роль його в контексті генези правового регулювання ІВ у цифровому просторі значна, тому зазначимо, що Сполучені Штати прийняли його з метою імплементації інтернет-договорів ВОІВ. Даний акт враховує у своїх положеннях особливості сучасних технологій щодо копіювання та розповсюдження цифрової інформації, в т.ч. інтернет-контенту, й передбачає суворі заходи покарання у разі порушення АП в Інтернеті. Його три основні оновлення у сфері захисту АП:

1. постачальникам онлайн-послуг в деяких ситуаціях буде надано особливий захист, у разі коли їх юзери порушують АП, в т.ч. і через створення системи повідомлень і запису (англ. notice-and-takedown system), через яку власники відповідних прав можуть інформувати постачальників онлайн-послуг про нелегальний матеріал;
2. власники авторських прав заохочуються до надання ширшого доступу до своїх творів у цифрових форматах із надання їм правового захисту від несанкціонованого доступу до таких об'єктів, наприклад, у вигляді обходу шифрування;
3. заборонено надавати неправдиві дані щодо керування авторськими правами, наприклад, імена творців тощо [156].

Закон про авторське право Китаю також інкорпорував три з вищезазначених принципів Інтернет-договорів ВОІВ. Щодо четвертого принципу про право правовласників оцифровувати об'єкти АП, він, хоча й не був втілений прямо, однак отримав своє де-факто застосування завдяки тлумаченню Верховного народного суду Китаю щодо авторського права в Інтернеті (2001 р.) [188, с. 591-592].

Окремо вкажемо на генезу правового регулювання функціонування інститутів ІВ в Євросоюзі. Так, як зазначає Р.Є. Еннан, в ЄС розвиток ПІВ був затяжним та складним через його територіальну приналежність, яка і

перешкоджала створення єдиного в Союзі. Країни-члени по-своєму регулювали відповідні відносини, що входили до виключної компетенції держав, а співпраця у відповідній сфері не вважалася пріоритетним завданням Євросоюзу (тому і відповідних НПА було недостатньо). Але зрештою проблема кореляції між здійсненням прав ІВ та слідуванням принципам свободи руху товарів і конкурентної політики у Союзі стали предметом кейсів Суду ЄС. Наступною фазою розвитку правового регулювання у зазначеному полі стають поступова гармонізація та уніфікація законодавства країн-членів з окремих питань ІВ [27, с. 8].

Щодо авторського права та суміжних прав, як зазначає Р.С. Еннан, зближенню правових систем країн-членів допомагал в більшості своїй директиви, в той час як щодо промислової власності - регламенти, бо регулювання стосується саме наднаціонального рівня. Окремо вказано на те, що незважаючи на виконання вимог Угоди ТРІПС, у держав-членів Союзу засоби охорони та захисту прав ІВ все одно мають відмінності, а це, в свою чергу, шкодить нормальному функціонуванню внутрішнього ринку та перешкоджає гарантуванню рівноцінного захисту та охорони відповідним правом на наднаціональному рівні. Тому у 2004 році і була прийнята Директива 2004/48/ЄС про забезпечення дотримання прав інтелектуальної власності, що дало початок розробці горизонтальних інструментів боротьби із піратством [27, с. 9-10]. Більш детально дану Директиву буде досліджено у Розділі 4.1., зазначимо лише те, що вона містить відповідні положення щодо процедур та засобів, які допоможуть гарантувати дотримання прав ІВ.

Діяльність європейських органів з уніфікації стосувалася, в більшості своїй, запровадження єдиних правил щодо реалізації майнових авторських прав, в тому числі права на відтворення, сповіщення, розповсюдження, слідування, переробку тощо. Звернемо увагу і на проголошену можливість визнання в Євросоюзі у якості первинного суб'єкта авторського права на

твір не тільки того, хто його безпосередньо створив, але й інвесторавиробника. На думку Р.С. Еннана, прагнення до уніфікації в царині норм АП та результати такої діяльності було проаналізовано відповідними органами з точки зору економічної вигоди, що може призвести до порушення балансу між інтересами людей як суспільства та авторів на користь підприємців-інвесторів [27, с. 11].

В контексті загальносвітової генези регулювання функціонування окремих інститутів інтелектуальної власності у кіберпросторі згадаємо і про раніше згаданий Порядок денний з Розвитку ВОІВ 2007 р., що містив 45 рекомендацій з адаптації активності органу до конкретних наявних потреб країн, що розвиваються. Окрім іншого, ці рекомендації стосувалися й поліпшення ситуації щодо доступу інтернет-користувачів до інформації, ІТ-спеціалістів - до вихідних кодів, а тих, хто навчається - до відповідних наукових матеріалів. Але конкретних міжнародно-правових реформ у відповідному полі на цей час ще не було введено.

Паралельно із вказаним відбувалося й розбудування європейської регіональної патентної системи та розробка і введення в дію стандартів охорони винаходів в Євросоюзі. В рамках регіональної економічної інтеграції почалося введення європейських інституційних механізмів по оформленню патентних прав. Уніфікація та гармонізація в даному напрямку результували у появу Директиви про правову охорону біотехнологічних винаходів та Регламенту про запровадження додаткового охоронного сертифіката щодо медичних продуктів. Щодо корисних моделей, то в Євросоюзі велася активна розробка пропозицій по заснуванню єдиної системи охорони таких об'єктів, котра передбачала, в тому числі, подання єдиної заявки, яка б забезпечила охорону на всій союзній території. Щодо промислових зразків, то гармонізація результувала і ухвалення Директиви 98/71/ЄЕС про правову охорону промислових зразків і Регламенту про промислові зразки ЄС. На початку нового століття,

у 2002 р. Єврокомісія також внесла проект Директиви про патентоспроможність винаходів, пов'язаних із комп'ютером, але його розгляд було припинено [27, с. 12].

В контексті авторського права та діджитал/кібернетичного простору важливо вказати на єдину систему охорони комп'ютерних програм й баз даних в ЄС. Так, кожен член має щодо таких об'єктів свої НПА, на які розповсюджуються загальні положення національного АП. Тим не менш, з метою гарантувати ефективний рівень охорони прав розробників програм для ЕОМ від несанкціонованого їх копіювання було введено в дію Директиву 91/250/ЄЕС про правову охорону комп'ютерних програм, а також Директиву 96/9/ЄС [27, с. 11].

Щодо суміжних прав, приблизно в той же час, гармонізація законодавства ЄС ознаменувалася введенням в національне законодавство членів захисту науково-критичних публікацій творів, та тих творів, що раніше не публікувалися або стали суспільним надбанням тощо. Важливим є те, що технічні засоби для ідентифікації об'єктів суміжних прав, які розповсюджуються цифровим способом отримав юридичне визнання. Все це та багато іншого ввійшло у новостворену Директиву 2006/115/ЄС про право на надання в прокат і право на надання в позичку та про деякі суміжні права у сфері інтелектуальної власності (від 12 грудня 2006 року) [27, с. 12].

Задля подолань перешкод у вільному русі товарів і послуг та недопущення негативного впливу на конкуренцію на спільному ринку в Євросоюзі було проведено роботу щодо подолання розбіжностей у національному законодавстві щодо торговельних марок. Так, ключовим задумом на рівні даного об'єднання стало запровадження торговельної марки Європейського союзу, що означало єдину реєстрацію ТЗ, що діяли б на всій його території. Так з'явився на світ Регламент 207/2009 щодо ТМ ЄС, відповідно до якого мало бути створене Відомство із гармонізації на

внутрішньому ринку. За рік до того була розроблена Директива 2008/95/ЄС щодо наближення законодавства країн-членів ЄС відносно торговельних марок [27, с. 3]. Відповідний документ також буде розглянутий у Розділі 4.1. даного дисертаційного дослідження, адже він містить не тільки визначення та ознаки ТМ, але й «абсолютні» підстави відмови у її реєстрації тощо.

Повертаючись до галузі саме цифрового (кібер-) простору, зазначимо, що окрім прийняття Бернської конвенції та "інтернет-договорів" ВОІВ, важливою для даного напрямку (в контексті охорони авторських і суміжних прав) стала й поява Директиви Європейського Парламенту та Ради 2001/29/ЄС про гармонізацію певних аспектів авторського права та суміжних прав у інформаційному суспільстві. Але в жодному з цих актів Всесвітня мережа Інтернет не зазначається як середовище використання відповідних творчо-інноваційних об'єктів, натомість використовується термін "цифрове середовище". Більш детально ці та інші документи будуть досліджені у Розділі 4 даного дисертаційного дослідження.

Для цілей даного дослідження вбачається важливим дослідити також генезу правового регулювання функціонування інститутів ІВ у цифровому домені у національному законодавстві нашої держави, особливо з урахуванням того, що Україна була внесена у 2020 р. до переліку країн, які порушують права ІВ та "завдають цим шкоду економічним інтересам Євросоюзу" [110].

У сучасному розумінні ПІВ на українських землях розвивається ще у ХІХ столітті, коли наші території були у складі Австрійської та Російської імперій, і вбирає у себе загальноєвропейські тенденції. Перші норми щодо правової охорони АП щодо публікації творів містилися у Цивільному кодексі Австрійської Монархії (1811 р.) і стосувалися права передруку і видавничої умови. У 1846 р. з'являються декілька галузевих актів, а саме патент про передрук (стосувався охорони літературної та художньої

власності), закон про літературну, музичну та художню власність, а кримінальне законодавство було покращене нормою про покарання за контрафакцію. Документ того часу, тим не менш, не містили безпосередніх положень щодо особи автора, регулювання співавторства, а тому до відповідних питань застосовувалася цивілістична концепція спільної власності. Але саме тоді було вперше врегульовано вільне використання творів, в т.ч. для цілей перекладу та цитування [294, с. 170].

Як зазначає Г.В. Довгань підпорядкування Австро-Угорській монархії гальмувало культурно-мистецькі процеси українців, тому й розуміння необхідності правової охорони результатів творчої діяльності у них сформується тільки наприкінці ХІХ ст. І уже 26 грудня 1895 р. був прийнятий закон про авторське право на твори літератури, мистецтва та фотографії, що був чинний для території західноукраїнських земель до 1926 р. і складався з 5 розділів та 68 параграфів. Так, дія цього документу, відповідно до його §1, поширювалася на твори літератури, мистецтва та фотографії, якщо їх створили в Австрії, або їх творцями є австрійські громадяни. Також вперше було врегульовано відносини співавторства. Були також закріплені АП упорядника на складені твори, презумпція авторства, а також присвоєння видавцеві АП на твори, видані під псевдонімом або анонімно тощо. Особисті немайнові та майнові авторські права не розмежовувались, лише окремі з них охоронялися. Відповідно до §22 правова охорона надавалася назві твору. Новелою даного закону також було введення реєстру авторів та їх безпосередніх творів, за формування якого відповідало Міністерство торгівлі, а ще - створення колегії експертів, які мали допомагати суддям при розгляді справ у сфері АП (перша така почала свою діяльність у Львові у 1896 р.). У зв'язку із прийняттям закону ЗУНР від 21 листопада 1918 р. про дію на її території австрійських законів до моменту прийняття власного законодавства з'явилася потреба і в

перекладі закону 1895 р., що виконав С. Дністрянський, вперше використавши українську юридичну термінологію [21, с. 47-50].

Щодо права промислової власності, то першим загальнодержавним НПА у сфері патентного права став Закон про привілеї від 15.08.1852 р. Так, згідно §1 винятковим привілеєм наділялися нові відкриття, винаходи, а також вдосконалення, предметом яких були новий виріб, спосіб чи метод виробництва. До таких об'єктів висувалася вимога місцевої новизни. кожному, хто претендував на відповідний привілей, мав звернутися із заявою до державної установи, куди також треба було подати опис, креслення та зразки результату винахідницької діяльності. Даний орган виконував те, що зараз прийнято називати формальною експертизою - перевіряв належність оформлення заявки, наявність всіх необхідних документів та сплату збору. Результатом такої перевірки було встановлення дата подання заявки, а з нею - і пріоритету. Далі відповідні матеріали досліджувалися Міністерством торгівлі та промисловості на предмет складення опису німецькою мовою або мовою коронного краю, кількості винаходів, яких стосується заявка, несуперечності об'єкту публічним інтересам. Корисність такого об'єкту перевірці не підлягала. Максимальний строк дії привілею складав 15 років, його можна було продати, передати у спадщину, піддати об'єкт ліцензуванню тощо. Але закон мав і суттєві недоліки, а саме застарілий явочний порядок привілейної видачі, відсутність можливості звернутися з апеляцією щодо визнання привілею недійсним, можливість видачі секретних привілеїв, а також підсудність справ про контрафакцію органам поліції [21, с. 50].

Далі послідував Закон про охорону винаходів (патентний закон) від 11 січня 1897 р., (не містив визначення винаходу, натомість його §1 наділяв правовою охороною нові, промислово придатні винаходи, а §5 - визнавав робітника винахідником, якщо інше не було передбачено трудовим договором, надаючи йому право на отримання винагороди. Строк дії

патенту складав 15 років. §29 позбавляв власника патенту, якщо той не був реальним винахідником або його правонаступником. Порядок отримання патенту передбачав проведення формальної експертизи, після чого відбувалася публікація відомостей про заявлений винахід, також Патентне відомство мало два місяці на подачу заявки й додатків до неї для загального ознайомлення (винахід на цей термін отримував тимчасову правову охорону). За навмисне порушення прав власника патенту передбачалося покарання у вигляді штрафу або арешту. Питання діяльності патентного суду, повірених та Патентного відомства бул регламентовані розділом II даного закону. Згодом, у вересні 1898 р. було видано Розпорядження мінторгівлі про організацію Патентного відомства з детальним описом його структур та повноважень. Того ж року світ побачили й інші НПА щодо патентного права, як от: про порядок діяльності Патентного відомства, про промислове використання винаходу, про вимоги до заявок та про представників у патентних справах, про патентних повірених та приватних техніків [21, с. 51-52].

Правова охорона промислових зразків базувалася на нормах імператорського патенту від 7 грудня 1858 р., а пізніше - закону від 23 травня 1865 р. про охорону зразків та моделей для промислових виробів. Варто вказати на те, що промислові зразки вважалися об'єктами торговельного права [5, с. 142-143]. Промисловим зразком вважався малюнок чи візерунок, який стосувався форми промислових виробів і був придатним до відтворення. До такого об'єкту, згідно §10 закону 1865 р., висувалася вимога абсолютної світової новизни. Виключних прав на зразок особа набувала з моменту його реєстрації у Торгово-промисловій палаті та видачі сертифікату. 3 роки становив строк правової охорони на такі об'єкти, а за навмисне порушення виключних прав на них слідувало покарання у вигляді штрафу або арешту [21, с. 54].

Щодо торговельних марок, то спочатку їх регламентація підпадала під дію закону про охорону промислових знаків (1858 р.), згодом - закону про охоронні марки від 6 січня 1890 р. Виключне право на використання даного об'єкту виникало через його реєстрацію у Торгово-промисловій палаті. Відомості про марки мали вноситися до двох реєстрів - у Торгово-промисловій палаті та у Мінторгівлі. Право на марку було тісно пов'язане з підприємством, для позначення товарів якого марка була зареєстрована. Строк правової охорони складав 10 років з можливістю повторної реєстрації об'єкту кожних 10 років. Навмисне порушення прав на зареєстровану марку тягнуло за собою покарання у вигляді штрафу або арешту з виплатою компенсації потерпілій особі [21, с. 56]. Тобто можемо підсумувати, що австро-угорський період для українців ознаменувався початком формування засад того, що сьогодні прийнято вважати ПІВ, і хоча він ніяк не стосувався безпосередньо кіберсередовища, але основи для регулювання ІВ уже було закладено.

Далі був період Російської імперії, де перші закони у сфері АП з'являються тільки у другій чверті ХІХ ст. Щодо охорони літературної власності, то свій початок він берез надання Академії наук та Комісії народних училищ привілеїв на друкування та продаж виданих ними книг. Не дивно, що характерною особливістю розвитку АП в імперські часи була тісна пов'язаність із цензурним законодавством (1720 р), що вимагало надати докази наявності у видавця прав на опублікування роботи при наданні її для цензури. Тобто це був перший акцент на необхідності дотримання АП. Перший імперський закон про авторське право з'явився у складі Цензурного статуту 1828 р. - у вигляді глави "Про авторів і видавців книг". В її §1 декларувалося виключне право автора на користування своїм твором як добросовісно набутим майном, а строк АП складав 25 років з дня його смерті автора. Також у документі містився перелік дій, що вважалися контрафакцією. Становлення авторського права в імперії, як зазначає Г.В.

Довгань, проходило в стані тотального нагляду за письменниками, із застосуванням каральної політики владою. У 1830 р. уряд затвердив нове Положення про права авторів, перекладачів і видавців, за яким строк охорони АП складав 35 років, а твір розглядався як річ. Тим не менш про особисті права автора нічого зазначено не було. Далі в галузі АП були поступово прийняті Положення про охорону прав композиторів (1845 р.), Положення про художню власність (1846 р.). У другій половині ХІХ ст. продовжуються цензурні обмеження творців, посилюється тиск на українську літературу. Головна особливість інституту авторського права в той час - сприйняття його як різновиду права власності [21, с. 58-60].

У березні 1911 р. було прийнято Положення про авторське право, яке розроблялось на основі німецьких законів 1901 р. й 1907 р. й Бернської конвенції, тобто було втілено новітню західноєвропейську доктрину АП. У ньому вперше визначено коло об'єктів, які охороняються АП (стаття 1), серед яких усні та письмові літературні твори, музичні, художні, фото та подібні їм твори (вперше фотографії отримали правову регламентацію рівноцінно із об'єктами АП). Новела документу - норми про співавторство, у випадку якого застосовувалися правила про спільну власність, і яке було двох видів - роздільне і нероздільне (ст-ст. 5 та 15). Ст. 68 закріпила права автора на відклик твору при наявності поважних причин. Декларувалося включне право всіма доступними способами відтворювати, публікувати та поширювати свій твір, згідно Статті 2. Також за автором було закріплено права перекладу, якщо про його збереження за автором було зазначено на титульному листі або у передмові. Також саме в цьому документі вперше містяться норми щодо видавничого договору. Дослідники вважають Закон 1911 р. важливим кроком, бо з прийняттям його у російському праві остаточно сформувалася концепція АП, яка відповідала в більшості своїй міжнародним стандартам [21, с. 61-68].

Щодо патентного права в Російській імперії, то воно розвинулося з привілею, і першим документом, в якому значилися всі основні засади сучасного патентного права, став привілей, наданий 13 грудня 1749 р. на відкриття заводу по виготовленню фарб. Перший місцевий закон щодо винахідництва побачив світ у 1812 р. у вигляді Маніфесту "Про привілеї на різні винаходи та відкриття в художествах і ремеслах", який складався з 6 глав. Він заборонив видачу привілеїв на винаходи, які суперечили суспільним інтересам (в сьогоденному розумінні), визнавав право першого заявника, і, головне - передбачав заявочну систему видачі привілеїв, яка сьогодні використовується в більшості країн світу (в т.ч. вона передбачена Статтею 16 ЗУ "Про охорону прав на винаходи і корисні моделі" 1993 р.). Також документ встановлював явочну система експертизи, виключність прав винахідника на використання винаходу. Внаслідок промислового перевороту Маніфест 1812 р. був доповнений Положенням про привілеї 1833 р., яке встановило охорону вдосконалень, більш високі вимоги до заявки та факультативний принцип видачі привілеїв, запроваджено попередній розгляд заявки. Новела - введення обов'язкового використання винаходу. Указ 1870 р. став першим патентним законом Росії; за ним заявки подавалися до Міністерства фінансів, строк дії привілею залежав від стану розвитку відповідної сфери промисловості. Нове Положення про привілеї на винаходи і вдосконалень прийняте у 1896 р., передбачало створення спеціалізованого Комітету з технічних питань при Департаменті торгівлі і мануфактур, що допомогло централізувати справи, розпорошені по різних міністерствам. Також було чітко визначено критерій суттєвої новизни, запроваджено систему "першого заявника" та інститут патентних повірених. Окремо передбачалася можливість подання заперечень третіми особами проти видачі привілею через відсутність новизни або присвоєння чужого винаходу. Строк правової охорони винаходів сягнув 15 років [21, с.

70-82]. Варто відзначити, що Російська імперія не приєдналася до Паризької конвенції 1883 р.

Подальша історія розвитку права інтелектуальної власності в Україні тісно пов'язана із періодом відродження української державності. Так, у 1918 р. гетьман П. Скоропадський зрікся влади, яка переходить до Директорії. Остання 26 грудня 1918 р. приймає декларацію, якою відновлює закони УНР [192, с. 86]. В складі Уряду діє Міністерство народного господарства, де є і відділ винаходів, який зрештою трансформують у так званий самостійний "патентовий уряд УНР", а у 1920 р. - в окремий Департамент охорони промислової власності". До повноважень останнього відносилися прийняття заяв на винаходи та удосконалення з метою проведення перевірки на новизну та подальшої видачі патенту, прийняття заяв на товарні знаки й затвердження таких тощо [115, арк. 1, 6].

Мала свої особливості і правова охорона прав ІВ на західноукраїнських землях у складі Польщі. На той час все ще залишалися в силі в різних регіонах держави закони інших держав. Так, в Галичині все ще діяв австрійські цивільний (1811 р.) та кримінальний (1852 р.) кодекси 1852 р., а у галузі АП - законодавство Австрії, Німеччини, Угорщини тощо [249, с. 197]. Отже, прийняття єдиного загальнодержавного закону у відповідній сфері було дуже актуальним. І, зрештою, у 1926 р. було прийнято Закон Республіки Польща "Про авторське право", що вміщував 7 розділів та 77 статей. Він містив положення про об'єкт авторського права, його суб'єктів та зміст прав авторів; про обмеження авторських прав та строк їх охорони; про основні види авторських договорів та агентський договір, а також норми щодо правової охорони. Але документ не містив конкретний перелік основних прав автора і не ділив їх на особисті і майнові. Тим не менш, він передбачав можливість відшкодування моральної шкоди, якщо буде доведено наявність умислу у діях порушника (ст. 61-69). Також добре врегульовано відносини щодо укладення видавничого договору (ст.

33-46). Порухеннями особистих прав слід було вважати привласнення авторства, авторського прізвища чи псевдоніму, незазначення автора у посиланні на його твір; опублікування твору без згоди творця; розкриття авторства тощо (ст. 58). У 1935 р. були ухвалені зміни до даного документу [301].

Щодо питань промислової власності, то у 1919 р. було видано три декрети: про патенти на винаходи, про охорону промислових зразків та моделей і про охорону товарних знаків. Вони зрештою були визнані невідповідними Паризькій конвенції. Тому у 1924 р. було прийнято Закон Республіки Польща "Про охорону винаходів, зразків та товарних знаків", який вміщував 162 статті та складався з 4 частин (про патенти на винаходи, промислові зразки й корисні моделі, товарні знаки і про органи Патентного Відомства та патентних повірених). В документі не було надано формально-логічне визначення терміну "винахід", але де-факто таким вважали нове технічне вирішення завдання, що можна використати у промисловості та торгівлі. У статті 5 перераховувалися об'єкти, що не підлягали патентуванню, як от наукові теорії, суперечні законодавству винаходи тощо. Критерії патентоздатності не вказувалися, але де-факто ними вважалися новизна та промислова придатність. Також Статтею 9 передбачалося право попереднього користувача, можлива була видача добровільних та примусових ліцензій. Система експертизи заявки була явочною, ще документом передбачався досить дієвий механізм захисту прав патентовласника із припинення незаконних дій порушником, який також вплачував неправомірно отриманий дохід за останні 3 роки і мав відшкодувати матеріальну і моральну шкоду. Щодо товарних знаків, то Закон 1924 р. не надав їх визначення, як і критеріїв вирізнення, але де-факто такими вважалися розрізняльна здатність та відносна новизна. Правову охорону ТМ отримували з моменту реєстрації, яка діяла 10 років з можливістю продовження [21, с. 105-108].

Через перегляд Паризької конвенції у 1925 р. трьома роками пізніше було змінено й Закон 1924 р. Розпорядженням Президента Республіки Польща, що вміщувало 245 статей. Особливих змін у змісті не було, але від патентовласника вимагалось почати використовувати винахід протягом трьох років від дати отримання патенту [155, с. 59-68], також охорона прав на об'єкти промислової власності посилилася (зросли штрафи за порушення прав на винахід, міг бути застосований й арешт на півроку) тощо [293, с. 9].

У часи СРСР правове регулювання у сфері ІВ базувалося на нормах і загальносоюзного законодавства. Для того періоду було нехарактерним забезпечення комплексної правової охорони результатів творчої інноваційної активності, стандартний поділ галузі робився на АП та винахідницьке право. Радянське нормативно-правове регулювання у відповідній сфері було надто залежним від внутрішніх факторів, а саме від особливостей адміністративно-командної системи управління. Так, свобода творчості була проголошена, але де-факто вона була дуже сильно обмежена [32, с. 47].

Але все змінилося у 1991 р., коли Україна отримала незалежність і почала розробляти та впроваджувати в життя власне законодавство, в т.ч. у сфері ПІВ. Наше держава за останні десятиліття відмітно активізувала зусилля щодо входження "на рівних" до світових структур, особливо у частині ПІВ та є нині учасницею більшості загальновизнаних міжнародних конвенцій і договорів у даній галузі.

Окремо слід наголосити на генезі правового регулювання саме національного законодавства у часи незалежності. Так, у 1996 р. прийнято Основний закон нашої держави, у якому містяться вже згадані у попередніх розділах дослідження статті 41 та 54 щодо права кожного на володіння, користування та розпорядження результатами своєї інтелектуально-творчої діяльності й гарантій свободи літературної, художньої, наукової і технічної творчості, а також захисту ІВ тощо.

У 1997 році в державі було започатковано систему державних стандартів у галузі промислової власності, а у наступному році в дію було введено такі стандарти як ДСТУ 3574-97 (про Патентний формуляр) та ДСТУ 3575-97 (про Патентні дослідження). Вони обов'язкові для дотримання суб'єктами господарської діяльності, якщо така діяльність повністю або частково фінансується з держбюджету, та мають рекомендаційний характер для всіх інших суб'єктів.

Наприкінці 20 та на початку 21 століття було введено в дію такі Кодекси:

- Кодекс законів про працю України (від 10.12.1971), в якому є Стаття 126 щодо гарантій, наданих працівникам - авторам винаходів, корисних моделей, промислових зразків, раціоналізаторських пропозицій (зміни внесено відповідно до ЗУ № 75/95-ВР від 28.02.95) та деякі інші щодо ІВ.
- Кодекс України про адміністративні правопорушення (від 07.12.1984), який містить, крім іншого, Статтю 51-2 щодо порушень прав на об'єкти ПІВ, якою документ було доповнено відповідно до ЗУ № 4042-12 (від 25.02.94), а подальші зміни до неї було внесено відповідно до ЗУ № 55/97-ВР (від 07.02.97), № 2362-III (від 05.04.2001) та № 2803-IX (від 01.12.2022).
- Господарський процесуальний кодекс України (від 06.11.1991), який вміщує, зокрема, норми щодо Вищого суду з питань інтелектуальної власності (Статті 3, 20, 22 тощо);
- Кримінальний кодекс України (від 05.04.2001), в якому містяться Статті 176 і 177 щодо порушень авторського права і суміжних прав та прав на винаходи, корисні моделі, промислові зразки, сорти рослин, топографії інтегральних мікросхем, раціоналізаторські пропозиції відповідно. Зміни у 176 Статтю було внесено відповідно до ЗУ № 3423-IV (від 09.02.2006), № 1111-V (від 31.05.2007), № 1019-VIII (від

18.02.2016), № 1977-VIII від (23.03.2017), № 2803-IX від (01.12.2022), у 177 Статтю - відповідно до ЗУ № 3423-IV (від 09.02.2006, № 1111-V (від 31.05.2007), № 1019-VIII від (18.02.2016).

- Цивільний кодекс України (від 16.01.2003 р.), який вміщує й Книгу Четверту, що безпосередньо та об'ємно регулює питання ПІВ, закріплюючи традиційну дворівневу систему законодавства про ІВ. Так, Главою 35 ЦК закріплені об'єкти та суб'єкти ПІВ, їх права та засади їх захисту тощо.
- Митний кодекс України (від 13.03.2012), окрім іншого, містить положення щодо реєстру об'єктів права інтелектуальної власності (Стаття 398 - зміни внесено відповідно до ЗУ № 202-IX (від 17.10.2019), № 202-IX (від 17.10.2019), № 202-IX від (17.10.2019), № 202-IX (від 17.10.2019), № 202-IX (від 17.10.2019), визначення контрафактних товарів, в т.ч., як таких, що є предметами порушення прав інтелектуальної власності на торговельну марку або географічне зазначення (Стаття 4) тощо.

Періодизація прийняття та зміни основних Законів України у відповідній сфері є наступною:

- ЗУ № 3687-XII Про охорону прав на винаходи і корисні моделі (від 15.12.1993) - внесення змін до даного НПА почалося у 2001 р., останні внесено у відповідності до ЗУ № 816-IX від (21.07.2020);
- ЗУ № 3688-XII Про охорону прав на промислові зразки (від 15.12.1993) - внесення змін почалося у 2001 р., останні внесено у відповідності до ЗУ № 815-IX (від 21.07.2020);
- ЗУ № 3689-XII Про охорону прав на знаки для товарів і послуг (від 15.12.1993) - внесення змін почалося у 2001 р., останні внесено у відповідності до ЗУ № 815-IX (від 21.07.2020);
- ЗУ № 3793-XII Про авторське право і суміжні права (від 23.12.93) - нині втратив чинність на підставі ЗУ № 2811-IX (від 01.12.2022);

- ЗУ № № 621/97-ВР Про охорону прав на компонування напівпровідникових виробів (від 05.11.1997) - внесення змін почалося у 1991 р., останні внесено у відповідності до ЗУ № 703-ІХ від (16.06.2020);
- ЗУ № 752-ХІV Про правову охорону географічних зазначень (від 16.06.1999) - внесення змін почалося у 2000 р., останні внесено у відповідності до ЗУ № 2572-ІХ від (06.09.2022);
- ЗУ № 2415-VIII Про ефективне управління майновими правами правовласників у сфері авторського права і (або) суміжних прав (від 15.05.2018) - із останніми змінами у відповідності до ЗУ № 2811-ІХ (від 01.12.2022).

Так, безпосередньо в процесі роботи над даним Розділом відбулися значні зміни у частині регулювання питань АП в Україні, адже Закон України про авторське право і суміжні права № 3792-ХІІ від 23.12.1993 втратив чинність на підставі Закону № 2811-ІХ від 01.12.2022 (втрата чинності від 01.01.2023). Цей факт має визначальне значення в контексті правового регулювання інститутів ІВ саме у цифровому (кібернетичному) середовищі. Так, у Статті 1 нового закону про АП надано визначення веб-сайту, гіперпосилання та веб-сторінки, інтерактивному наданню доступу (як поширенню об'єкта АП чи суміжних прав для публіки "з використанням ... у тому числі в мережі Інтернет або інших інтерактивних мережах, зокрема розміщення гіперпосилань та розміщення на одному веб-сайті цифрового контенту з іншого веб-сайту..."). Також визначено терміни "обліковий запис", "цифровий контент" тощо. Статтею 53 поняття піратства у відповідній сфері доповнено Інтернет-піратством як незаконним використанням відповідних об'єктів із застосуванням Інтернету. Стаття 56 регулює порядок припинення порушень у відповідній галузі з використанням всесвітньої мережі. Новий закон врегулював й інші питання, що пов'язані із використанням ІВ у кіберсередовищі [66].

Отже, генеза правового регулювання функціонування різних інститутів інтелектуальної власності у цифровому домені в світі загалом та безпосередньо в Україні характеризується як загальними закономірностями, так і специфічними особливостями. Як було зазначено, свої витoki правове регулювання ІВ загалом бере ще у 17 столітті, але у контексті саме кібернетичного простору таке починає активно формуватися аж наприкінці 20 століття. Внесення відповідних змін до міжнародних договорів з ПІВ, введення в дію інтернет-договорів ВОІВ та розробка на їх фундаменті національного законодавства країн світу, відповідна впровадження Директив та Регламентів ЄС, а також розробка та удосконалення українського національного правового масиву - все це сьогодні є основою оперування об'єктами та правами ІВ у цифрового просторі.

І хоча для України дана правова стежина ще є досить новою, але локальне правове регулювання дійсно покращується нормотворцями з урахуванням сучасних кібернетичних тенденцій. так, розширюється список об'єктів ІВ, в тому числі й тих, чиє використання пов'язане із функціонуванням кібердомену. Законодавець намагається конкретизувати відповідні аспекти та особливості цих об'єктів, тим самим зменшуючи кількість прогалин у праві, що особливо важливо при вирішенні спорів. Уже зараз ми можемо спостерігати позитивні тенденції щодо процесів набуття та захисту прав інтелектуальної власності у Всесвітній мережі, в тому числі. Але важливо не зупинятися, адже саме безперестанне вдосконалення законодавство та механізмів його реалізації щодо охорони прав інтелектуальної власності загалом та безпосередньо у кіберпросторі є надважливим завданням. Воно потребує прийняття виважених та адекватних рішень у контексті внесення змін до відповідних НПА з урахуванням євроінтеграційних процесів нашої держави.

Саме тому знання особливостей генези правового регулювання функціонування інститутів ПІВ загалом та у цифровому середовищі безпосередньо є вкрай важливими, саме на їх фоні можна розробляти та впроваджувати нове правове регулювання з урахуванням помилок та недосконалостей регулювання минулих років та навіть століть. Такі знання разом з науковими доробками вчених формують собою науково-теоретичне підґрунтя інтелектуальної власності та допоможуть в подальшому створити та впровадити більш дієве регулювання відповідних відносин.

3.3. Актуальні питання правового регулювання відносин щодо дотримання права інтелектуальної власності у глобальних інформаційних та комп'ютерних мережах

Як вже стало зрозуміло з попередніх розділів даного дисертаційного дослідження, роль правового регулювання відносин щодо дотримання права інтелектуальної власності є дуже важливою, особливо в розрізі цифрового середовища (кіберпростора). Так, в сучасному світі загалом, та безпосередньо в Україні швидкими темпами розвивається електронна комерція та електронний бізнес, а тому різні організації та підприємства намагаються усіма доступними засобами захистити свої прав інтелектуальної власності у Всесвітній мережі як безпосередньому втіленні кіберсередовща.

Слід нагадати, що сьогодні інтелектуальна власність є складовою нематеріальних активів підприємства [11, с. 126], а тому порушення авторських прав, прав на засоби індивідуалізації та інших прав інтелектуальної власності можуть стати причиною не тільки втрати коштів, але й ділової репутації компаній. Саме тому важливо розуміти, які виклики, проблеми та взагалі питання правового регулювання відносин щодо дотримання права інтелектуальної власності у глобальних інформаційних

та комп'ютерних мережах є найбільш актуальними сьогодні. Дане питання й буде детально досліджено далі.

Технології сьогодні розвиваються невпинно, і нині майже кожна людина у світі має змогу бути активним користувачем кіберпростору, а з тим - і легко обмінюватися інформацією, використовуючи комп'ютери та різні гаджети, що об'єднані через комп'ютерні мережі у цифровому просторі. І серед таких даних, які передає інтернет-юзер, можуть бути й ті, на які поширюється ПІВ. Тому сьогодні розвиток кібертехнологій нерідко призводить до порушення прав інтелектуальної власності в Мережі.

Окрім "традиційних" порушень інтелектуальної власності, Всесвітній мережі відомі особливі порушення (виходячи з їх суті, назовемо їх гібридні), а саме фреймінг, глибокі посилання, продаж піратської продукції, що нині є досить непростою задачею для правоохоронних органів. Велика кількість веб-ресурсів пропонує встановити безкоштовно ПЗ, що є піратською копією та здійснюють іншу нелегальну діяльність, що значно ускладнює боротьбу із порушеннями авторських прав в кіберпросторі.

Можемо сказати, що однією із головних проблем у вказаній сфері є порушення прав на онлайн-контент (в розрізі Авторського права). Так, розміщені в Мережі твори художнього, літературного, наукового чи іншого змісту нерідко стають об'єктами отримання прибутку від їх використання. Якщо таке робиться без дозволу власника, то має місце порушення його авторських прав. Відповідні порушення, зазвичай, проявляються у формі використання творів без дозволу правовласника, створення та розповсюдження копій програмного забезпечення та їх подальший продаж, незаконне копіювання авторських текстів, зображень з вебсайтів.

Перелічені дії, як відомо, заборонені законодавством, адже, відповідно до Статті 12 нового ЗУ про авторське право і суміжні права, саме суб'єкт авторського права (яким є автор чи інші особи, що законно володіють матеріальними правами на твір) вправі дозволяти або забороняти

використання авторсько-правового об'єкту іншими особами [66].
Відповідно, лише з дозволу правовласника інша особа може розміщувати твори в Інтернеті для загального користування.

Але згідно зі статтею 22 Закону 2811-ІХ ви можете вільно використовувати твір без згоди правовласника, безкоштовно, без вказівки на автора та джерела запозичення. Випадками такого вільного використання є: відтворення об'єкту АП в цілях налаштування, демонстрування чи ремонту обладнання, відтворення у вигляді макета, креслення або плану споруди задля проведення реконструкції, відтворення з метою забезпечення судових проваджень, нормотворчості, забезпечення громадської безпеки, а також публічне виконання музичних творів в ході офіційних, релігійних, ритуальних церемоній тощо. На аналогічних умовах, але із вказівкою на авторство та джерела запозичення дозволено цитування, відтворення з метою забезпечення освітнього процесу чи ведення наукових досліджень (без цілі отримання економічної вигоди), репрографічне відтворення суб'єктами освітньої діяльності, відтворення в електронній формі для дистанційного навчання, доведення до загального відома задля висвітлення поточних подій, відтворення у каталогах, створення на основі первинного твору попури, пародії, карикатури тощо [66].

Важливо також вказати на можливість, відповідно до статті 24 Закону, вільного відтворення бібліотеками та архівами примірників твору репрографічним способом, музеями з відкритим доступом для відвідувачів, іншими організаціями із збереження фондів, якщо така діяльність не здійснюється з метою отримання комерційної вигоди [66]. Це робиться, коли є підозра, що оригінал роботи може бути втрачений, пошкоджений, а сама така копія буде використана суто з "доброчесною" метою - для навчання чи наукових досліджень.

Все значно складніше у випадку із онлайн-бібліотеками, які досить часто нелегально розміщують захищені АП роботи. Це такі вебресурси, як

Library Genesis, Twirpx тощо, метою яких є безкоштовний обмін науковими та освітніми матеріалами, які юзери особисто завантажують на сайт такої бібліотеки.

Як зазначає Н.В. Троцюк, процедура створення електронної бібліотеки в Україні є справою надскладною, що передбачає, крім іншого, створення Реєстру суб'єктів АП на опубліковані роботи та укладення договорів із правовласниками, виплатою їм винагороди тощо. А тому, як вважає науковиця, така ресурсомісткість процедури нерідко спонукає українські електронні бібліотеки до нелегального розміщення на своїх веб-сторінках творів, що охороняються авторським правом [107, с. 106].

У контексті авторського права треба окремо згадати про піратство програмного забезпечення. Нагадаємо, що піратство в розумінні ПІВ, зазвичай виявляється у несанкціонованому відтворенні і тиражуванні, розповсюдженні, продажі твору, який отримав захист як об'єкт АП. Тобто будь-яке несанкціоноване використання творів під захистом авторського права, їх продаж без належного попереднього дозволу - це піратство [312].

На офіційному сайті ІНТЕРПОЛУ надано визначення цифровому піратству, яке стосується незаконного копіювання та (або) розповсюдження об'єктів, що захищені АП, через Всесвітню мережу Інтернет. Таке дуже негативно впливає на творчі індустрії, включаючи видавництво, кіно, телебачення, музику та ігровий контент, а також піддає споживачів ризику фінансових втрат і може створити ризики безпеці для користувачів, наприклад, у разі викрадення ідентифікаційного номера або перенаправлення неповнолітніх осіб на неприйнятний вміст [157].

Відповідно, коли ми говоримо про піратство програмного забезпечення, то маємо на увазі те ж саме, що і піратство щодо інших об'єктів АП, тільки в даному випадку об'єктом правопорушення виступають комп'ютерні програми і аналогічні матеріали. Зазвичай піратство ПЗ стосується створення неавторизованих копій такого комп'ютерного

програмного забезпечення, що, відповідно захищене відповідно до нашого законодавства про авторське право.

У цьому контексті зазначимо, що відповідно до п. 21 Статті 1 нового Закону про АП №2811-ІХ, законним користувачем комп'ютерної програми (далі - КП) вважається особа, що "правомірно володіє копією комп'ютерної програми, виготовленою правомірно". Згідно ж статті 20 відповідного НПА, охорона розповсюджується на оригінальні комп'ютерні програми, виражені у вихідному або об'єктному кодах, і надається саме формі вираження КП. Відповідною формою не буде вважатися графічний інтерфейс, виконувани функції або формат файлів даних для експлуатації функцій КП. При цьому не підлягають відповідній охороні ідеї та принципи, на яких базується будь-який елемент КП [66].

Як зазначає А. Діксіт, піратство програмного забезпечення буває наступних видів:

- малозначна крадіжка (від англ. *soft lifting*), яка передбачає передачу КП чи іншого ПЗ неавторизованому суб'єкту, тобто особі, що не є стороною відповідної ліцензійної угоди на використання такого об'єкту;
- підробка програмного забезпечення, тобто незаконне виготовлення копій ПЗ, які імітують оригінал і, зазвичай коштують відчутно менше, ніж оригінальний продукт. Така підробка включає в себе не тільки незаконне виготовлення ПЗ, але й створення обгортки (коробки), матеріального носія та інструкційних матеріалів, що виглядають максимально схожими із оригінальним об'єктом;
- оренда копії ПЗ для використання протягом певного часу без дозволу правовласника, що, відповідно, порушує ліцензійну угоду програмного забезпечення [174].

Піратство програмного забезпечення та взагалі інтернет-піратство є, на жаль, досить розповсюдженим феноменом навіть у країнах із

розвинутою економікою та якісним правовим захистом об'єктів ІВ. Це обумовлене, в більшості своїй, легкістю копіювання творів та надто високими цінами на оригінальній продукції.

Тим не менш, як зазначають спеціалісти ІНТЕРПОЛУ, є чимало ризиків, на які наражає себе користувач піратського контенту:

- дійсно, ціни на відповідний вміст значно нижчі за ціни на оригінальний твір. Тим не менш, за такого стану речей творчі індустрії, різні організації мовлення та безпосередньо податкові органи не отримують належні їм доходи, відповідно, не заробивши грошей, відповідні суб'єкти будуть набагато менше витратити на створення нового контенту. Менше контенту - менше потрібно робітників для роботи з ним, а отже і менше робочих місць у відповідній сфері.
- користувач може не отримати заявлені послуги чи товари, а також втрати більше грошей, адже немає ніякої гарантії такого. До того ж сплачені вами кошти зараховуються не на офіційні законні рахунки правовласників, а на рахунки піратів за складними схемами відмивання грошей. А ще у злоумисників залишаються дані ваших платіжних засобів, що теж може стати причиною крадіжки коштів з вашого рахунку. Ну, і вам просто можуть перестати надавати відповідну послугу (наприклад, трансляції контенту чи підтримки ПЗ) без якихось застережень;
- серйозні ризики кібербезпеки споживачів також йдуть рука об руку із нелегальним контентом. Так, відповідні матеріали можуть містити неприйнятний вміст або зловмисне ПЗ, що воліє заразити гаджет юзера, можливі й витоки та зломи даних, викрадення особистої інформацію користувача - а з ними й акти шахрайства [157].

Найпопулярнішими джерела онлайн-піратства (або цифрового (діджитал) піратства є:

- веб-ресурси, що пропонують прямі трансляції. Але на сторінці із "зламаним" контентом буде чимало спаму, реклами, а також зловмисного ПЗ типу вірусів, що скрито завантажуються без дозволу користувача;
- однорангові мережі (англ. *peer-to-peer networks, P2P*). Такі мережі можуть застосовуватися для спільного використання та обміну файлами (наприклад, музикою, фільмами, ПЗ тощо), що може призвести до порушення права власників авторських прав. Таке можливо, наприклад, коли один користувач купує ліцензійну копію твору і завантажує її в мережу P2P, а користуються таким об'єктом вже інші, "неавторизовані" користувачі [247];
- кіберблокери та хмарні сервіси. Різні хмарні сервіси як от Google Drive, Dropbox тощо призначені для зберігання та обміну файлами, що дає змогу й зловмисникам завантажувати в "хмару" нелегальний контент. Подібні сервіси, звісно, намагаються блокувати відповідні облікові записи, але й кіберпорушники не стоять на місці, створюючи нові і знову завантажуючи нелегальний вміст;
- вебсайти онлайн-аукціонів. Зазвичай таке стосується попереднього "випробування" (тестингу) ПЗ з метою пошуку недоліків та "дір" у ньому, для чого зацікавленим користувачам компанія-розробник надсилає версію програми та інструкції щодо взаємодії з нею, а після тестування користувач має повернути отримане. Пірати ж, перш ніж повернути таке, роблять копії ПЗ для своїх цілей тощо [133].

Сприяє поширенню інтернет-піратства, на нашу думку, також реклама, яку купують відомі бренди і яка розміщується автоматично, в тому числі на піратських веб-ресурсах, й доступність контенту для звичайних користувачів. Саме тому інтернет-піратство є надто поширеним не тільки в нашій державі, але й в усьому світі, тим не менш підходи до його подолання відрізняються. Так, наразі стала популярною практика перекладення

відповідальності за запобігання розповсюдженню нелегального контенту на провайдерів, вони також мають здійснювати контроль за таким розповсюдженням. У деяких країнах, зокрема, Сполученому королівстві та Франції впроваджено механізм розсекречення даних абонентів, які надали доступ до нелегального контенту, що передбачає відповідне звернення до судової установи чи спеціалізованого органу з авторського права та суміжних прав в Інтернеті.

Щодо нашої держави, то тут діє некомерційна організація «Українська антипіратська асоціація» (її вебсайт знаходиться за посиланням: <https://apo.kiev.ua/>), що покликана боротися із онлайн-піратством. Крім іншого, діє спеціальний вебсайт із розміщеним на ньому переліком вебресурсів, що підозрюються у незаконному розміщенні контенту (вебсайт знаходиться за адресою: <http://blacklists.org.ua/>). Знаючи порушників "у лице", бренди під час купівлі реклами, можуть ігнорувати відповідні веб-сайти, тим самим не підтримуючи інтернет-піратство. Окремо запроваджено й ініціативу «Чисте небо», яка кооперує свою діяльність із кіберполіцією у боротьбі із онлайнпіратством та підтримує публічне інформування про сайти та провайдерів, які є порушниками (вебсайт ініціативи: <https://legalcontentua.org/>).

Також до порушень саме авторських прав у кіберсередовищі деякі вчені додають **посилання** (англ. *Linking*), які спрямовують веб-юзера з однієї веб-сторінки на іншу шляхом натискання на певне позначення (зазвичай, текст чи зображення) без виходу з поточної веб-сторінки. Таке створює загрозу правам власника веб-ресурсу, бо той може втратити дохід, пов'язаний із кількістю відвідувачів його сайту. А самі ж юзери можуть бути введені в оману, бо вирішать, що обидві веб-сторінки пов'язані між собою та знаходяться під одним доменним іменем (що належить одному власникові) [174].

На думку дослідників, особливо складно все із глибокими посиланнями, адже щодо них не існує жодного відповідного національного чи міжнародного правового акту, що є "на руку" кіберпорушникам. Правова проблема виникає в цьому контексті щодо встановлення часу (стадії) здійснення відтворення твору, тобто мова про етап формування глибокого посилання. І тут вже постає питання про те, коли саме відтворення відбувається - під час доступу до посилання, яке не потребує схвалення, або ж у момент переходу за посиланням за власним бажанням юзера [174].

Проблемними виявились і внутрішні посилання. У браузері, яким користується людина, формуються карта посилань для отримання зображень із різних джерел, які й копіюються кінцевим користувачем, що, зазвичай, навіть не підозрює про отримання зображень з різних веб-ресурсів. У даному випадку також досить складно відстежити точний момент відтворення зображень. І хоча людина, що створила таке посилання не розповсюджувала твір безпосередньо, але АП порушила, бо надала можливість створювати неавторизовані копії творів [174].

Прикладом ситуації порушенням у формі "посилання" є справа *Shetland Times Ltd. проти Доктора Джонатана Уїлса та Zetnews Ltd.*, що слухалася у Сесійному суді (вищому цивільному суді Шотландії). Так, судовий орган видав тимчасову заборону на копіювання відповідачами без згоди позивача заголовків з газети позивача на свій сайт і створення гіперпосилань з цих заголовків на сторінку позивача, де і розміщена стаття, під відповідним заголовком. Справа в тому, що такі "лінки" дозволяли інтернет-користувачеві, відразу переходити до відповідної статті, оминаючи домашню сторінку позивача. Тим самим юзери оминали й будь-які рекламні матеріали, які могли міститися на такій сторінці [274].

Серед порушень у галузі авторського права виокремлюють і **фреймування** (фреймінг - від англ. *framing*). Слід пояснити, що веб-сторінка, зазвичай складається із ланок, так званих фреймів, що є окремими

завершеними незалежними елементами розмітки документів для перегляду сторінок сайту у браузері. І фреймінг, відповідно, полягає у розміщенні у фреймах посилань на матеріали інших веб-ресурсів, вміст сторінок яких можна переглядати тут же, у фреймі, не переходячі на безпосередній сайт розміщення відповідного матеріалу.

За практикою Індії та деяких інших країн, фреймування не надто популярне, а сайти, які використовують фрейми із контентом інших веб-сайтів, сприймають як крадіїв веб-контенту. Кейсів з даного питання небагато, а тому, вірогідно, що саме розробника буде визнано відповідальним за порушення авторського права, якщо спірний матеріал буде видозмінено під час фреймінгу, або користувачі будуть введені в оману щодо джерела спірної інформації [284].

Окрім іншого, зауважимо і на такому копірайт-порушенні, як незаконне використання бази даних. Зазвичай суб'єкти стикаються із незаконним проникненням, "вторгненням" (англ. trespassing) в саму базу та її копіюванням, а також в конфіденційність відомостей в ній, безпосередньою їх крадіжкою та подібними діями.

Окремі виклики для права інтелектуальної власності у кіберпросторі створило сьогодні й активне впровадження штучного інтелекту (далі - ШІ). Так, основна проблема, на нашу думку, полягає у неавторизованому створенні контенту, адже алгоритми ШІ можуть створювати великі обсяги матеріалів, які порушуватимуть вже існуючі об'єкти, захищені авторським правом. Відповідно, виникатимуть і труднощі із визначенням авторства, що ще більше ускладнить захист та правозастосування інтелектуальної власності, зокрема, у кіберпросторі. Варто вказати й на те, що ШІ може сприяти здійсненню порушень, коли його алгоритми автоматизовані, що може оптимізувати діяльність із порушення ППВ, тим самим сприяючи піратству та створенню контрафакту.

Не менш актуальним та проблемним питанням правового регулювання відносин щодо дотримання права інтелектуальної власності у глобальних інформаційних та комп'ютерних мережах залишається кіберсквоттинг та порушення щодо засобів індивідуалізації учасників у цивільному обороті.

Кіберсквоттинг (від англ. *cybersquatting*), як зазначено в Заключному звіті процесу ВОІВ щодо доменних імен в Інтернеті, це навмисна, недобросовісна реєстрація доменного імені з порушенням прав на торгові марки та знаки обслуговування; за термінологією організації це “зловживання реєстрацією доменного імені” [184]. Відповідно до С.Б. Булеци та А.В. Тегзи, кіберсквоттингом є недобросовісна реєстрація, продаж чи використання доменного імені чужої ТМ задля отримання прибутку [140, с. 60].

Варто вказати на те, що доменне ім'я як особливий цивільно-правовий об'єкт [183, с. 128] наразі офіційно не є об'єктом інтелектуальної власності відповідно до нашого законодавства. Але якщо такий засіб ідентифікації учасників у цивільному обороті зареєструвати як товарний знак (торгову марку), то і відповідна охорона буде надана такому об'єкту [12]. У зв'язку із зазначеним для цілей даного дослідження вватимемо доменні імена (як частини ТМ) об'єктами інтелектуальної власності.

Отже, зловживання реєстрацією доменного імені, зазвичай, проявляється у реєстрації доменного імені, що відповідає існуючому ТЗ задля подальшого його перепродажу справжнім власником торговельної марки, також може мати місце імітація доменного імені як ТМ в тому вигляді, щоб ввести в оману юзера відомого вебсайту тощо. Для уникнення подібного необхідно, щоб реєстратори доменних імен неухильно дотримувались відповідної політики ICANN.

Дослідники виділяють наступні види кіберсквоттингу:

- географічний - коли має місце реєстрація доменного імені (далі - ДІ), що тотожне назві певного населеного пункту, географічного району тощо;
- галузевий - реєстрація ДІ за назвою товару, послуги, виду діяльності тощо;
- іменний - реєстрація ДІ, схожими/тотожними до імен, псевдонімів, прізвищ відомих осіб.
- брендовий – реєстрація ДІ, що дуже схожі або навіть тотожні до відомих ТЗ чи комерційних найменувань [59, с. 126].

Також кіберсквотинг може бути захисним, коли суб'єкт реєструє ДІ подібне до свого власного [140, с. 60].

Окремо виділяють і так званий **тайпсквотинг** (від англ. *typosquatting*). Це така практика реєстрації веб-адреси, яка є схожою на URL-адресу цільового вебсайту, але не один-в-один, задля введення користувача в оману і направлення його на фішинговий веб-ресурс [267]. Тобто це різновид онлайн-шахрайства, заснованого на припущенні про те, що юзери передбачувано погано володіють орфографією [137]. Тобто, зазвичай тайпсквотинг виглядає як друкарська помилка gsl час написання, описка. Не варто плутати його із так званим *Domain Spoofing* (з англ. "підробка домену"), коли правопорушник розробляє версію-підробку сайту, наприклад, свого конкурента, і такий ресурс буде виглядає ідентично до оригіналу, але знаходиться за іншим URL-посиланням [267].

К. Заїді серед порушень щодо доменних імен також називає мета-теги або метатегування. Мова про особливу техніку збільшення кількості відвідувачів веб-ресурсу через включення в розділ ключових слів таких зазначень, які не мають ніякого відношення до даного сайту чи, наприклад, бренду. Робиться таке із метою спонукати пошукові системи спрямовувати користувачів на відповідний вебсайт. Це може негативно сказатися на ТЗ

певної компанії, якщо веб-сайт містить мета-теги інших ресурсів, бо відповідне впливає на їхній бізнес [313].

Саме брендовий кіберсквоттинг та тайпсквоттинг, на думку С.Б. Булеци, є найнебезпечнішими серед різновидів кіберсквоттингу, адже їх головна мета - отримати перевагу над конкурентами у комерційній сфері, також вони нерідко призводять до суттєвих майнових збитків й шкоди діловій репутації суб'єктів господарювання. Інші види науковці відносять до так званого домейнінгу; вони не призводять до серйозних збитків і будуть кваліфіковані як правопорушення лише за відповідності умовам визначення акту як незаконного кіберсквоттинга [140, с. 60].

Друга категорія інтелектуальної власності, яка має відношення до кіберправа та одночасно до сфери засобів індивідуалізації учасників у цивільному обороті - це торгові марки. Найчастіше проблеми виникають у разі використання товарного знаку у господарській діяльності без згоди правовласника, наприклад при виробництві або продажі контрафактних товарів, а також коли ТМ застосовується таким чином, що в уяві споживача виникає плутанина щодо походження товару або послуги. Тобто обидва вказані випадку взаємопов'язані. Відповідно, коли торгова марка однієї компанії використовується на сайті іншої (без відповідного дозволу), то будемо говорити про порушення відповідних прав в кіберпросторі. Варто мати на увазі, що те, чи відбувається порушення через Інтернет чи ні, значення не має, адже елементи порушення прав на ТЗ залишаються незмінними.

Як зазначає практикуючий юрист Я. Георгіадес, порушення прав на ТМ зазвичай є простим у тому сенсі, що воно має місце коли подібне або тотожне позначення використовується таким чином, що створюється ймовірність плутанини щодо походження товарів або послуг і можливості асоціації між двома торговельними марками, або використовувати на тих товарах й послугах, які не мають відношення до оригінального товарного

знаку, але їх реєстрація надасть переваги недобросовісному реєстранту. Умовами, які свідчитимуть про наявність порушення слід вважати схожість загального враження, яке справляють дві торгові марки, будь-які докази фактичної плутанини споживачами та фізична близькість товарів на ринку [220].

Щодо зазначеної плутанини, то такий критерій має свої особливості. Так, відповідач у позові про порушення прав на ТЗ задля свого захисту може посилатися на використання ТМ як пародії. Нею буде вважатися використання загальновідомого твору з метою критики, сатири, коментаря щодо оригінальної роботи, і відповідно, таке дозволено, адже введення в оману щодо походження товару від певного виробника не буде мати місце. У якості приклада наведемо кейс 2008 року, коли Wal-Mart позивався до жителя Джорджії (США) як до порушника прав на ТМ. Даний суб'єкт, як було встановлено, створив сайт і логотип зі словами "Walocaust", використавши при цьому фірмовий логотип позивача задля критики останнього. Але Федеральний суд постановив, позивач не може посилатися в даному випадку на законодавство про торговельні марки, інакше таке буде вважатися перешкоджанням у висловленні відповідачем своїх поглядів. Головний аргумент - неможливість створення плутанини у споживача щодо відповідного веб-сайта з компанією Wal-Mart [225].

Цікавим є й кейс Lancome проти eBay, коли Брюссельський комерційний суд відмовився притягнути відповідача до відповідальності за контрафактну косметику, що продається через належний йому сайт. Але eBay несе відповідальність за правопорушну діяльність на її онлайн-майданчику. При цьому, за постановою суду, власник ТМ може перешкоджати оператору такого торговельного майданчику рекламувати продукти під цією конкретною ТМ, якщо для споживача не буде очевидним походження товару [220].

Штучний інтелект, про який було згадано вище, також ускладнює й захист ТМ. Зокрема, на його базі можуть створюватися підробки продуктів або нелегальний контент, що надто схожий на вже існуючі ТЗ, відповідно виявлення правопорушення може бути ускладнене. Можливості ШІ в царині анонімізації та автоматизації можуть сприяти правопорушній активності в частині використання лазівок в системі товарних знаків, що, знову ж таки, ускладнює відстеження та притягнення порушників до відповідальності.

Є актуальним сьогодні і проблема захисту патентів в контексті правового регулювання відносин щодо дотримання права інтелектуальної власності у глобальних інформаційних та комп'ютерних мережах. Як відомо, видача такого охоронного документа, в тому числі, засвідчує і право його власника дозволяти чи забороняти іншим створювати, використовувати відповідний винахід, пропонувати його для продажу, імпортувати тощо.

В цьому сенсі варто згадати справу Alcatel-Lucent USA проти Newegg Inc та Overstock.com Inc 2011 року, коли два найбільших американських інтернет-магазини звинуватили у порушенні трьох патентів позивача. Порушення таких було пов'язано із застосуванням вміщуваних в них функцій електронної комерції, а саме розкривного списку, текстових полей, пошуку на вебсайті та інструментів, які виправляють орфографічні помилки користувача. Натомість відповідачі стверджували, що патенти Alcatel є недійсними, адже використовують технологію, яка не є оригінальною та базується на попередніх винаходах. Суд підтримав відповідачів, погодившись із "очевидністю" запатентованих технологій, тобто тим, що вони є добре відомими та недвозначними [268].

Також не варто забувати і про штучний інтелект в розрізі патентів, що пов'язані із використанням Всесвітньої мережі. Можна дійти висновку, що в онлайн-сфері патенти стосуються здебільшого методів ведення бізнесу в

Інтернеті, особливо в частині електронній комерції, як от використання лише однієї кнопки для здійснення онлайн-купівлі товару на маркетплейс-сайті. Але поява штучного інтелекту змусила патентні відомства по всій земній кулі активно шукати відповідь на питання про те, як поводитися з винаходами, які не є результатом людської творчості, а створені безпосередньо ШІ.

Наостанок варто зазначити на існуванні декількох теорій, що описують необхідність захисту прав інтелектуальної власності взагалі, та можуть бути застосовані, на нашу думку, в аспекті, відповідно, кіберсередовища, зокрема в Інтернет-мережі. Так, першим, згідно Г. Аггарвала, є так званий утилітарний підхід. Він зиждеться на тому, що творець має отримувати такі права, які б заохочували винахідників та авторів "творити", створюючи об'єкти, захищені ПІВ, щоб це приносило максимальну користь максимальній же кількості осіб. За другого підходу, що базується на роботах Дж. Локка, людина, яка докладає зусиль для дослідження чогось, що або не належить жодній особі, або "вже є спільним", володіє "інтелектуальною власністю своїх зусиль", яку країни повинні поважати та захищати. Є й третій підхід, за Кантом і Гегелем, згідно якого права ІВ є приватними правами творців і надають їм унікальні права (як от тільки автор має право відтворювати та публікувати свої твори чи надавати дозвіл іншим особам на такі дії). За четвертого підходу (в його основі ідеї Джефферсона та Маркса) права інтелектуальної власності мають бути сформовані таким чином, щоб «досягти привабливої культури». На відміну від утилітарного підходу, дана модель не наголошує на «найбільшому благу найбільшій кількості» [292].

Отже, значно зросла кількість правопорушень із розвитком технологій. Всесвітня мережа як найбільш використовуваний оплот кіберсередовища дозволила людям легко копіювати та відтворювати чужий контент без відповідного дозволу. Найбільшою проблемою в даному

контексті було й залишається онлайн-піратство, хоча під загрозу нерідко попадають також патенти, торгові марки та інші засоби індивідуалізації учасників у торговельному обороту. Уряди окремих країн та інші органи впроваджують нормативні акти, що покликані забезпечити максимальний захист інтелектуальної власності в інформаційних та комп'ютерних мережах, адже відповідні порушення призводить не лише до втрати можливого доходу та репутації комерційними суб'єктами, але й сприяють небажанню інвесторів вливати капітал у відповідну сферу, а також незацікавленості творців у створенні нових творчо-інноваційних продуктів. Для вирішення цих проблем в Україні необхідно переглянути старі та розробити нові НПА з урахуванням досвіду провідних країн світу та думки вчених. створити нові закони.

Висновки до Розділу 3

Розвиток інформаційних технологій, зростання їх кількості та складності породили й збільшення кількості актуальних питань правового регулювання відносин щодо дотримання права інтелектуальної власності у кібернетичному просторі взагалі та в окремих глобальних інформаційних й комп'ютерних мережах. Серед проблем та викликів, які найчастіше зустрічаються у відповідній сфері, варто назвати онлайн-піратство, тобто несанкціоноване використання та продаж інтелектуальної власності, що належить іншій особі, чим грішать не тільки окремі-веб-сайти, але й соціальні мережі, що значно полегшили користувачам публікацію та обмін контентом в Інтернеті. Торгові марки, доменні імена, інші засоби індивідуалізації учасників у торговому обороті, патенти тощо - все це нині під загрозою у кібернетичному просторі. Ще більше занепокоєння сьогодні викликає і використання технологій штучного інтелекту у зв'язку із вказаним. Влади країн, окремі організації та навіть окремі веб-ресурси впроваджують різні акти задля забезпечення максимального захисту

результатам творчо-інтелектуальної діяльності осіб, застосовують нові системи для перешкоджання вільному копіюванню та розповсюдженню контенту у глобальних інформаційних мережах тощо.

Але, на жаль, цього не завжди достатньо, щоб захистити права відповідних правовласників і самі об'єкти. Саме тому так важливо знати особливості структури відповідних відносин, їх генезу та властивості правового регулювання, а також нагальні загрози та проблеми у відповідній сфері, щоб створити та впровадити дієві механізми та засоби захисту й охорони прав, адже тільки так можна дійсно сприяти бажанню авторів та інноваторів творити, тільки так можна забезпечити їх визнання та отримання ними належної фінансової винагороди. Відповідно таке сприятиме і економічному розвитку як окремих країн, так і всього світу.

У третьому розділі дисертаційного дослідження на основі використання теоретичних наукових методів, в тому числі, гіпотези, теорії, наукового моделювання тощо та загальнонаукових методів пізнання було досліджено актуальні питання правового регулювання відносин щодо дотримання права інтелектуальної власності у кіберпросторі. В ході роботи детально проаналізована структура відповідних відносин, надано їй юридичну характеристику. Детальна увага приділена також генезі правового регулювання функціонування окремих інститутів інтелектуальної власності у кібернетичному домені, визначено актуальні питання правового регулювання відносин щодо дотримання відповідних права у глобальних інформаційних та комп'ютерних мережах. Результати, отримані в процесі дослідження, дали змогу дійти наступних висновків:

1. Визначено структуру правовідносин як симбіоз суб'єктів та доцільного способу зв'язку між ними з основою на суб'єктивних юридичних правах та обов'язках по відношенню до певних соціальних благ чи інтересів. На основі зазначеного було надано визначення поняттю структури відносин щодо дотримання права

інтелектуальної власності у кіберпросторі - це симбіоз суб'єктів, що вступають у правовідносини з приводу інтелектуальної власності, і доцільного способу зв'язку між ними з основою на суб'єктивних юридичних правах та обов'язках по відношенню до певних соціальних благ чи інтересів у кіберпросторі.

2. Надано перелік елементів структури відносин щодо дотримання права інтелектуальної власності у кіберпросторі. Ними є об'єкт правовідносин, їх суб'єкти та зміст. Відповідно, окрім традиційних для права інтелектуальної власності об'єктів, які умовно можна розділити на 4 групи (об'єкти авторського права, об'єкти суміжних прав, об'єкти промислової власності (сюди увійшли об'єкти патентного права і засоби індивідуалізації), нетрадиційні об'єкти, для цілей правового врегулювання відносин ІВ у кібернетичному домені, додано також безпосередньо інформацію, інформаційні системи й інформаційно-телекомунікаційні технології, інформаційні ресурси і продукти, доменні імена тощо. Суб'єктами ж відносин щодо дотримання права інтелектуальної власності у кіберпросторі є творці об'єктів права інтелектуальної власності, власники відповідних прав, правонаступники та інші особи, чия діяльність пов'язана із використанням, захистом результатів творчо-інноваційної діяльності, а також ті, хто вступає у такі відносини в процесі діяльності у кібернетичному просторі та безпосередньо Інтернеті - провайдери, оператори зв'язку, реєстратори, інтернет-реєстри тощо. Зміст правовідносин складають безпосередньо суб'єктивні права та юридичні обов'язки зазначених суб'єктів, де істотними складовими суб'єктивного права є правовикористання, правовиконання та правозахист. Відповідно, у віртуальному просторі суб'єктивне право проявляється у вигляді права-користування, -вимоги, -поведінки, - претензії . Також підкреслюється, що суб'єктивні права учасників

правовідносини у кіберпросторі розкриваються саме через власні дії користувачів, адже вони провокують виникнення, зміну та навіть припинення прав і обов'язків інших учасників взаємодії у кібернетичному домені, а не просто через обов'язки третіх осіб.

3. Зазначено, що визначення і правова кваліфікація вказаних елементів структури відносин щодо дотримання права інтелектуальної власності у кіберпросторі допоможе проаналізувати наявне законодавство та віднайти у ньому недоліки, і на їх основі - визначити тенденції подальшого удосконалення відповідного законодавства, розроблення нового, а також шляхи розвитку у відповідній галузі. В зв'язку із вказаним підкреслюється актуальність питання виявлення суб'єктів правопорушення щодо інтелектуальної власності у кібердоміні, адже діюче законодавство не дає чіткого розуміння щодо визначення відповідних осіб.
4. Зазначено, що на розвиток правового регулювання функціонування окремих інститутів інтелектуальної власності у кіберпросторі суттєвий вплив мало прийняття Бернської конвенції та "інтернет-договорів" ВОІВ, а також ряду НПА Європейського Парламенту та Ради (зокрема, Директиви 2001/29/ЄС про гармонізацію певних аспектів авторського права та суміжних прав у інформаційному суспільстві). Особливістю їх є те, що вони не містять визначення Інтернету як середовища використання досліджуваних творчо-інноваційних об'єктів, натомість використовується термін "цифрове середовище". Для України вирішальними у визначеному питанні став час, починаючи з 1991 р., коли держава стала незалежною і почала розробляти та впроваджувати в життя власне законодавство. Відповідно вказано на те, що в останні десятиліття в Україні відмітно активізувалися зусилля щодо входження "на рівних" до світових структур, особливо у частині ППВ, а сама держава є нині учасницею

більшості загально визнаних міжнародних конвенцій і договорів у даній галузі.

5. Підкреслено важливість знання особливостей генези правового регулювання функціонування інститутів права інтелектуальної власності загалом та у цифровому середовищі безпосередньо, адже саме на їх фоні можна розробляти та впроваджувати нове правове регулювання з урахуванням помилок та недосконалостей регулювання минулих років та навіть століть. Такі знання разом з науковими доробками вчених формують собою науково-теоретичне підґрунтя інтелектуальної власності та допоможуть в подальшому створити та впровадити більш дієве регулювання відносин у досліджуваній галузі.
6. Наголошено на важливості розуміння інтелектуальної власності як складової нематеріальних активів підприємства, у зв'язку із чим стає зрозумілим, що порушення авторських прав, прав на засоби індивідуалізації та інших прав інтелектуальної власності можуть стати причиною не лише грошових втрат, але втрати ділової репутації відповідного суб'єкта. Відповідно наголошується на важливості розуміння викликів, проблем та спірних питань правового регулювання відносин щодо дотримання права інтелектуальної власності у глобальних інформаційних та комп'ютерних мережах. Серед вказаних проблем найбільшою вбачається онлайн-піратство, особливо піратство програмного забезпечення, безпосередній продаж піратської продукції, фреймінг, глибокі посилання, метатегування; гостро стоїть також питання захисту патентів та боротьби із безпідставним використанням торгових марок, доменних імен (особливо в частині такого порушення як кіберсквоттинг) та інших засобів індивідуалізації учасників у цивільному обороті. Не менш актуальною в контексті даного дисертаційного дослідження є й

проблема використання технології штучного інтелекту, який відіграє значну роль у царині анонізації та автоматизації процесів у кіберпросторі, тим самим нерідко сприяючи правопорушним діям.

7. Підкреслено важливість розробки та впровадження ефективних нормативно-правових актів з урахуванням досвіду провідних країн світу. Юридичним особам наполегливо рекомендовано не тільки розвивати й контролювати свою інтелектуальну власність, але й вживати всіх доступних засобів для її захисту. Кінцевим користувачам кіберпростору - індивідам необхідно опанувати засади інформаційної та кібернетичної гігієни, а також не нехтувати всіма доступними засобами захисту своїх творінь й взрощувати в собі повагу до чужих здобутків у сфері творчості та інновацій. Тому важливу роль покладено й на суспільну обізнаність у боротьбі з проблемами порушень інтелектуальних прав у кіберпросторі. Таким чином для захисту прав інтелектуальної власності у цифровому середовищі потрібна участь всіх інформаційних суб'єктів - держави, суспільства, окремих індивідів, а також комплексний підхід до вироблення та впровадження засобів та методів захисту відповідних прав - і не тільки правових, а й соціальних та безпосередньо технологічних.
8. Вбачається за необхідне досягнення однорідності в законодавстві про права інтелектуальної власності, адже відповідні права мають територіальний характер, відповідно, і різні країни встановлюють різні вимоги та правила щодо захисту майнових та немайнових прав, термінів охорони, особливостей реєстрації тощо. Не менш проблемним є й питання відповідальності та ролі онлайн-посередників, як от реєстратори доменних імен, надавачі інтернет-послуг, провайдери тощо. Відповідальність таких осіб має залежити від їх обізнаності щодо наявного правопорушення, їх дій у даному

контексті, реакції на повідомлення про порушення і не тільки. Актуальність однорідності тут також поза сумнівів, адже різні юрисдикції по-різному визначають відповідальність онлайн-посередників.

Результати дослідження, викладені у Розділі 3, відображено у таких публікаціях автора: [144]; [342]; [330]; [153]; [161]; [1662]; [353]; [4228].

РОЗДІЛ 4. ЮРИДИЧНА КОМПАРАТИВІСТИКА ЯК МЕТОД ДОСЛІДЖЕННЯ ПРАВОВИХ ОСНОВ РЕГУЛЮВАННЯ ВІДНОСИН ДОТРИМАННЯ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ У КІБЕРПРОСТОРИ

4.1. Правові основи регулювання відносин дотримання права інтелектуальної власності у кіберпросторі в країнах ближнього та дальнього зарубіжжя

Законодавство більшості країн світу щодо інтелектуальної власності включає нормативно-правові акти, які захищають і забезпечують дотримання прав творців літературних творів, музики, винаходів, промислових зразків та інших робіт, об'єднаних поняттям «інтелектуальна власність». Здебільшого, у світі зазначений концепт включає "традиційні" для нас області на кшталт авторського права, патентів, товарних знаків і комерційної таємниці.

Захист інтелектуальної власності в різних державах, проте, може бути досить складним для обробки та виконання. На жаль, у багатьох країнах рівень охорони відповідних об'єктів та прав на них слабший, ніж у ЄС та США, що особливо негативно позначається на правах винахідників та авторів, а також інших правовласників, які хочуть зберегти свої об'єкти в таємниці та захистити їх.

Важливо відмітити, що у світі використовуються дві окремі системи авторського права: загального (її використовують Велика Британія та Сполучені Штати Америки), що гарантує тільки майнові права, а саме авторське право прирівняно до форми власності; та цивільного права (її використовують країни континентальної системи права, тобто європейські держави), яка охороняє і майнові, і немайнові права. В континентальній системі права ще декілька сторіч тому панували погляди німецьких філософів, зокрема, Канта, які трансформувалися у відповідні концепції,

відповідно до яких творча діяльність творця (автора) є невід'ємною від його особистості, є продовженням (відображенням) його особистості а тому їй має бути надана охорона на основі природної справедливості.

Різницю у підходах можна простежити й у термінологічному апараті. Так, поняття «*copyright*» (дослівно з англ. - право на виготовлення копій) є сталим для країн англо-саксонської системи, а «*droit d'auteur*» (безпосередньо авторське право) - для країн європейської системи. Але насуттєвіша різниця вбачається саме в тому, що для першого підходу (загальне право) характерне практичне ототожнення авторського права із формою власності, яку правовласник може використовувати будь-яким способом в комерційних цілях, і творцем якої може бути як фізична, так і юридична особа. Тобто саме майновий потенціал інтелектуальної власності має визначальне значення. Якщо ж ми говоримо про країни континентального права, то і тут право автора розуміється як право власності, але до уваги береться також не менш важливе інтелектуально-філософське розуміння щодо уже згаданої природної справедливості, коли твір - це вираженням особистості автора [5, с. 25-27].

Наразі "континентальний" підхід, за якого за авторами визнаються їх "моральні" права, є прийнятним для більшості країн світу, але Сполучені Штати, що приєдналися до Бернської конвенції, все одно більш схильні до концепції *copyright*. Що стосується авторки дисертаційного дослідження, то вона притримується підходу, що прийнятий у континентальній правовій системі права.

Відповідно далі буде зроблено аналіз найбільш вдалої правозастосовної практики та законодавства країн ЄС, СНД та безпосередньо США у галузі правового захисту інтелектуальної власності в кібернетичному просторі.

4.1.1. США

У Сполучених Штатах Америки питання правового забезпечення інтелектуальної власності взагалі і в кіберпросторі зокрема врегульовано як федеральним законодавством, так і офіційними нормативно-правовими актами окремих штатів, на нього також поширює свою дію набір міжнародних конвенцій, які адмініструються ВОІВ та СОТ. Так, згідно з п. 8, розділу 8, статті 1 чинної Конституції, Конгрес покликаний, у тому числі, "сприяти прогресу науки та корисних мистецтв, надаючи на обмежений термін авторам та винахідникам виключне право на їх відповідні твори та відкриття" [147]. Цей пункт як джерело повноважень законодавчого органу стосовно інтелектуальної власності називають «пунктом (застереженням, нормою) про патентне та авторське право» або «пунктом про інтелектуальну власність». Можна говорити про те, що ця норма фактично надає два різні повноваження:

1. гарантує творцям об'єктів інтелектуальної власності виключне право на результати їх творчості на певний термін - це основа нормативно-правового регулювання авторського права в США;
2. гарантує винахідникам виняткові права на їх відкриття на визначений термін - це основа американського патентного права.

Зазначимо націленість охорони відповідно до Пункту про інтелектуальну власність безпосередньо на авторів літературних творів та винахідників відкриттів. У цьому формулювання "твори авторів" можна розглядати як вказівку на належність результату творчості саме людині, а не штучному інтелекту, чи, наприклад, тварині.

Як зазначає Т.Т. Очоа, застереження про інтелектуальну власність не містить формулювання про гарантії щодо товарних знаків, тому об'єкти захищені пунктом (застереженням) про торгівлю. Дослідник також вказує на певну архаїчність і, тому, неясність вживаної термінології, наприклад, «корисні мистецтва» - це не художні твори, а роботи ремісників та інших

майстрів; «науки» відносяться не лише до областей сучасних наукових досліджень, а й взагалі до всіх наявних знань [245, с. 133].

Безпосередній федеральний Закон про авторське право або Розділ 17 Кодексу Сполучених Штатів (англ. *An Act for the general revision of the Copyright Law, title 17 of the United States Code, and for other purposes*, також - 17 U.S.C.) було прийнято в 1976 році, і він все ще перебуває у дії. Він складається з 13 розділів, присвячених предмету та обсягу АП, його терміну дії, праву власності та передачі авторських прав, повідомлення про АП, можливим порушенням у цій сфері та засобам правового захисту від такого, імпорту та виробничим вимогам, захисту мікросхем, оригінальних зразків, цифровим пристроям звукозапису та відповідним носіям, відеокліпам, окремі положення стосуються Бюро авторських прав, процедури суддівства по АП, систем захисту та управління правами.

Крім іншого, 17 U.S.C. містить положення про *fair use* (англ. "сумлінне використання") щодо репрографічного контенту. В даному випадку сумлінним використанням буде вважатися вільне фотокопіювання, якщо воно наслідує освітню мету, використовується для професійної підготовки суб'єктів або для проведення наукових досліджень (розділ (англ. *section*) 107); і якщо репрографічний матеріал буде використано як копію архівом або бібліотекою (розділ 108). При цьому розділ 108g чітко вказує на те, що відтворення або розповсюдження відповідного матеріалу не повинно мати на меті отримання комерційної вигоди при поширенні великої кількості екземплярів, які зроблені з одного і того ж матеріалу, а також без систематичного відтворення або поширення цих репрокопій.

Section 107 також декларує, що для визначення, чи є конкретне використання сумлінним, треба враховувати наступні фактори: мета і характер використання, наприклад, освітня або комерційна; обсяг та суттєвість використаної частини оригіналу; його характер, зокрема ступінь творчості; вплив використання ринку. Окремо зазначимо розділ 106, який

наділив правовласників п'ятьма винятковими правомочностями, а саме: правом на відтворення роботи, тобто її копіювання; правом створювати похідні твори, ґрунтуючись на версії-оригіналі; правом на публічне виконання роботи; правом на її публічний показ; та правом на публічне розповсюдження шляхом продажу та здачі у найм, прокат. Також вкажемо на норму 17 USC 801 (b) (1) (D), згідно з якою щодо потокової передачі музики (через цифрове радіо та сайти) судді у справах про роялті повинні максимально знизити будь-який негативний вплив на структуру задіяних галузей та на прийнятту галузеву практику з цього питання [131].

Через 19 років, до п'яти зазначених було додано виняткове право на виконання звукозапису за допомогою цифрового звуку. Це стало можливим завдяки поправкам до 17 U.S.C. §§ 106, 114-115 у вигляді Закону про право на цифрове виконання в звукозаписах 1995 року (англ. *Digital Performance Right in Sound Recordings Act*, також - *DPRA*). Він був прийнятий у зв'язку із відсутністю права виконання звукозаписів у оригінальній версії 17 U.S.C. та побоюваннями, що діджитал-технології замінять собою продаж творів у "фізичній" формі. Право на виконання звукозаписів за цим Актом обмежено передачею через "цифру", що й зумовило його "мізерність" у порівнянні із правами на виконання для інших типів творів. Цей закон, з урахуванням потенційного впливу послуг на продаж звукозаписів, встановив такі правила:

- мовні передачі без підписки не сплачують ліцензійні збори;
- якщо має місце неінтерактивна передача запису через всесвітню мережу, то сплаті підлягає ліцензійний платіж, суму якого встановлює Рада з авторського права;
- інтерактивні служби передачі через Інтернет мають укласти ліцензійну угоду із правовласниками.

При цьому на DPRA звернувся шквал критики, оскільки, згідно із новими положеннями, композитори, як і раніше, отримували набагато

більші права на виконання, ніж безпосередні виконавці творів. Також трирівнева система викликала негатив у мовних організацій, адже накладала більше навантаження на інтерактивні служби Інтернет-передачі [146, с. 466-467].

Окремо слід зазначити норму розділу 17 U.S.C. (§ 117) Закону США про авторське стосовно обмеження виключних прав на комп'ютерні програми, що зазнала певних змін. Поправки до попередньої версії документа включали, крім іншого, заміну терміна «законний власник» (комп'ютерної програми) на «власник», що призвело до зміцнення позиції постачальників програмного забезпечення, за якою клієнти не володіють таким програмним забезпеченням, а лише користуються ним за ліцензією. Загальна сутність норми 17 U.S.C. (§ 117) полягає в тому, що власник копії комп'ютерної програми, захищеної авторським правом, отримує право відтворювати її аз однієї з таких причин:

- використання, тобто установка на свій пристрій (його жорсткий диск) і запуск програми в оперативній пам'яті;
- копіювання ПЗ для ремонту або обслуговування пристрою зчитування, але з обов'язковою умовою про подальше знищення такої копії після завершення відповідних дій;
- створення бекапів, архівних копій на випадок втрати даних у разі пошкодження пристрою [150].

Також у 1992 році у 17 U.S.C. була додана глава 10 § 1001, відома як Закон про домашній аудіозапис (англ. *Audio Home Recording Act*, також - *AHRA*), що стосується цифрових пристроїв аудіозапису і носіїв. Відповідно до цього НПА можна випускати записи у особливих цифрових форматах типу Sony та Philips Digital Audio Tape без остраху отримати позов про порушення відповідних прав. Основні нововведення:

- введено в дію перший державний технологічний мандат, згідно з яким вироблені, розповсюджені та імпортовані цифрові

аудіозаписувальні пристрої, що продаються або виготовляються в США, а також імпортовані звідси, мають бути оснащені особливою Системою управління послідовним копіюванням (SCMS);

- на національному рівні встановлено гонорари за пристрої та носії, частина яких йде безпосередньо звукозаписуючому суб'єкту;
- встановлена заборона обходу технічних засобів захисту авторських прав, так само як і імпорт, розповсюдження або виробництво подібних інструментів для обходу SCMS, за що накладається штраф у розмірі до 25 доларів за 1 запис або до 2,5 тисяч доларів - за пристрій [196, с. 315-316].

Були внесені поправки також до 17 U.S.C. 101, 506, 507; 18 U.S.C. 2319, 2320; 28 U.S.C. 1498 шляхом прийняття в 1997 Закону про заборону "електронних" крадіжок (англ. *No Electronic Theft Act*, також - *NET Act*). Він передбачає кримінальне переслідування порушників авторських прав за певних обставин, навіть у разі коли таке правопорушення не приносить комерційної вигоди порушнику. Справа в тому, що до його прийняття, для складу злочину була потрібна наявність такої вигоди, відповідно, коли людина нелегально скачувала або завантажувала авторсько-правовий контент, вона не несла відповідальності. Наразі ж зловмисника чекає штраф або до 5 років позбавлення волі [196, с. 233, 316].

Наступним розгляду підлягають поправки до 17 U.S.C. §§ 108, 203(a)(2), 301(c), 302, 303, 304(c)(2) , відомі як Закон про продовження авторського права 1998 (англ. *The Copyright Term Extension Act of 1998*, також - *Sonny Bono Copyright Term Extension Act, CTEA*), або як «Закон про захист Міккі Мауса» (англ. *Mickey Mouse Protection Act*). Він, як і українське законодавство, наділяє автора майновими правами на строк усього його життя та 70 років після. У разі співавторства, термін інший: охорона передбачається протягом 120 років після створення роботи, або 95 років після її публікації - залежно від того, який термін підійде раніше [285]. У

зв'язку із цим варто ще раз звернутися до Пункту про інтелектуальну власність, що містить формулювання «обмежений час», відповідно до якого заборонено встановлювати строкові авторські права та патенти. Проте у справі *Eldred v. Ashcroft* (2003) Верховний суд США виніс ухвалу про те, що неодноразове продовження терміну дії авторського права не буде вважатися безстроковим авторським правом. В даному випадку мало місце відхилення від норм, передбачених СТЕА, і, отже, порушення конституційного формулювання про обмежений термін дії [175].

Також слід проаналізувати окремі положення так званого Закону про цифровий захист від крадіжки 1999 року (англ. *Digital Theft Deterrence and Copyright Damages Improvement Act*), який замінив собою норму 17 U.S.C. §§ 504(c), суттєво посиливши чинні цивільно-правові санкції за порушення авторських прав. Так, якщо попереднім законодавством було передбачено мінімальний штраф для правопорушника в обсязі 500 доларів за твір, а максимальний становив від 20 до 100 тисяч доларів за твір, що залежало від умисності діяння, то тепер пропонувалося встановити допустимий мінімум на рівні 750 доларів, а максимум - 30-150 тисяч доларів. Основною метою зазначеного є запобігання порушенням авторських прав у цифровому середовищі, особливо, піратства щодо ПЗ [158].

В 1998 році Закон про обмеження відповідальності за порушення авторських прав в Інтернеті (англ. *Online Copyright Infringement Liability Limitation Act*, також - *OCILLA*) додав собою 17 U.S.C. §§ 512. Він захистив постачальників онлайн-послуг (скорочено - OSP), тобто провайдерів та інших інтернет-посередників, від наслідків їх власних дій, що несуть пряме порушення авторських прав (при створенні несанкціонованих копій) та від потенційної вторинної відповідальності за протиправні дії третіх осіб. Вказане буде мати місце, якщо OSP дотримується 2 вимог, а саме:

- прийме та дотримуватиметься політики звернення та закриття облікових записів тих, хто повторно порушує АП;

- не буде втручатися в «стандартні технічні заходи», тобто ті, які власники авторських прав застосовують під час ідентифікації або для захисту творів. [234].

OSP також отримують імунітет від відповідальності за порушення авторських прав під час передачі, кешування, зберігання або посилання на нелегальний контент. У цьому випадку фінансової відповідальності не буде, але суд може зобов'язати OSP виконати деякі дії типу відключення доступу до спірного контенту. Додатково OSP, який вимагає такий імунітет, зобов'язаний призначити агента, якому надходитимуть повідомлення про порушення авторських прав, а також вчасно відповідати на запит розкрити відомості про юзерів-порушників. Також, коли ресурси OSP використовуються як сховище нелегального контенту, важливо, щоб постачальник послуг не отримувал у зв'язку із такими матеріалами фінансову вигоду, не знав про наявність таких матеріалів і після отримання повідомлення від правовласників вжив усіх необхідних заходів для видалення спірного контенту або заборонив доступ до нього [234].

Але, оскільки світ перейшов у епоху цифровізації, через кілька десятиліть вказаний НПА, який було прийнято ще у 1976 році, навіть з поправками перестав задовольняти повною мірою потреби регулювання у сфері інтелектуальної власності, особливо в кібернетичному просторі. Тому 14 травня 1998 року, з метою імплементації інтернет-договорів ВОІВ, Сполучені Штати ухвалили Закон про авторське право в цифрову епоху (англ. *Digital Millennium Copyright Act*, також - *DMCA*), який врахував сучасні технології в галузі копіювання та розповсюдження даних. Їм вводиться кримінальна відповідальність за виробництво та розповсюдження послуг та пристроїв, що допомагають обійти заходи захисту (підтримування в силі) авторського права (мова про так зване управління цифровими правами - англ. *digital rights management* або *DRM*). Кримінально-караним визнається і навмисний обхід контролю доступу

навіть у разі, якщо порушення самого авторського права не було здійснено де-факто. Важливим аспектом Акту слід вважати запровадження досить жорстких заходів покарання порушення авторських прав в Інтернеті. DMCA складається з 5 розділів (англ. *Titles*):

- Розділ I – *WIPO Treaties Implementation* (секції 101-105) – присвячений імплементації інтернет-договорів VOiB;
- Розділ II - *Online Copyright Infringement Liability Limitation* (секції 201-203) - вводить обмеження при накладенні відповідальності на інтернет-провайдерів та інших постачальників онлайн-послуг у разі порушення авторських прав під час здійснення певних видів діяльності;
- Розділ III - *Computer Maintenance Competition Assurance* (секції 301-302) містить виняток про те, коли відповідальність не накладається у разі створення копії комп'ютерної програми, якщо пристрій активується для проведення ремонту або обслуговування;
- Розділ IV - *Miscellaneous provision* (секції 401-407) - містить норми щодо функцій Бюро реєстрації авторських прав, недовговічних (тимчасових) записів, дистанційного навчання, обмежень ексклюзивних прав, у тому числі для бібліотек та архівів, веб-трансляції звукозаписів у всесвітній мережі, застосування колективних договорів при передачі прав на фільми;
- Розділ V – *Vessel Hull Design Protection Act* (секції 501-505) – містить положення про нову форму захисту конструкції корпусу судна [156].

Крім іншого відзначимо, що його параграф 1205 вказує на заборону скасування або ослаблення положень будь-якого федерального або штатівського закону щодо запобігання втручанням у приватне життя людини у зв'язку з використанням Інтернет-мережі. Одним із найважливіших положень DMCA варто вважати поширення охорони на всі об'єкти авторського права, розміщені в Інтернеті. Варто знати, що у разі,

якщо порушник прав доведе свою необізнаність у тому, що його дії є порушенням, то відповідальність накладатися не має. До об'єктів авторського права даним законом також висувається вимога про унікальність. У зв'язку із цим згадаємо про американський термін “*transformativeness*”, згідно з яким охорону отримують лише оригінальні твори, тоді як зображення або інші матеріали, що використовуються, наприклад, на веб-сайтах, тобто в кібернетичному просторі, зазвичай є копією або частиною оригінального твору. Примітною у зв'язку із зазначеним варто вважати справу 1991 року *Feist Publications v. Rural Telephone Service* 499 US 340, за якою суд виніс рішення про невизнання порушення авторського права щодо компіляцій або творів, які не відповідають оригіналу, відповідно, під дію авторського права підпадають лише оригінальні роботи, а не їхні копії, що розміщуються в Інтернет-мережі [182]. Також DMCA вніс поправки до DPRA, у тому числі змінивши вимоги та структуру державної ліцензії щодо цифрових звукозаписів.

У 2007 році була зроблена спроба внести поправки до DMCA і 17 U.S.C. 504(c)(2) шляхом внесення законопроекту про свободу та інновації, що відроджує підприємництво у Сполучених Штатах від 2007 року (англ. *Freedom and Innovation Revitalizing United States Entrepreneurship Act*, також - *FAIR USE Act*). Цей НПА мав би просувати інновації, заохочувати впровадження нових технологій та захищати права споживачів на сумлінне використання. Передбачалося, що споживачі, купуючи цифрові медіа, зможуть ширше використовувати їх для власної зручності без порушення авторських прав на такий твір. Цей документ містив два особливі положення: нове визначення порушення АП та внесення поправок до списку винятків для обходу АП. Законопроект передбачав шість поправок до DMCA щодо:

- Бібліотек та архівів. Їм дозволялося обходити авторські права при компіляції аудіовізуальних творів у бібліотечній колекції з метою викладання.
- Небажаного контенту. Акт дозволяв обхід за допомогою техзасобів ПЗ, що пропускає небажані матеріали на зразок наготи і подібного.
- Персональних мереж. 3 розділ документа дозволяв зберігання та передачу контенту особистою мережею, але прямо забороняв його завантаження у всесвітню мережу.
- Творів у складі суспільного надбання. Дозволялося без порушення АП використання матеріалів, що перебувають у суспільному надбанні (прикладом такого є Книги Google).
- Робіт та досліджень, що становлять суспільний інтерес. Дозволялося використати твір для цілей критики, коментарів, досліджень та подібного.
- Fair use для збереження твору. Передбачалося, що бібліотеки та архіви зможуть створювати копії творів, у яких їх значно обмежив DMCA [186].

Проте законопроект прийнятий не був, як такий, що провокував би злом авторсько-правових об'єктів і містить надто розмиті формулювання.

Раніше згаданий Пункт про торгівлю (комерцію) (англ. *Commerce Clause*) міститься в п. 3, розділу 8, статті 1 американської Конституції, відповідно до якого Конгрес наділений правом "регулювати торгівлю з іноземними державами, між штатами, та з індіанськими племенами" . Вважається, що зазначений Пункт протягом тривалого часу розглядався як надання ширших повноважень Конгресу та обмеження регулюючих повноважень штатів. При цьому значення терміна "торгівля" (комерція) є спірними, адже американська Конституція прямо не визначає його. Так, згідно з однією із точок зору, мова саме про торгівлю та обмін, згідно з іншою - про більш широке розуміння комерційних та соціальних відносин

між жителями різних штатів, що впливає на розмежування між федеральною владою та владою відповідних штатів [145].

Закон про розширення споживчого вибору та конкуренції в галузі бездротового зв'язку (англ. *Unlocking Consumer Choice and Wireless Competition Act*) прийнято у 2013 році на противагу правовому визначенню Бібліотеки Конгресу з питання обходу технологічних заходів доступу до захищеного авторським правом ПЗ на мобільних телефонах з метою підключення до бездротових телекомунікацій. Так зване "розблокування" передбачає зняття технічного обмеження або особливого ПЗ, "вшитого" в мобільні телефони виробником для обмеження їх використання в деяких локаціях або мережах [300].

Єдиний закон про комерційну таємницю (англ. *Uniform Trade Secrets Act*, також - *UTSA*) 1979 року (з поправками 1985 р.) був прийнятий з метою уніфікувати закони штатів з питань комерційної таємниці. Як уже згадувалося у попередніх розділах, такий об'єкт інтелектуальної власності часто стає об'єктом порушень в кібернетичному просторі, особливо в ІТ-сфері. Згаданий закон мав особливу важливість для тих підприємців, які працюють у двох та більше штатах. До кінця 2020 року його підписали 48 штатів, деякі з них змінили формулювання документа "під себе". *UTSA* складається з 12 розділів, причому розділ 1 містить використовувану термінологію; розділи 2–4 перераховують засоби правового захисту від порушень, зокрема це судова заборона, відшкодування збитків, а також гонорари адвокатів; розділи 5–12 містять додаткові положення щодо застосування НПА та його зв'язку з іншими документами. Основна суть Акту полягає у наданні правовласникам юридичної монополії терміном на 17 років в обмін на публічне розкриття винаходу. Цікаво і положення § 1.1, що розкриває суть "неналежних засобів" (англ. *Improper means*), що включають хабарі, крадіжку, введення в оману, порушення або всіляке

спонукання до порушення обов'язку зберігати секретність, а також шпигунство з використанням електронних та інших засобів [299].

Як свідчення бажання Конгресу слідувати нормам UTSA в 2016 році світ побачив Закон про захист комерційної таємниці (англ. *Defend Trade Secrets Act*, також - *TSA*), кодифікований в 18 USC § 1836, що і дозволяє власникам комерційної таємниці звертатися з позовом до федерального суду у випадку присвоєння такого об'єкта зловмисником. Він також розширив дію Закону про економічне шпигунство 1996 р. щодо кримінальної відповідальності за певні види незаконного присвоєння комерційної таємниці. Крім того, Акт наділив юридичним імунітетом корпоративних інформаторів [190].

Не менш важливо для цілей захисту об'єктів інтелектуальної власності в кіберпросторі забезпечувати належну охорону товарним знакам та доменним іменам. Так, у 1995 році було прийнято Федеральний закон про "розведення" товарних знаків (англ. *Federal Trademark Dilution Act*, також - *FTDA*). Цей НПА захищає відомі ТМ від використання, яке погіршує їхню дистинктивну здатність, навіть у разі, коли немає небезпеки змішання чи конкуренції. Надалі більшість положень цього Акту було заміщено нормами Закону про перегляд закону про "розведення" товарних знаків (англ. *Trade mark Dilution Revision Act*) 2006 року. "Розмиття" товарного знака, тобто зменшення його розрізняльності, має місце, коли його використання будь-ким, крім власника, погіршує розпізнавальну здатність знака, при цьому таке варто відрізнити від безпосереднього порушення прав на товарний знак. Останнє відбувається, коли особа інша, ніж власник ТМ, використовує позначення таким чином, що це може викликати плутанину у клієнтурі. До набрання чинності Законом про перегляд у 2006 році НПА 1995 р. поширював свою охорону тільки на «відомі» товарні знаки та захищав ТМ лише від «фактичного» розведення і навіть не від «заплямування». Останній термін застосовувався до випадків,

коли асоціація через схожість між новим знаком та відомим знаком завдає шкоди репутації останнього [181].

У жовтні 2006 року набув чинності *Trade mark Dilution Revision Act*, звільнивши правовласників оригінального товарного знака від доведення наявності «фактичного розведення». Також було розмежовано поняття «розмиття» та розведення за рахунок «заплямування» ТМ. Крім судової заборони як загальноприйнятого засобу правового захисту, власник знака може також претендувати на інші засоби, у тому числі відшкодування збитків, знищення контрафакту, оплати судових витрат тощо [296].

Щоб нівелювати недоліки FTDA, в 1999 році був прийнятий Закон про захист прав споживачів проти кіберсквотингу (англ. *Anticybersquatting Consumer Protection Act*, також - АСРА), він надав право звертатися з позовом у випадку, якщо хтось зареєструє, вестиме комерційну діяльність або інакшим чином буде використовувати доменне ім'я, подібне до ступеня змішування з торговою маркою іншої особи. Цей НПА кодифікований 15 U.S.C. § 1125(d) і своїм основним завданням має недопущення кіберсквотингу, тобто реєстрацію доменного імені з ТМ іншої особи, яка містить торговельну марку з метою подальшого перепродажу або недобросовісного використання. Норми АСРА наділяють власника товарного знака правом звернутися до суду з позовом до власника доменного імені, який:

- хоче одержати прибуток від використання знака;
- використовує доменне ім'я, яке є ідентичним або подібним до ступеня змішування зі знаком для товарів та послуг;
- використовує безпідставно товарний знак, пов'язаний із Червоним Хрестом або з олімпійським символом [283].

Процедура захисту своїх прав за АСРА буде розглянута у Розділі V цього дисертаційного дослідження як альтернатива процедурі UDRP. Варто

вказати, що критики цього закону вказують на його неглобальне охоплення та здатність обмежувати свободу слова.

У 2008 році було прийнято Закон про пріоритизацію ресурсів та організацію інтелектуальної власності (англ. *Prioritizing Resources and Organization for Intellectual Property Act*, також - *PRO-IP Act*), що суттєво збільшив обсяг відповідальності за порушення прав на патенти, ТМ та авторські права. НПА застосовується також у випадках, коли на споживача накладаються санкції за порушення, вчинене іншою особою. Актом були внесені зміни до попередніх документів щодо захисту інтелектуальної власності щодо цивільного та кримінального правозастосування, координації зусиль держорганів у галузі інтелектуальної власності, так само як і фінансування програм ІС Міністерства юстиції. Так, норми PRO-IP Act підвищили максимальний штраф за компіляції до 30 тисяч доларів США, окремо збільшивши обсяг штрафу за повторні порушення. За виробництво та продаж контрафактних товарів правопорушнику доведеться заплатити від 1 до 200 тисяч доларів США, за повторне діяння - від 1 до 2 мільйонів доларів. Міністерство юстиції отримало право на цивільну конфіскацію активів та обладнання, що використовується при скоєнні правопорушення з подальшим його продажем через аукціон. Також документ розширює список повноважень уряду щодо арешту та конфіскації незаконного обігу підробленої документації та пакувальних матеріалів. Закон забороняє експорт-імпорт товарів, що порушують авторські права (розділ 105). Ще він заснував Управління представника США із захисту прав інтелектуальної власності та посаду координатора із захисту прав інтелектуальної власності в Адміністрації президента [251].

Закон Орріна Г. Хетча - Боба Гудлатта про модернізацію музики (англ. *Orrin G. Hatch-Bob Goodlatte Music Modernization Act, MMA*) - це НПА 2018 року, що регулює питання АП для музики та аудіозаписів у зв'язку із розповсюдженням нових форматів та подібних технологій, таких як

цифрова потокова передача. Закон включає 3 окремі законопроекти, раніше внесені до Конгресу, що трансформувалися в окремі Розділи ММА:

- Розділ I – Закон про модернізацію музики. Направлений на покращення положення ліцензування та пов'язаних з ним платежів, які виплачуватимуться з урахуванням послуг потокового мультимедіа. Три основні положення цього розділу:
 - a. потрібно заснувати некомерційне керуюче агентство, яке створило б базу даних власників ліцензій на механічне відтворення музичних робіт, оскільки фактичне виконання та запис ведуться за іншою ліцензією. Також цей орган встановить загальні ставки роялті під час використання музичних сповіщень для потокових сервісів;
 - b. композиторам та авторам текстів гарантується виплата частини ліцензійних відрахувань за механічне відтворення їх робіт у фізичному чи цифровому вигляді за прописаною у договорі ставкою;
 - c. вносяться зміни до судової процедури у спрах щодо ставок роялті, а саме для таких справ буде призначено випадкового суддю зі складу Окружного суду Сполучених Штатів Південного округу Нью-Йорка [132].

Також цього разу включили положення Закону про чесну гру та справедливу оплату (англ. *Fair Play Fair Pay Act*) щодо способів виплати ліцензійних відрахувань наземними радіомовними компаніями та службами потокової інтернет-передачі [132].

- Розділ II – Закон про компенсацію артистам спадщини за їхні пісні, послуги та важливий внесок у суспільство. Він декларує віднесення аудіозаписів, випущених до 1923 р. до громадського надбання через 3 роки після набуття чинності цим законом (1 січня 2022 року), записів 1923-1956 років - протягом наступних десятиліть [132].

- Розділ III - Закон про розподіл коштів для музичних продюсерів. Він припускає, що некомерційна організація SoundExchange, яка розподіляє гонорари за звукозаписи, також передаватиме частину гонорарів продюсерам, мікшерам, звукооператорам, якщо вони брали участь у творчому процесі зі створення звукозапису [132].

США також відзначилися рядом законопроектів, які, хоча й не набули законної сили і не були введені в дію, але містять досить важливі, на нашу думку, положення, які б могли бути взяті за основу при роботі над національним законодавством в галузі захисту об'єктів інтелектуальної власності у кібернетичному просторі. Так, проект Закону про захист прав інтелектуальної власності (англ. *Intellectual Property Enforcement Act*, також - *S.2317*) 2007 року, у разі прийняття, повинен був посилити дію законів про інтелектуальну власність у США через внесення поправок до розділів 17-18 Кодексу Сполучених Штатів та Закону про товарні знаки 1946 року. Першочерговим завданням Акту було надати можливість Мін'юсту звертатися до суду з цивільними позовами проти веб-ресурсів-файлообмінників, і, надалі, присуджувати власнику відповідних авторських прав певне відшкодування (реституцію), обсяг якого визначався секцією 504, а еквівалентна йому сума - секцією 3663 3(6) (B) Розділу 18. Також законопроектом пропонувалося скасувати секцію 509 щодо конфіскації та реституції. Акт передбачав й створення особливого підрозділу, який допомагав би відділу з комп'ютерних злочинів та інтелектуальної власності Міністерства юстиції. Щодо поправок до Закону про товарні знаки, то проект пропонував надання додаткового захисту для вилучених даних про авторські права та товарні знаки з метою забезпечення нерозголошення конфіденційних даних [206]. Необхідної підтримки, зрештою, даний НПА не отримав і введений в дію не був.

У 2011 році Палатою представників Сполучених Штатів було прийнято до розгляду особливий законопроект «Про протидію онлайн-

піратству» (англ. *Stop Online Piracy Act*, також - *H.R. 3261*, скорочено – *SOPA*). Його метою був захист інтелектуальної власності творців контенту в Інтернеті від крадіжки для заохочення створення нових робіт та досліджень, що тим самим сформує більше робочих місць у країні. При цьому відповідачами у справах про інтернет-порушення відповідних прав визнавалися посередники, тобто ті, хто розміщує контент, забезпечує електронну торгівлю ним тощо. Другою метою SOPA декларує захист від підроблених (контрафактних) ліків, оскільки споживачі відповідних товарів не завжди могли виявити факти шахрайства на веб-сайтах, де замовляли продукцію. Варто зазначити, що цей документ, у разі прийняття, розширив би можливості національних правоохоронних органів та місцевих правовласників у боротьбі із нелегальним контентом у Мережі, торгівлею інтелектуальною власністю та контрафактом [276].

Законопроект вимагав, щоб будь-який учасник діяльності в Інтернеті (від провайдера до рекламодавця) за будь-яким зверненням правовласника інтелектуальної власності негайно припинив би надання послуг веб-ресурсу-пірату та взаємодію з ним, наприклад, шляхом відключення його від каналів оплати за використання матеріалів тощо. При відмові від зазначеного, такі учасники інтернет-діяльності автоматично прирівнювалися б до співучасників правопорушення. Відповідно до *H.R. 3261* також визнавалося кримінально-караним діянням несанкціоноване потокове мовлення або інше поширення захищеного авторським правом матеріалу, покарання в даному випадку склало б 5 років ув'язнення. Імунітет від судового переслідування в даному випадку отримав би кожен, хто добровільно та з власної ініціативи ввів заходи проти інтернет-порушників [276]. SOPA так і не отримав належної підтримки і не був прийнятий, адже багато його противників впевнені в порушенні таким Актом Першої поправки до американської Конституції, введенні ним

інтернет-цензури, і, що головне, обмеження свободи слова та можливості розвитку Всесвітньої Мережі.

Не менш негативний відгук отримав і законопроект Про запобігання реальним мережевим загрозам економічному творчому потенціалу та крадіжці інтелектуальної власності (англ. *Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act*, також - *Protect IP Act*, *Protect Intellectual Property Act*, скорочено - *PIPA*). Цей документ 2011 року пропонував надати американському уряду та власникам авторських прав спеціальні додаткові інструменти для блокування веб-ресурсів із шахрайським змістом, контрафактною продукцією та таких, що порушують авторські права. Карними за цим Актом визнавалися дії щодо поширення підробок, незаконно виконаних копій, а також виробництво та використання технологій подолання технічних засобів захисту авторських прав. Веб-сайти, що сприяють подібним діям, також визнавалися порушниками. Його основна націленість – зарубіжні “піратські” ресурси. Постраждалими особам та американським офіційним органам РІРА дозволяла звертатися до суду з клопотанням про конфіскацію власності порушника навіть без попереднього розслідування, або у відсутності власника таких ресурсів. Щойно санкцію суду отримано, дозволено вимагати від фінансових підприємств припинити грошові перекази, від провайдерів та подібних осіб – видалити посилання на зловмисницький ресурс. В результаті, доступ до такого сайту-порушника буде можливий тільки через його IP [250].

На противагу двом попереднім досить жорстким проектам НПА наприкінці 2011 року до Конгресу було внесено на розгляд законопроект Про онлайн-охорону та правозастосування у цифровій торгівлі (англ. *Online Protection and Enforcement of Digital Trade Act*, також - *OPEN Act*). Головна його відмінність у порівнянні зі згаданими попередниками полягала в тому, що він не допускав блокування вебсайтів, вилучення доменів і блокування

доступу відвідувачів веб-ресурсу з метою недопущення дискримінації інтересів користувачів. Головним завданням цього НПА було визнано припинення (недопущення) отримання незаконної вигоди несумлінними власниками вебсайтів. Правовласникам у зв'язку із зазначеним дозволялося вимагати накладення заборони на проведення фінансових операцій ресурсами-порушниками та отримання ними прибутку від розміщення у себе реклами. У той же рік було внесено на розгляд і законопроект про обмін і захист кіберрозвідувальної інформації (англ. *Cyber Intelligence Sharing and Protection Act*, також - *CISPA*), метою якого була протидія кіберзлочинності, завдання ж полягало у спрощенні процедури обміну відомостями про кіберзагрози між урядом та комерційними структурами [111, с. 105].

Закон про аташе з інтелектуальної власності (англ. *Intellectual Property Attache Act*, також - *IPAA*) був оприлюднений у липні 2012 року в продовження провального SOPA. Його метою було розширення присутності так званих аташе з інтелектуальної власності по всій земній кулі. Ці суб'єкти виступили б «дипломатами» з інтелектуальної власності для США, тим самим заохочуючи інші держави забезпечувати дотримання законів про авторське право. Таких аташе представляло б Міністерство торгівлі [227].

З точки зору науки варто також розглянути проект Закону про дослідження (англ. *Research Works Act*, також - *102 HR 3699*) 2011 року. У ньому містилися норми про заборону встановлення відкритого доступу на дослідження, що фінансуються із федерального бюджету. Таким чином Акт скасовував чинну Політику публічного доступу Національних інститутів охорони здоров'я Сполучених Штатів, згідно з якою дослідження, що фінансуються платниками податків, були доступні в Мережі Інтернет на безкоштовній основі. Відповідно такі платники, які раніше заплатили за саме дослідження, змушені були б платити ще раз, але вже за те, щоб

ознайомитися з результатами цього дослідження. Закон прийнятий не був, інакше він би також істотно обмежив обмін науковими даними [262]. Зазначена Політика публічного доступу NIH – це так званий мандат на відкритий доступ 2004 року, яка набула чинності у 2008 році. Згідно з нею, наукові роботи, дослідження з яких фінансує американський Національний інститут охорони здоров'я, повинні бути розміщені через спеціальний репозиторій PubMed Central, що самоархівується, на безкоштовній основі протягом року після публікації. Авторські права при цьому зберігаються, а розповсюдження робіт здійснюється за ліцензіями Creative Commons.

Зазначимо, що чинні норми та правила США щодо інтелектуальної власності взагалі і в кіберпросторі зокрема досить широко і добре опрацьовані. Взагалі щодо об'єктів інтелектуальної власності діють досить жорсткі правила з експорту-імпорту відповідних продуктів, для деяких із них потрібна експортна ліцензія перед відправкою, і навіть не у всі країни може бути здійснено продаж. Також в країні ведуть активну діяльність із захисту інтелектуальної власності взагалі та безпосередньо у кіберпросторі спеціальні органи, про які піде мова далі.

Завдання щодо видачі американських патентів та реєстрації торгових знаків покладено на спеціальне федеральне агенство - Відомство США з патентів та товарних знаків (англ. *United States Patent and Trademark Office*, також - *USPTO*). До його функцій віднесено надання консультацій президенту та іншим урядовим структурам у відповідній сфері, а також просування охорони інтелектуальної власності по всій земній кулі. Організація співпрацює з іншими агенціями з метою забезпечення дотримання положень про інтелектуальну власність в угодах про вільну торгівлю та інших міжнародних договорах. USPTO веде і просвітницьку діяльність, розробляючи та впроваджуючи освітні програми з метою зміцнення поваги до відповідних результатів творчо-наукової діяльності. Одним із основних пріоритетів органу названо забезпечення збереження за

США лідерства у сфері інновацій, особливо, що стосується штучного інтелекту [291].

Відділ комп'ютерної злочинності та інтелектуальної власності (англ. *Computer Crime and Intellectual Property Section*, також - ССІРС) займається кримінальними справами з розслідування комп'ютерних злочинів та порушень прав інтелектуальної власності. Відомство здійснює пошук та збір цифрових доказів фактів скоєння таких злочинів у комп'ютерній сфері та мережах, а також надає технічні та юридичні консультації як національним агенствам, так і по всьому світу. Методи, які використовує ССІРС, включають, в себе, крім іншого: ведення високоефективних та конфіденційних розслідувань та судових переслідувань; просування міжнародної політики щодо забезпечення дотримання законів про комп'ютерні злочини та інтелектуальну власність поза територією США; проведення цифрового слідчого аналізу на найвищому рівні; розробку та просування політик і нормативно-правових актів щодо злочинів, пов'язаних із комп'ютерами та інтелектуальною власністю [126].

Комп'ютерна команда екстреної готовності США (англ. *United States Computer Emergency Readiness Team*, також - *US-CERT*) покликана проводити аналіз мереж та цифрових медіа та мінімізувати кількість кіберзагроз та інших уразливостей, вона також займається інформуванням про вказані загрози та координує діяльність з реагування на кіберінциденти. Цей орган є частиною Агентства кібербезпеки та безпеки інфраструктури (*Cybersecurity and Infrastructure Security Agency*, також - *CISA*) Міністерства внутрішньої безпеки Сполучених Штатів. *US-CERT* виступає партнером у відносинах останнього з державним та приватним секторами. Таким чином, головне завдання Команди – захист американської національної інтернет-інфраструктури. Згадане Агенство *CISA* відповідає за ведення діяльності щодо забезпечення розуміння, управління та зниження ризиків для кібернетичної та фізичної інфраструктури США. Воно забезпечує безпеку

та відмовостійкість критичної інфраструктури для всіх американців. На CISA покладено функцію забезпечення своєчасно обміну актуальними відомостями між федеральними та нефедеральними суб'єктами та приватним сектором. До її складу також увійшли відділи кібербезпеки, безпеки інфраструктури, екстреного зв'язку, інтегрованих операцій, національний центр з управління ризиками, національна гвардія аварійних технологій та інші органи, що відповідають за забезпечення порядку в кіберпросторі та інформаційному середовищі [127].

Таким чином, патенти, авторські права, комерційні таємниці та товарні знаки - це 4 головні типи об'єктів інтелектуальної власності в американському праві, вони одночасно є цінними активами для кожної компанії, а тому відносини щодо їх створення та використання повинні бути детально врегульовані, а самі об'єкти - якісно захищені. У цій державі зазначені питання регулюється як федеральним законодавством, так і законодавством штатів, на них також поширює свою дію система загальноновизнаних міжнародних конвенцій. З урахуванням вищезгаданого аналізу основних американських НПА можна з упевненістю заявити про те, що регулювання правовідносин у сфері інтелектуальної власності взагалі, і в кіберпросторі зокрема у Сполучених Штатах по праву можна назвати одним з найврегульованіших і всеосяжних. Це законодавство передбачає як зрозумілу для більшості цивільну та кримінальну охорону, так і прикордонний захист прав інтелектуальної власності. У країні діють USPTO та агентства-партнери, які надають онлайн-інструментарій та необхідні відомості з питань захисту та забезпечення дотримання прав інтелектуальної власності.

Американський правовласник несе відповідальність за цивільне правозастосування своїх прав інтелектуальної власності та може повідомити про її крадіжку в режимі онлайн шляхом звернення до веб-ресурсу Національного координаційного центру з прав інтелектуальної

власності. Автор дисертаційного дослідження вважає за доцільне для українських нормотворців перейняти досвід американських колег у регулюванні правовідносин, пов'язаних із захистом та здійсненням прав власників інтелектуальної власності в кібернетичному просторі.

4.1.2. Європейський Союз та країни Європи

Законодавство країн Європи є досить вдалим та логічним. Окремі Директиви ЄС присвячені саме питанням регулювання відносин інтелектуальної власності у кіберпросторі. Але перш, ніж перейти до розгляду такого правового масиву, звернемо увагу на певні особливості захисту відповідних прав на європейському континенті.

Як вже було зазначено вище, є два підходи до розуміння авторського права, і сьогодні більшість людей ототожнюють поняття *copyright law* із авторським правом у розумінні континентальної правової сім'ї. Відповідно до згаданих німецьких філософських поглядів автор мав право на охорону результату своєї творчості завдяки природній справедливості, бо відповідна творчість - це невіддільний елемент його особистості. Дана концепція дала початок формуванню так званої доктрини моральних прав авторів («*droit moral*») у 19 столітті, відповідно до якої особисті немайнові права автора отримали своє офіційне закріплення як у локальних НПА, так і у міжнародних правових актах. Англо-американська система, яка базувалася на Статуті королеви Анни, мала на меті комерційне використання результатів творчості автора. Різниця у концепціях результувала у різних підходи до вирішення питань щодо об'єктів та суб'єктів авторського права, обсягу їх правомочностей та моменту виникнення відповідних прав. Так, законодавство країн загального права охороняють за допомогою "копірайту" не тільки літературні та твори мистецтва, ає й фоно, телепрограми тощо. При цьому до першої групи об'єктів, як відомо, висувається вимога щодо оригінальності, а до другої - ні. Також

англосаксонські держави вимагають фіксації правового об'єкта на матеріальному носії, інакше правова охорона не буде надана. Також щодо суб'єктного складу, автором твору в даному випадку може бути визнана юридична особа, а особисті немайнові авторські права можуть бути захищені саме в порядку застосування загального права. Майнові ж права дають автору виключну монополію на певні види дії з відповідним об'єктом творчості.

Щодо країн континентальної системи, то тут об'єктом авторського права вважається тільки результат інтелектуальної творчої діяльності, який є оригінальним, при чому в окремих випадках його фіксування на матеріальному носії задля отримання охорони не вимагається. У вказаних державах автором твору може бути лише фізична особа, що своєю творчою працею і створила відповідний результат. Особисті немайнові "моральні" права автора визнаються невід'ємними від особи автора, невідчужуваними, а перелік майнових - не є вичерпним. Саме ж авторське право виникає в момент створення відповідного твору і не потребує попереднього виконання ніяких формальностей [5, с. 26].

Слід розуміти, що коли ми сьогодні говоримо про авторське право у розумінні загальної системи права, то маємо на увазі надання відповідного захисту опублікованому чи неопублікованому оригінальному творінню і матеріальним правам автора. У цивільно-правовому ж розумінні, беруться до уваги саме "моральні", невідчужувані права, а відповідне авторське право невіддільне від особи творця. Тут ми маємо справу із об'єктом творчості як вираженням особистості автора, а тому відповідні права і мають бути захищені.

"Континентальний" підхід, за якого за авторами визнаються їх "моральні" права, є приятним для більшості країн світу, але Сполучені Штати, що приєдналися до Бернської конвенції, все одно більш схильні до концепції *copyright*. Що стосується авторки дисертаційного дослідження, то

вона притримується підходу, що прийнятий у континентальній правовій системі права.

Далі детально розглянемо законодавство Євросоюзу щодо забезпечення прав інтелектуальної власності та безпосередньо зазначеного "континентального" авторського права у кіберпросторі.

Авторське право ЄС на даному етапі розвитку продовжує уніфікувати та гармонізувати права інтелектуальної власності держав-членів Союзу. У зв'язку із зазначеним, Євросоюзом були прийняті директиви, які зобов'язують держави-члени насамперед досягти певних цілей за допомогою реалізації їх у своїх національних законодавствах. Такий стан речей підтримується і рішеннями Суду ЄС. Так, всі члени підписали Бернську конвенцію 1886 р. і посилено дотримуються її, так як це - обов'язкова вимога для вступу і перебування в Союзі. Першим актом серед інших варто назвати *Directive 91/250/EEC on the legal protection of computer programs* (також – *Computer Programs Directive* – Директива про захист комп'ютерних програм). Пізніше документ було змінено, і сьогодні остання його версія має назву 2009/24/EC. У статті 1 цього НПА зазначено норму про необхідність охорони комп'ютерних програм як літературних творів у розумінні Бернської конвенції, при цьому саме поняття «комп'ютерні програми» також поширюється на підготовчий проектний матеріал софту. Також п.2 статті 7 декларує вимогу про конфіскацію незаконних копій комп'ютерної програми по законодавству відповідної держави-члена [170].

Директива 93/98/ЄЕС від 29 жовтня 1993 р., згодом замінена директивою 2006/116/ЄС, мала на меті забезпечення єдиного терміну дії авторських та суміжних прав на всій території Союзу. Оскільки Бернська конвенція встановлювала мінімальні терміни охорони, ЄС збільшив її до 70 років від дня смерті автора (це так званий *post mortem auctoris*) незалежно від дати першої публікації твору, про що йдеться у Статті 1 Директиви. Для

суміжних прав термін охорони встановлено на рівні 50 років з обчисленням дати початку дії у відповідності зі Статтею 3 [169].

Директива 2001/29/ЄС щодо гармонізації деяких аспектів авторського права та суміжних прав в інформаційному суспільстві в параграфі 9 преамбули вимагає, щоб така гармонізація ґрунтувалася на високому рівні захисту, адже зазначені права мають вирішальне значення для інтелектуальної творчості, а їхня безпосередня охорона потрібна для розвитку творчості на користь авторів, виконавців, споживачів та інших осіб. Також проголошується, що інтелектуальна власність є невід'ємною частиною власності. Статті 2–4 визначають виняткові права, при цьому право на репродукцію відокремлено від права на повідомлення для загального відома та доведення до загального відома, до останнього документ включає публікацію контенту в Інтернеті. Стаття 5 перераховує винятки з авторського права, віддаючи їх на відкуп державам-членам. Але один виняток залишається обов'язковим для всіх учасників - короткочасне чи випадкове копіювання як частина мережі передачі чи легального використання [166].

Таким чином інтернет-провайдерів звільнили від відповідальності за переданий контент, навіть якщо він нелегальний. П. 2-3 статті 5 дозволяють державам-членам робити винятки у правах на репродукцію та на доведення для загального відома у певних випадках. Стаття 6 директиви зобов'язує членів забезпечити належний правовий захист від навмисного обходу технологічних заходів захисту об'єктів авторського права, у тому числі від несанкціонованого копіювання. Таким положенням директива показала себе суворішим документом у порівнянні із DMCA, який забороняє тільки обхід. Також згідно з параграфом 52 преамбули, охорона за допомогою технічних засобів для забезпечення безпечного середовища під час надання інтерактивних послуг повинна здійснюватися таким чином, щоб широка

публіка за бажання могла отримати доступ до об'єктів, що охороняються, з будь-якої точки і в будь-який час [166].

Директива 96/9/ЄС про правову охорону баз даних як ще одного важливого цифрового об'єкта, що нерідко використовується у кіберпросторі, була націлена на гармонізацію обробки БД згідно із авторським правом та правом *sui generis* для авторів тих БД, на які АП не поширюється. При цьому визначення зазначеному об'єкту дає Стаття 1(2), розуміючи під ним "добірки незалежних творів, даних або інших матеріалів, розташованих систематичним або методичним способом та індивідуально доступними через електронні та інші засоби". Щодо неелектронних БД, то про них сказано у параграфі 14 преамбули. При цьому, згідно з параграфом 23, комп'ютерні програми для створення баз не є базами даних [173].

Директива 2004/48/ЄС щодо реалізації прав на інтелектуальну власність доповнила собою норми Угоди ТРІПС щодо правозастосування. Так, останній документ встановлює кримінальне покарання, а перший стосується саме цивільно-правових засобів захисту. Члени Союзу зобов'язані використовувати ефективні та дієві засоби правового захисту та санкції проти контрафакту та піратства. Відповідно до статті 1 предмет ведення Директиви – це захист прав інтелектуальної власності, у т.ч. промислової власності. Заходи та засоби відновлення порушених прав як сфера дії документа згадані у Статті 2, що вимагає від них бути справедливими, збалансованими та стримуючими від правопорушень. Таким чином, має місце дублювання норми статті 41 Угоди ТРІПС. Засоби правового захисту мають бути доступні для авторів та інших суб'єктів, які правомірно використовують об'єкт інтелектуальної власності. Стаття 6 дозволяє учаснику процесу звернутися за доказами щодо наявного порушення, якщо такі розумно доступні та достатні для підтримки позову. При порушенні в комерційних масштабах члени ЄС роблять все необхідне для надання фінансових та інших документів та заарештовують майно

порушника, при цьому забезпечуючи захист конфіденційних даних (Статті 6 та 9) [168].

Стаття 7 дозволяє проводити заходи щодо забезпечення доказів також до початку судового розгляду, серед яких фізичний арешт та арешт контрафакту і матеріалів для його провадження та розповсюдження. Параграф 2 преамбули гарантує винахіднику та творцю отримання законного прибутку від свого інтелектуального об'єкта. Широке поширення робіт, тим не менш, не повинно перешкоджати свободі вираження думок, переміщенню інформації або захисту персональних даних, у тому числі у всесвітній мережі. Параграф 9 говорить про те, що повсюдне використання Інтернету дає можливість зловмисникам миттєво розповсюджувати піратську продукцію по всій земній кулі. Тому застосування матеріального права інтелектуальної власності має бути ефективним внаслідок певних захисних дій на рівні Співтовариства, для чого особливо важливим є зближення законодавства держав-членів у цьому питанні [168]. Таким чином, можемо зробити висновок, що мета цієї директиви - це регулювання захисту прав інтелектуальної власності, а не самих таких прав. Також наголосимо, що документ встановив додаткові заходи щодо захисту цифрових авторських прав, при цьому локальні НПА країн-членів в інших областях не були затронуті.

Директива 2010/13/ЄС про погодження деяких положень, встановлених законом, постановами або адміністративними актами в державах-членах, що стосуються надання аудіовізуальних медіапослуг (також - Директива про аудіовізуальні медіапослуги, англ. *Audiovisual Media Services Directive*) встановила принципи безпечного та відкритого аудіовізуального медіа-ландшафту в європейських країнах: її норми вимагають від постачальників медіа-послуг надавати особливий захист від шкідливого контенту неповнолітнім людям, а також зробити все необхідне, щоб дозволити кожному користуватися аудіовізуальними медіа-послугами.

Таким чином держави-члени можуть забезпечити доступність головних подій у безкоштовному ефірі для свого народу. Основним принципом НПА є принцип країни походження, що дозволяє вести транскордонне розповсюдження телеканалів. Зазначене дозволить забезпечити легкодоступність контенту для широкої аудиторії, тим самим стимулюючи творчість з метою економіки та культурної різноманітності на європейському просторі [146].

Директиву переглянули у 2018 році. У статті 1 нового документа надано визначення аудіовізуальних медіапослуг як послуг, націлених (повністю або в частині) на надання публіці програм під редакційною відповідальністю постачальника медіа-послуг для інформування, навчання або розваг через мережі електронних комунікацій. Подібною послугою варто вважати телевізійні передачі та інші аудіовізуальні медіа-послуги на запит. Стаття 7 оновленого акта вимагає від усіх держав-членів створити онлайн-контактний пункт для надання інформації та отримання скарг з будь-яких питань доступності контенту, і він має бути єдиним, загальнодоступним та легкодоступним, особливо для людей з обмеженими можливостями. Стаття 5 зобов'язує країни Союзу надати гарантії щодо своїх постачальників медіа-послуг, які повинні забезпечити легкий, прямий та постійний доступ для набувача послуги до таких відомостей як (це мінімальна вимога): назва, географічна адреса розташування, контакти для швидкого зв'язку, вказівка на державу -член, якому постачальник підпорядковується, і навіть на компетентні регулюючі чи наглядові органи [146].

Директива 2014/26/ЄС про колективне управління авторськими та суміжними правами та багатотериторіальне ліцензування прав на музичні твори для онлайн-використання на внутрішньому ринку в параграфі 38 преамбули зазначає, що інтернету не відомі межі, а тому має місце фрагментація онлайн-ринку музичних послуг у ЄС, та й сам єдиний

цифровий ринок не повністю сформовано. І особливо помітна фрагментація європейського цифрового ринку музичних онлайн-сервісів, при цьому попит на доступ до цифрового контенту і пов'язаних з ним сервісів дуже високий. Вирішити такі проблеми, згідно з НПА, покликані організації з колективного управління правами [172].

Важливими є і документи щодо торгових марок. Так, Директива (ЄС) 2015/2436 про зближення законів держав-членів, що стосуються товарних знаків у Статті 1 вказує сферу своєї дії, а саме індивідуальні та колективні товарні знаки, гарантійні та сертифікаційні тощо. Як зазначено в параграфі 6 преамбули, Комісія вважає за необхідне, з метою задоволення сторін та забезпечення якісних та оптимізованих систем реєстрації знаків, модернізувати систему реєстрації ТЗ в ЄС та адаптувати її до епохи Інтернету [161]. Іншим документом з цього питання є Регламент (ЄС) 2017/1001 про товарний знак Європейського Союзу. Важливою для цілей цього дослідження є Стаття 113 про те, що рішення Відомства з товарних знаків мають бути доступні онлайн для ознайомлення та консультацій згідно з принципами прозорості та передбачуваності. При цьому кожна зі сторін розгляду, щодо якого винесено рішення, вправі вимагати видалення будь-яких персональних даних, включених у рішення [255].

Регламент (ЄС) 2017/1128 про транскордонну переносимість послуг онлайн-контенту на внутрішньому ринку заборонив геоблокування онлайн-контенту в ЄС за дотримання деяких вимог. Він гарантує необмежений доступ до платного підписного онлайн-контенту кожному європейцю незалежно від місця його перебування на території Союзу. При цьому висувається вимога про "тимчасовість" такої присутності, що зобов'язує постачальника контенту забезпечити підписникам транскордонну переносимість, без стягнення додаткових зборів. Таке обмеження не поширюється на безкоштовні пропозиції постачальника. НПА також

встановив правила щодо мінімізації обсягів збору персональних даних користувачів з метою ідентифікації країни-члена [256].

У Статті 1 Регламент переносимості визначає предмет та сферу застосування. Стаття 2 визначає термінологію документа, а статті 3-9 містять основні положення Регламенту. Так, статті 3-4 передбачають зобов'язання постачальника послуг забезпечити транскордонну переносимість послуг онлайн-контенту та визначають місце проживання одержувача такої послуги як місце її надання або як місце доступу та використання при знаходженні одержувача тимчасово в іншій державі-члені. Стаття 5 наділяє постачальника послуг онлайн правом перевірки такої країни. У 6 статті описано спеціальне правило про транскордонну переносимість безкоштовних послуг онлайн-контенту. Стаття 7 регулює договірні положення між правовласниками та постачальником послуги, а також між ним та споживачем. Стаття 8 захищає особисті дані одержувачів послуг [256]. Таким чином Регламент - один із засобів створення загальносоюзного єдиного цифрового ринку, заснованого на якісному доступі до онлайн-товарів та послуг, оптимальних умовах для цифрових мереж та цифрової економіки. При цьому Єврокомісія під таким єдиним цифровим ринком розуміє саме європейський, де фізособи та юрособи зможуть безперешкодно отримувати доступ вести свою онлайн-діяльність на підставі чесної конкуренції та високого рівня захисту персональних даних споживачів.

Директива (ЄС) 2018/1972 про запровадження Європейського кодексу електронних комунікацій у Статті 1 зазначає, що присвячена гармонізації регулювання електронних комунікаційних мереж, послуг, пов'язаних із ними засобів та деяких аспектів термінального обладнання в усіх країнах Європейського Союзу. Стаття 2 дає визначення електронної комунікаційної мережі, під якою розуміє системи передачі та обладнання для комутації та маршрутизації, так само як інші ресурси для передачі

сигналів через електромагнітні та подібні засоби, в т.ч. супутникові мережі, мережі фіксованого та мобільного зв'язку, куди входить і Інтернет тощо. При цьому електронна комунікаційна послуга є послугою, зазвичай на платній основі, через згадані електронні комунікаційні мережі, за винятком тих, які відносяться до редакційного контролю контенту, що передається такими мережами, наприклад, це послуга доступу до інтернет-мережі [19].

Стаття 84 зобов'язує держав-членів забезпечити для споживачів на своїх територіях доступ до послуги ширококутового інтернет-доступу та доступу до сервісів голосової комунікації на якісному рівні, у фіксованому місці та, що важливо, за доступною ціною. При цьому, згідно зі Статтею 85, за відсутності у країни, в силу національних умов, здатності до вказаного, особливо щодо забезпечення прийнятної ціни на послугу, що позбавляє жителів з невисоким доходом можливості користуватися нею, то таким державам зобов'язується вжити необхідних заходів для забезпечення доступності прийнятної послуги ширококутового доступу до Інтернету для зазначеної категорії осіб хоча б у фіксованому місці. До Директиви є спеціальні додатки, так Додаток V містить мінімальний перелік послуг, які повинна забезпечувати послуга ширококутового доступу до інтернету в розумінні статті 84(3), це наступні: e-mail, пошукові системи, онлайн-інструментарій для базової підготовки та навчання, інтернет-банкінг, сервіси пошуку роботи, покупки товарів, e-governance, відеодзвінки та інше [19].

Раніше діяла Директива 2003/98/EC про повторне використання інформації державного сектора (також - *PSI Directive*), яка запровадила положення про недискримінацію, прозорість, ліцензування, стягнення плати, та використовувані інструментів для полегшення виявлення та повторного використання інформації з державного сектору. У статті 13 Єврокомісії ставилося завдання з проведення аналізу застосування Директиви з подальшою доповіддю-звітом про це та про можливі

уточнення до липня 2018. Звіт був зроблений, він підтвердив сприяння Директиви досягненню її основних політичних цілей, однак були виявлені і недоліки потенціалу інформації державного сектора для європейської економіки та суспільства загалом. Так з'явилася Директива 2019/1024 про відкриті дані та повторне використання інформації державного сектора, яка набула чинності 16 липня 2019 року. Вона спрямована на вирішення спірних питань у галузі управління та використання даних та вказує на важливість принципу повторного використання та публікації в комерційних та некомерційних цілях відкритих державних даних органів держсектора. Але для цілей даного наукового дослідження особливе значення має визначення «набору даних високої цінності», яким присвячені параграфи 66-69 та інші преамбули. Вони включають інформацію з різних тематичних добірок і важливі для розвитку суспільства та економіки та повинні публікуватися на повністю безкоштовній основі через інтерфейси прикладного програмування API у кожній із країн-учасниць. До них, крім іншого, відносяться згідно зі статтею 13(1) ліцензовані відкриті дані [162].

На початку 2019 року Єврокомісія вирішила стандартизувати використання ліцензій Creative Common як стандартів для відкритих ліцензій відповідно до політики повторного використання. Це важливо, оскільки Creative Commons визначають особливості управління умовами авторського права, що стосуються всіх творчих матеріалів, ним захищених. У випадку Директиви 2019/1024 має місце формування передової практики для полегшення повторного використання даних, які організація робить загальнодоступними у всесвітній мережі.

Директива (ЄС) 2019/789, яка встановлює правила застосування положень авторського права та суміжних прав щодо окремих інтернет-трансляцій мовних компаній та ретрансляції радіо- та телепрограм доповнила собою Директиву 93/83/ЄЕС. Метою прийняття документа послужила суттєва модернізація правового регулювання у зазначеній сфері

через настання цифрової ери та стрімкого поширення Інтернет-технологій, так само як і посилення боротьби з Інтернет-піратством. Цікавим є положення параграфу 14 преамбули, що наказує операторам ретрансляції, які надають послуги у супутникових, мобільних та інших IP-мережах, Інтернеті користуватися механізмом обов'язкового колективного управління правами. Щоб забезпечити достатні гарантії проти несанкціонованого використання об'єктів, що охороняються, послуги ретрансляції через всесвітню мережу підпадають під дію даного НПА тільки при наданні їх в середовищі, де тільки у авторизованих користувачів є доступ до ретрансляцій, і рівень безпеки контенту забезпечується досить високий [164].

Директива ЄС 2019/790 про авторське право та суміжні права на єдиному цифровому ринку внесла собою поправки до Директив 96/9/ЄС та 2001/29/ЄС. У параграфі 2 документа зазначено, що він прийнятий у галузі авторського права та суміжних прав, щоб сприяти функціонуванню внутрішнього ринку, забезпечувати належний захист правовласників, спростити правооформлювальні процедури тощо. У пар.22 зазначено, що винятком з охорони (тобто добросовісним використанням) інтелектуального об'єкта варто вважати його використання з єдиною метою ілюстрації для навчання під час викладацької та навчальної діяльності у приміщеннях навчальних закладів або поза такими, наприклад, у музеї, бібліотеці та лише в тому обсягу, який виправданий такими цілями. При цьому виняток поширюється і на об'єкти, створені за допомогою цифрових засобів, які можуть бути підключені до Інтернету, і на ті, які використовуються на відстані за допомогою безпечних електронних середовищ, наприклад, у контексті онлайн-курсів. При цьому зазначеним безпечним електронним середовищем вважається цифрове середовище викладання та навчання, доступ до якого мають лише викладачі та учні (студенти) за допомогою відповідних процедур аутентифікації. Параграф 62 говорить про сервіси-

файлообмінники, які не повинні надавати послуги, основна мета яких полягає в тому, щоб дати користувачам можливість завантаження та обміну файлами, захищеними авторським правом, із комерційною метою. Платформи для розробки програмного забезпечення з відкритим вихідним кодом та обміну ним, некомерційні наукові або освітні репозиторії, некомерційні онлайн-енциклопедії виключені із визначення постачальника онлайн-послуг з обміну контентом [165].

Директива (ЄС) 2019/770 про деякі аспекти контрактів на поставку цифрового контенту та цифрових послуг, відповідно до своєї статті 2(6) захищає споживачів, тобто будь-яких фізосіб, що діють стосовно угод, що підпадають під цю Директиву, з метою, що виходить за рамки торгівлі, бізнесу, ремесла чи професії зазначених суб'єктів. У статті 10 зазначено, що якщо має місце обмеження, яке впливає із порушення будь-якого права 3-ї сторони (прав інтелектуальної власності серед інших прав), і таке обмеження перешкоджає використанню цифрового контенту або послуги, споживач має право використовувати засоби правового захисту. Продавець зобов'язаний надати такі цифрові "покупки", що відповідають вимогам відповідності як одному з головних понять сучасного договірної права. Параграф 19 преамбули говорить про те, що для забезпечення швидкого технологічного розвитку даний НПА поширює свою дію також на комп'ютерні програми, музику, ігри, відео- та аудіофайли, електронні книги тощо, так само як і на діджитал-послуги зі створення, розробки, зберігання, отримання доступу до даних у цифровій формі, і вже згаданих об'єктів, також якщо вони обробляються на хмарних сервісних платформах і у соціальних мережах [163].

Директива буде застосовуватися незалежно від середовища передачі або надання доступу цифровим об'єктам, але не щодо послуг доступу в інтернет, що не залежать від номера телефону. Параграф 33 висуває вимогу про застосування Директиви тільки до елементів загального договору, що

складаються з постачання цифрового контенту або цифрових послуг, решту елементів слід врегулювати нормами національного законодавства. Але коли мають місце пакетні контракти із пропозицією до придбання цифрового контенту (послуги) разом з послугою міжособистісного зв'язку на основі номера або послугою доступу до всесвітньої мережі, норми даного НПА щодо зміни цифрового контенту не застосовуються до елемента цифрового контенту або послуги з пакета, вони застосовуються до усіх елементів пакета загалом. Параграф 60 вимагає, щоб споживач сприяв продавцеві щодо перевірки причини відсутності відповідності, викликані цифровим середовищем споживача з використанням технічно доступних засобів, які не становитимуть особливих труднощів для споживача. Це можливо, наприклад, шляхом надсилання автоматично згенерованих звітів про інциденти, і лише у виняткових та обґрунтованих випадках споживачеві доведеться дозволити віртуальний доступ до свого цифрового середовища [163].

На окрему увагу заслуговують нормативно-правові акти Євросоюзу щодо кібернетичного простору як середовища для здійснення взаємовідносин у відношенні інтелектуальної власності. Так, Регламент (ЄС) 2021/694 заснував Програму «Цифрова Європа» та скасував Регламент 2015/2240. У преамбулі (пар.14) зазначено, що Програма націлена на підтримку цифрової трансформації промисловості та сприяння ефективному використанню промислового потенціалу на благо громадян та юридичних осіб Євросоюзу та включає п'ять основоположних цілей, а саме: високопродуктивні обчислення; Штучний інтелект; кібербезпека та довіра; просунуті цифрові навички; розгортання та оптимальне використання цифрових можливостей та функціональної сумісності. Пар. 15 вказує на взаємозалежність цих цілей, так, ШІ не зможе існувати без кібербезпеки, для нього ж ключовими будуть можливості високопродуктивних обчислень. Пар. 17 говорить про Європейські центри цифрових інновацій

для стимуляції запровадження передових цифрових технологій. Пар. 36 зазначає, що Європарламент наголошує на важливості загальноєвропейського підходу до кібербезпеки та наполягає на важливості підвищення поінформованості населення у цьому питанні. Головним обов'язком керівників бізнесу та політичних груп визнається кіберстійкість [257]. Пар. 37 чітко вказує на неможливість досягнення необхідного рівня кібербезпеки лише через національні ініціативи. У Пар. 39 довіра користувачів розуміється як головна умова функціонування Єдиного цифрового ринку. При цьому технології кібербезпеки, а саме цифрова ідентифікація, криптографія та виявлення вторгнень покликані забезпечити таку довіру до онлайн-дій та транзакцій для всіх суб'єктів кібервідносин. Пар. 61 наголошує на важливості реалізації Програми в такому вигляді, щоб забезпечити повну повагу Союзним та міжнародним рамкам захисту інтелектуальної власності, адже на неї покладено ключову роль у розвитку інновацій, і, відповідно, вона є обов'язковою для ефективної реалізації Програми. Стаття 2 визначила кібербезпеку як дії, що забезпечують захист мережевих та інформаційних систем, так само як і їх користувачів та інших суб'єктів, що зачіпаються кіберзагрозами. Стаття 3 ще раз перераховує 5 цілей Програми, а стаття 6 присвячена безпосередньо кібербезпеці та довірі, причому дії щодо цього завдання мають здійснюватися насамперед через Європейський центр компетенції у галузі промисловості, технологій та досліджень у сфері кібербезпеки та Мережу національних координаційних центрів. У Додатку 1 до Регламенту зазначено, що Програма покликана стимулювати зміцнення та створення потенціалу захисту цифрової економіки, соціуму та демократії ЄС за допомогою зміцнення його промислового потенціалу та конкурентоспроможності у сфері кібербезпеки. Для цього ставляться такі завдання: спільне інвестування в обладнання для кібербезпеки, інфраструктури та ноу-хау, що допоможе забезпечити стабільність критично важливих інфраструктур та єдиного

цифрового ринку; забезпечення впровадження дієвих рішень щодо кібербезпеки та довіри в країнах ЄС; запровадження нових програм та політик для усунення прогалин у навичках з кібербезпеки тощо [257].

Також у ЄС діє Резолюція Європейського парламенту 2013/2606 (RSP). Вона присвячена Стратегії кібербезпеки Європейського союзу, головною метою якої є встановлення та забезпечення функціонування відкритого, безпечного та захищеного кіберпростору.

Окремо варто відзначити Директиву 2011/93/ЄС про боротьбу із сексуальним насильством та сексуальною експлуатацією дітей та дитячою порнографією, яке прийшло на зміну раніше діючому Рамковому рішенню Ради 2004/68/ІН. Для зазначеної мети Преамбула (пар. 26) закликає країни Союзу полегшити процедуру розслідування зазначених злочинів та пред'явлення звинувачень у кримінальному судочинстві з тим, щоб було менше негативного впливу на дітей-жертв сексуального насильства в кіберпросторі. Для цього ініціювання таких правоохоронних дій не повинно залежати від повідомлення чи звинувачення від потерпілого та його представників. Пар. 12 відносить до серйозних форм сексуального насильства та експлуатації неповнолітніх також дії з використанням інформаційно-комунікаційних технологій, а саме онлайн-домагання через сайти, соціальні мережі та чати. Стаття 2 визначила такий контент як дитяча порнографія, зарахувавши до такого будь-який матеріал, який візуально зображує дитину, залучену до реальної чи змодельованої поведінки сексуального характеру; зображення дитячих статевих органів тощо. При цьому виконанням порнографічного контенту слід вважати живу демонстрацію, спрямовану на аудиторію, у тому числі за допомогою інформаційних та комунікаційних технологій [171]. На жаль, зразки таких заборонених "творів" у формі відеороликів - досить часте явище у кіберпросторі.

Регламент (ЄС) 2021/784 про боротьбу із поширенням терористичного контенту в Інтернеті також набув особливого значення останнім часом. Він встановив єдині правила щодо протидії неправомірному використанню послуг хостингу з метою розповсюдження серед населення терористичного контенту в Інтернеті. Стаття 1 вимагає від постачальників послуг хостингу вживати заходів для захисту основних прав, зокрема свободи слова та інформації у відкритому та демократичному суспільстві. Стаття 1(3) вимагає не визнавати терористичним контентом ті матеріали, які надаються населенню в освітніх, публіцистичних, художніх чи дослідницьких цілях або для протидії терористичним актам, навіть якщо вони виражають полемічні та суперечливі погляди під час публічних дебатів [258].

Щодо органів, які опікуються питаннями інтелектуальної власності в Євросоюзі взагалі та в кіберпросторі зокрема, то слід згадати Регламент (ЄС) 386/2012, який поклав на Відомство щодо гармонізації у внутрішньому ринку завдання, пов'язані із захистом прав інтелектуальної власності, а саме покращення розуміння цінності інтелектуальної власності та наслідків порушень відповідних прав, сприяння підвищенню поінформованості населення про них; підвищення кваліфікації осіб, які забезпечують захист відповідних прав, надання механізмів для покращення онлайн-обміну відомостями з цього питання між ними та розширення знань про технічні інструменти для запобігання подібним порушенням тощо (Стаття 2). Держави-члени зобов'язані, відповідно до Статті 5, за запитом Відомства або з власної ініціативи не лише надати статистичні дані про порушення прав інтелектуальної власності, а й інформувати орган про важливі судові прецеденти та про свою спільну політику, методики та стратегії захисту прав інтелектуальної власності [260].

Регламент (ЄС) 513/2014 заснував у рамках Фонду внутрішньої безпеки інструменти фінансової підтримки співпраці поліції з метою

попередження злочинів та управління кризовими ситуаціями. У Преамбулі (пар.1) зазначено мету Євросоюзу - забезпечення високого рівня безпеки у сфері свободи, безпеки та правосуддя, для чого потрібні спільні скоординовані дії правоохоронних органів, Європолу та інших відповідних органів ЄС. Пар. 2 вимагає, задля досягнення зазначеної мети, спільно боротися, зокрема, проти тероризму і кіберзлочинності, а пар. 3 перераховує 5 стратегічних цілей спільних ініціатив, де, серед іншого, зазначено підвищення безпеки громадян і бізнесу в кіберпросторі. Стаття 4 (е) закликає країни-учасниці усіляко сприяти придбанню, та забезпеченню техобслуговування європейських та національних ІТ-систем, модернізувати їх та обладнання, особливо ретельно перевіряти системи інформаційних та комунікаційних технологій, щоб забезпечити якісну співпрацю Союзу в галузі кібербезпеки та протидії кіберзлочинності, зокрема це стосується Європейського центру кіберзлочинності. Додаток I до Регламенту містить список стратегічних пріоритетів ЄС, серед яких зазначені й заходи щодо запобігання та боротьби з кіберзлочинністю, підвищення рівня безпеки мешканців та підприємств у кіберпросторі. Для цього варто використовувати правоохоронні та судові органи, впроваджуючи відповідні проекти щодо підвищення можливості протидії кібератакам [261].

Регламент (ЄС) 2021/887 заснував Європейський центр промислової, технологічної та дослідницької компетенції в галузі кібербезпеки (далі – Центр) та Мережа національних координаційних центрів (далі – МНКЦ). Відповідно до Статті 1 також він встановив правила призначення таких національних координаційних центрів та правила створення Співтовариства з питань кібербезпеки. Стаття 3 говорить про місію Центру та МНКЦ, а саме про допомогу Євросоюзу у зміцненні свого лідерства та стратегічної автономії в галузі кібербезпеки зі збереженням дослідного, академічного, технологічного та іншого потенціалу ЄС у галузі

кібербезпеки, які є основою, в тому числі, інформаційної безпеки, про яку йшлося у Розділі 2 даного дисертаційного дослідження, а саме таких її основ як конфіденційність, цілісність та доступність даних. У статті 8 сказано про завдання Співтовариства, а також його склад, до якого включені представники промисловості, академічних та дослідницьких організацій, інших відповідних асоціацій громадянського суспільства [259].

Отже, у Євросоюзі щодо авторського права діє особлива "континентальна" концепція, за якою саме вираження особистості авторів у своїх творчих об'єктах є основою надання охорони відповідним правам. Це в рівній мірі стосується й інших творчо-інтелектуальних об'єктів, що існують у кіберпросторі. З урахуванням вищенаведеної характеристики нормативно-правових актів ЄС у вигляді директив та регламентів, можна зробити висновок, що Європейський Союз успішно та ефективно регулює на правовому рівні питання захисту прав на об'єкти як авторського права та суміжних прав, так і промислової власності.

Загалом, ЄС і його країни-члени є впевненими прихильниками відкритого, стабільного і безпечного кіберпростору, у якому вшановується верховенство права та основоположні права і свободи людини. Союз стурбований зростанням рівня зловмисної поведінки у кіберпросторі, включаючи збільшення кількості випадків крадіжки інтелектуальної власності у процесі його використання. Саме тому всі країни-члени покликані боротися з подібними зловмисними діями та розвивати міжнародне співробітництво для забезпечення стабільності в кібернетичному домені.

Законодавством ЄС передбачені різні інструменти та механізми для запобігання порушенню в галузі інтелектуальної власності взагалі, і на досудовій стадії зокрема. Превентивні заходи включають відправку вимоги про видалення нелегального контенту з веб-ресурсу його власнику, а оператору зв'язку - про необхідність здійснити технічні заходи щодо

закриття доступу до таких матеріалів і такі, які перешкоджають повторному завантаженню спірних об'єктів на даний ресурс. Правомірність таких вимог оцінюється національними судами. Також у Союзі робляться спроби впровадження додаткових обов'язків для веб-платформ у вигляді необхідності заключати ліцензійні угоди з правовласниками, що має допомогти у протидії неправомірному використанню об'єктів творчості в кібернетичному просторі Євросоюзу. Однак така методика отримала великий обсяг критики через суперечність її існуючій практиці та законодавству ЄС.

4.1.2. Країни СНД

У Союзі незалежних держав кожна країна має своє національне законодавство з питань інтелектуальної власності. Щодо авторсько-правового інституту, то за часів СРСР діяла централізована система відома як Всесоюзне агентство з авторських прав. У зв'язку зі скасуванням цього органу кожна союзна республіка прагнула створити свій власний національний спеціалізований орган з авторського права.

Більшість членів СНД окремо вступили до членів ВОІВ, а також стали учасниками більшості її договорів. Зараз в багатьох із таких країн все ще триває проектно-законодавча робота в галузі інтелектуальної власності, особливо щодо захисту відповідних прав в інтернеті, обробки цифрової інформації за допомогою ІКТ та захисту персональних даних при здійсненні покупок у веб-магазинах.

Країни-учасниці СНД взяли на себе зобов'язання щодо надання взаємодопомоги (правової та інформаційної) у сфері патентних, авторських та суміжних прав, про що говорять прийняті Угоди про співпрацю у галузі авторського права (1993 р.), Алма-Атинські рекомендації (1995 р.) та інші документи. Відповідальність за злочини у сфері інтелектуальної власності відрізняється від держави до держави. Також немає єдиного документа,

уніфікуючого норми у тому чи іншому напрямі у сфері захисту прав інтелектуальної власності. Як уже зазначалося, кожна держава має свої власні НПА. Про них і йтиметься далі.

Можна сказати, що захист прав інтелектуальної власності в Азербайджані забезпечується на середньому рівні. Так, національне нормативно-правове регулювання охоплює авторські та суміжні права, топології інтегральних мікросхем, патенти, промислові зразки, товарні знаки, зазначення місця походження товарів та інші загальноприйняті інтелектуальні об'єкти, але також заявлено багато скарг у зв'язку з контрафактною продукцією. Особливо часто має місце використання неліцензійного програмного забезпечення, причому не лише окремими індивідами, а й у державному секторі. Держава приєдналася до більшості договорів ВОІВ, у т.ч., тих, що стосуються правового регулювання відносної інтелектуальної системи в кіберпросторі, а саме до інтернет-договорів ВОІВ (ДАП та ДВФ). В Азербайджані також діє особливий закон №365-IVQ "Про забезпечення прав інтелектуальної власності та про боротьбу з піратством" (від 22 травня 2012 року), ухвалений на виконання п. 13 частини I статті 94 державної Конституції. Даний НПА регламентує відносини у зв'язку із забезпеченням захисту прав інтелектуальної власності, охороною інтересів відповідних правовласників, запобіганням правопорушенням у цій сфері, включаючи нелегальне виробництво та розповсюдження екземплярів захищених об'єктів [73]. Також варто зазначити, що у 2014 році держава запустила спеціальну систему захисту авторських прав у мережі Інтернет. Такий захист має бути надано Центром забезпечення прав інтелектуальної власності в рамках Агентства з авторських прав Азербайджану. За задумом розробників, як механізм захисту авторських прав, повинна використовуватися виплата авторам певної винагороди у разі вільного використання об'єктів авторських прав на веб-ресурсах [302].

Авторське право у Вірменії до 2006 р. регулювалося національним законом про авторське право та суміжні права №ЗР-28 (від 28 січня 2000 р.). Нова редакція (№ 121) закону покликана надати більший обсяг охорони авторам, яких раніше закликали керівники телерадіокомпаній письмово відмовитись від роялті, пояснюючи таке порушенням можливістю безкоштовно рекламувати себе як авторів творів та виконавців під час трансляції таких робіт. Цікаву норму містить вірменське законодавство щодо співавторів, до яких віднесено і авторів аудіовізуальних робіт. Взаємини між зазначеними суб'єктами, як і належить, визначаються укладеним між ними договором [34, 248].

Зміни, внесені до закону в 2013 р. (від 30.09.13 НО-106-N) серед іншого, включали вказівку на термін «гіперпосилання». Також тепер інтернет-виданням необхідно обов'язково вказувати активне посилання на джерело публікованих даних у своїх матеріалах. Ще встановлювалась норма про те, що копіювання частин інформації з друкованої преси та взятої на веб-ресурсі, а також подальша публікація подібних відомостей в інших джерелах можливі лише в тому обсязі, який не передасть повністю зміст оригінального матеріалу [287].

У країні також функціонує Вірменське авторське товариство Армавтор, до відання якого віднесені питання захисту авторських правомочностей. Загалом країна цілеспрямовано домагається зближення національного законодавства із міжнародними стандартами в галузі інтелектуальної власності, для чого впроваджує інструменти захисту відповідних прав, а також проводить інформаційно-просвітницькі заходи щодо супутніх питань. У сфері застосування законодавства з інтелектуальної власності головну роль віддано Агентству інтелектуальної власності Вірменії (AIPA), у чії повноваження також включено інформування правоохоронних органів та широкого загалу про наслідки порушень прав товарних знаків та авторського права [310, с. 4].

У Грузії діє Закон про авторське право та суміжні права 1999 р., згідно з ним термін захисту авторських прав аналогічний українському - весь час протягом життя автора та 70 років з моменту його смерті, після чого творча праця переходить у суспільне надбання (статті 31-32). Зазначимо, що дозволені як *fair use* деякі види використання комп'ютерних програм та баз даних, про що сказано у статтях 28-30 закону [70].

Грузія також "прославилася" засиллям неліцензійного ПЗ, але оскільки захист інтелектуальної власності – це одна із обов'язкових умов євроінтеграції, то влада країни намагається всіляко змінити ситуацію. Так, на початку 2015 р. місцевий уряд підписав угоду з компанією Microsoft, таким чином держава стала першою на пострадянському просторі, чий державний апарат був повністю оснащений ліцензованим софтом. Міністерство освіти та науки впроваджує аналогічне правило у школах. Також останнім часом країна активно переходить на використання хмарних технологій [223].

Грузія є "чистим імпортером прав інтелектуальної власності", вона привела своє законодавство про інтелектуальну власність у відповідність до стандартів Європейського союзу. Сакпатенти, національний центр інтелектуальної власності країни, проводить політику по підвищенню поінформованості громадян щодо правових механізмів захисту та забезпечення дотримання відповідних прав. При цьому таке забезпечення, все ж таки, не розвинене належним чином і вимагає посилення прозорості та підзвітності [189, с. 36, 46].

Що стосується Республіки Казахстан, то тут діє Закон про авторське право та суміжні права 1996 р., до якого у 2012 році внесено зміни. Так, стаття тепер містить термін "інтернет-ресурс", яким вважається «електронний інформаційний ресурс, технологія його ведення та використання, що функціонує у відкритій інформаційно-комунікаційній мережі, а також організаційна структура, що забезпечує інформаційну

взаємодію». Така сама норма визначає відтворення як зберігання творчої роботи у будь-якій матеріальній формі, що включає і відкриті інформаційно-комунікаційні мережі. Дано й визначення власнику такого інтернет-ресурсу, ним є суб'єкт, який повноцінно реалізує права володіння, використання та розпорядження цим ресурсом, при цьому важливо розміщувати дані в Інтернет-середовищі акуратно, інакше на відповідальну особу може накладатися цивільна та адміністративна відповідальність [68].

Закон республіки № 537-IV 2012 р. також змінив положення статті 129 Кодексу про адміністративні правопорушення, додавши до неї пп. 3-5, віднісши до переліку випадків незаконного використання творів розміщення таких у всесвітній мережі з метою надання необмеженому колу осіб доступу до них, що карається винесенням попередження, якщо немає ознак кримінально-каранного діяння. Також до зазначеного переліку віднесено і створення веб-ресурсів для подальшого доступу до обміну, зберігання та подібних активностей, якщо також не спостерігається наявність кримінально-каранного діяння, при цьому на порушника накладається штраф, сума якого зростає при повторенні подібних діянь протягом 1 року. після накладення санкцій [71].

Захист інтелектуальної власності сьогодні визнаний одним із ключових завдань країни, оскільки вона прагне вступити до Світової організації торгівлі. Тому основні сили у цій сфері кинуті на боротьбу з інтернет-піратством. Відповідно до Концепції правової політики держави на період 2010-2020 рр., з метою реалізації прав громадян як власників виняткових прав на об'єкти ІВ, було визначено основні напрямки розвитку національного права, у т.ч. щодо приведення чинних НПА, які визначають права інтелектуальної власності, у відповідність до міжнародних стандартів, але з урахуванням національних інтересів [215]. Питання захисту авторських прав у країні віднесено до відання Казахстанського авторського товариства та Асоціації казахстанських авторів та виконавців

тощо. В основному їх діяльність ґрунтується на колективному управлінні майновими авторськими правами місцевих та іноземних авторів та виконавців.

У Киргизькій Республіці сьогодні діє закон про авторське право та суміжні права 1998 р. Виходячи з його норм, можна віднести передачу творів у всесвітню мережу до права на відтворення, розповсюдження або повідомлення твору для загальної інформації по кабелю або з використанням подібних засобів. З 2002 року держава також бере участь у інтернет-договорах ВОІВ. Колективне управління авторськими та суміжними правами віддано у відання Державного агентства з науки та інтелектуальної власності при Уряді країни (Киргизпатент). Також зараз діють різні системи цифрового управління правами (так звані *DRM systems*), що передбачають управління контентом у діджитал-формі при поширенні його у всесвітній мережі та недопущення незаконного його поширення, а також всіляке сприяння легальному використанню творчих робіт в умовах розвитку сучасних технологій.

Заходи захисту прав інтелектуальної власності в Інтернет-мережі передбачені у цивільному, адміністративному та кримінальному законодавстві країни. Так, статті 10-11 місцевого ЦК та статті 48-50 Закону про авторське право передбачають такі заходи у цьому випадку: визнання відповідних прав; відновлення становища до порушення прав; превентивні методи проти правопорушень; відшкодування завданих збитків; стягнення отриманого під час порушення доходу; виплату компенсації у розмірі 20-50000 мінімальних розмірів оплати праці замість двох попередніх стягнень; вживання інших законних заходів. Стаття 150 киргизького Кримінального кодексу передбачає виплату потрійного айипу або позбавлення волі строком до 3 років та неможливість обіймати певні посади на аналогічний термін у разі незаконного умисного використання об'єктів АП або суміжних прав, або такого правопорушення, скоєного з необережності із заподіянням

великого об'єму шкоди. Стаття 340 Кодексу про адміністративну відповідальність передбачає штраф у розмірі 5-10 мінімальної заробітної плати (далі - МЗП) (для фізосіб) або 10-20 МЗП (для посадових осіб) за незаконне виготовлення чи інше незаконне використання екземплярів творчих робіт [94].

Також у країні активно борються з кіберсквотингом та кіберпіратством. Зазначається, що правова охорона доменних імен та товарних знаків у країні сильно відрізняється, що тягне за собою зловживання і, відповідно, велику кількість судових розглядів у цій сфері. Тому до закону республіки про товарні знаки, знаки обслуговування та найменування місць походження товарів 2003 р. було додано норму про визнання несанкціонованим використання товарного знака, тотожного або подібного до ступеня змішування зі знаком іншого власника, як домен, тобто в такому разі матиме місце порушення права власника товарного знака. Норма також вимагає насамперед отримати дозвіл власника ТЗ на його використання як домену, інакше на власника домену накладається відповідальність. При цьому доказом порушення буде експертний висновок Киргизпатента, який здійснює такі експертизи. Ще вона накладає на уряд держави обов'язок розробити порядок використання товарного знака або подібного позначення як адреси в інтернеті. Згадані статті ЦК та стаття 41 місцевого закону про товарні знаки припускають громадянську відповідальність порушника. 341 стаття Кодексу про адміністративну відповідальність накладають штрафи за незаконне використання чужого товарного знака у розмірі 5-20 МЗП (для громадян), 20-100 МЗП (для посадових осіб). Стаття 191 Кримінального Кодексу за незаконне неодноразове використання чужого товарного знака передбачає накладення штрафу у розмірі 200-400 МЗП або громадських робіт терміном 180-240 годин, або арешт строком до півроку. Аналогічне покарання передбачено за порушення, якщо таке завдало великих збитків [94].

Молдова має консолідовану комплексну нормативну базу інтелектуальної власності, адже країна намагалася інтегрувати у всесвітню економічну систему. Місцеве законодавство було приведено у відповідність до вимог Угоди ТРІПС. У 2007 році було ухвалено поправки до молдавського Кримінального кодексу, які встановили, крім іншого, кримінальне покарання за порушення прав інтелектуальної власності. Після зазначеної дати вся нормативна база ІВ була переглянута з метою гармонізації документів з європейськими стандартами. У зв'язку із зазначеним, були прийняті в новій редакції закони про охорону промислових малюнків та моделей (2007 р.), товарних знаків (2008 р.); винаходів (2008 р.); географічних зазначень (2008 р.), а також Закон про авторське право та суміжні права (2010 р.). Щодо останнього зазначимо Статтю 3, що дає визначення поняття «доведенням до загальної інформації в інтерактивному режимі», ним вважається надання доступу до об'єктів ІВ, у тому числі, засобами бездротового зв'язку, включаючи всесвітню інтернет-мережу та інші комп'ютерні мережі. Стаття 66 цього Закону присвячена постачальникам послуг передачі даних та хостерам [69].

Під час модернізації зазначених п'яти НПА було враховано норми Директиви 2004/48/РЄ від 29.04.2004 р. щодо захисту прав на інтелектуальну власність. У 2015 р. було прийнято поправки до чинних актів з охорони промислових малюнків та моделей, товарних знаків, винаходів. Молдова також приєдналася до багатьох договорів ВОІВ, СОТ, ЮНЕСКО. Регулятором у сфері, що розглядається, країна обрала Державне агентство з інтелектуальної власності (AGEPI), до обов'язків якого входять стратегічне планування та реалізація задач з розвитку національної системи ІВ, управління такою структурою та всіляке сприяння просуванню ініціатив з удосконалення нормативно-правового регулювання. Дане агентство створило Комісію з медіації в галузі інтелектуальної власності, до її відання віднесено розгляд спорів з ІВ, до такої процедури сторони можуть вдатися

як до, так і після порушення процесу в арбітражі або суді. Також у рамках АГЕРІ діє Національна комісія з інтелектуальної власності (НКІС), яка відповідає за координацію та забезпечення взаємодії владних структур та власників прав на інтелектуальну власність [263].

Авторське право в Таджикистані регулюється спеціальним законом про авторське право та суміжні права № 726 1998 р., при цьому АП діє протягом усього життя автора та 50 років після його смерті. Загалом, з метою забезпечення охорони інтелектуальної власності у країні прийнято 18 законів. Республіка також є учасницею понад 20 міжнародних угод та договорів у цій сфері. У державі створено Національний патентно-інформаційний центр для захисту держінтересів щодо винаходів, промислових зразків, товарних знаків та знаків обслуговування. Авторські права за кордоном забезпечує відділ права, захисту прав авторів та суміжних прав при Міністерстві культури. У 2014 р. було прийнято національну стратегію розвитку інтелектуальної власності держави на 2014-2020 рр., націлену на розвиток охорони інтелектуальної власності та управління використанням її потенціалу. Спеціальна Апеляційна рада розглядає суперечки щодо об'єктів промислової власності як досудова інстанція. Національний інноваційний Інтернет-портал Республіки з'явився у 2014 р. [38]. Зазначимо, що у чинному законодавстві немає конкретних норм, які встановлюють відповідальність інформаційних посередників за порушення виняткових прав та передбачають заходи оперативного впливу, наприклад, блокування доступу до веб-ресурсів. Ці питання, як правило, врегульовані в ліцензійних договорах між такими посередниками та регулятором області в особі Служби зв'язку при Уряді.

Закон № ЗРУ-42 «Про авторське право та суміжні права» у редакції 2007 р. діє в Узбекистані та повністю відповідає вимогам Бернської Конвенції. Він посилив відповідальність інтернет-провайдерів за порушення АП. Важливим нововведенням стало визначення терміна

«доведення до загальної інформації», яким є виключне право авторів, відповідно, розміщення в інтернеті контенту без укладання договорів із цими суб'єктами – це порушення чинного законодавства. Також саме автор наділений винятковим правом на використання свого твору в Мережі, і будь-яке використання творчої роботи в ній можливе лише з дозволу автора. Узбецький Кримінальний кодекс (ст. 149) передбачає штраф у розмірі 25-75 МЗП, або виправні роботи на 3 роки, або арешт на строк до півроку за присвоєння авторства, примус до співавторства або розголошення без дозволу автора інформації про його творчі об'єкти до їх офіційної реєстрації чи публікації. Також передбачено цивільну та адміністративну відповідальність за порушення прав інтелектуальної власності. Так, від порушника можна вимагати визнання прав, відновлення становища до порушення, відшкодування збитків (у т.ч. втраченої вигоди), виплати компенсації (у т.ч. моральної шкоди) та подібні заходи. Захистом відповідних прав займається Агентство інтелектуальної власності при Міністерстві юстиції країни [1].

Також президентським Указом № УП-4947 від 07.02.2017 р. було прийнято Стратегію дій з п'яти пріоритетних напрямів розвитку Республіки Узбекистан у 2017–2021 роках. У 2021 р. Постановою Президента № ПП-4965 від 28.01.2021 р. з метою вдосконалення системи охорони об'єктів ІВ у контексті зазначеної Стратегії з 01.04.2021 р. було знято законодавчі обмеження на реєстрацію ТЗ та знаків обслуговування виключно на ім'я юридичних осіб та фізосіб-підприємців, виходячи з норм міжнародних договорів у цій сфері. Також підлягав впровадженню порядок прискореної експертизи з метою суттєвого скорочення термінів державної реєстрації об'єктів ІВ. Незвичну норму передбачено п.2 цієї Постанови, а саме Агентству з інтелектуальної власності слід використовувати аутсорсинг у процесі проведення державної експертизи заявок на відповідні об'єкти. П. 5 вимагав запустити "Патентну платформу" при Агентстві для обліку об'єктів

інтелектуальної власності в електронній формі в режимі реального часу [103].

Отже, відносини щодо інтелектуальної власності в кібернетичному просторі на теренах країн СНД на сьогоднішній день врегульовані на середньому рівні, хоча позитивна динаміка, безумовно, спостерігається, а з нею і зростання кількості нормативно-правових актів, присвячених врегулюванню відповідних правовідносин. Але жодна з країн Співдружності не має уніфікованого документа, присвяченого саме відносинам інтелектуальної власності в кібернетичному домені, відповідно кількість прогалин у законодавстві цієї сфери все ще залишається значною. А таке, в свою чергу, сприяє збільшенню кількості випадків порушення прав інтелектуальної власності. Розумним кроком у цьому випадку стане прийняття одноманітного закону, який поширюватиме свою дію на всі держави-члени СНД. Також доцільно встановити та впровадити спеціальну підвідомчість спорів про захист виняткових прав при використанні контенту у кібернетичному просторі арбітражним судам. У системі цих органів для формування одноманітної практики у справах буде доречним створити Суд з інтелектуальних прав.

Сьогодні країни, що розглядаються, є членами ВОІВ та учасницями більшості адміністрованих організацією договорів. Це відповідає узгодженості між законодавчим регулюванням процедур захисту авторських, суміжних прав та отримання патентів у країнах СНД та Євросоюзу. Проте запозичення норм про охорону прав ІВ у країнах ЄС для країн СНД, на думку автора дисертаційного дослідження, допоможе більш детально та якісно врегулювати питання забезпечення прав у кібернетичному просторі, що є ключовим завданням у цій сфері.

4.2. Суб'єкти міжнародно-правової охорони права інтелектуальної власності

Як зазначалося раніше, в Україні діє низка важливих правових джерел у галузі інтелектуальної власності та регулювання кіберпростору. При створенні цього законодавчого масиву нашою державою враховувалися багаторічний досвід та практика відомств розвинених країн. Але, як відомо, національне законодавство застосовується лише в межах держави. А, отже, нечесні суб'єкти можуть порушувати відповідні права й поза територією їх виникнення, що негативно позначається на становищі авторів літературних творів, виконавців, винахідників та інших суб'єктів творчої діяльності.

У зв'язку із зазначеним на міжнародному та регіональному рівнях функціонують різні організації, що займаються питаннями інтелектуальної власності взагалі, та в кібернетичному домені, зокрема. Важливим напрямом співпраці української держави з відповідними міжнародними організаціями стало забезпечення друку адаптованих видань для українських читачів із особливими потребами.

По праву можна назвати головним серед згаданих суб'єктів Всесвітню організацію інтелектуальної власності, яка здійснює координацію заходів з міжнародного співробітництва у відповідній сфері. Вона також є ключовою спеціалізованою організацією у системі ООН. Основні конвенції, що захищають права ІВ, учасницями яких стали більшість країн світу, адмініструються саме ВОІВ. Україна тісно співпрацює з цією організацією з питань розробки та впровадження сучасних гармонізованих вимог щодо надання правової охорони відповідним об'єктам інтелектуальної власності.

Важко переоцінити роль Корпорації з управління доменними іменами та IP-адресами саме у контексті регулювання прав інтелектуальної власності у кібернетичному просторі. Ще з кінця минулого століття ця міжнародна некомерційна організація здійснює регулювання питань,

пов'язаних із доменними іменами та іншими аспектами функціонування Інтернету.

Суспільство Інтернету є міжнародною професійною організацією, чия головна мета - розвиток та забезпечення доступності мережі Інтернет. І хоча даний суб'єкт безпосередньо не займається проблемами інтелектуальної власності, але він забезпечує організаційну основу для низки інших консультативних та дослідницьких груп. Також це Суспільство сприяє розробці нових інтернет-технологій.

Взагалі, варто відзначити, що саме неурядові організації стали ключовими суб'єктами у регулюванні та забезпеченні функціонування всесвітньої мережі, без якої сьогодні ми вже не уявляємо кібернетичний простір. Наразі кількість таких організацій зростає, що забезпечується переважно підвищенням ступеня участі суб'єктів громадянського суспільства. Так, Рада з архітектури Інтернету займається питаннями його проектування та надає консультації раніше згаданому Суспільству. До Робочої групи проектування Інтернету входять розробники, дослідники, оператори. Серед її функцій - пошук проблем та відповідних рішень із технічних питань, а також розробка стандартів та угод щодо загальних архітектурних принципів протоколів Мережі.

На окрему увагу заслуговує Консорціум всесвітньої павутини, що складається з понад 350 організацій. Він не тільки розробляє та впроваджує інтернет-стандарти, але й надає відповідні рекомендації "відкритого" типу.

Можна зробити висновок, що міжнародна організаційна система охорони прав інтелектуальної власності сьогодні розвинена досить добре і має тенденцію до формування єдиних регулятивних підходів. Але технології розвиваються семимильними кроками, отже, розвиваються і витончені способи порушення норм права у сфері інтелектуальної власності. Саме тому роль вказаних організацій така важлива.

4.2.1. Всесвітня організація інтелектуальної власності (ВОІВ)

Всесвітня організація інтелектуальної власності (англ. *World Intellectual Property Organization, WIPO*) - це спеціалізована установа ООН з питань творчості та інтелектуальної власності. На даний момент (2022 р.) членами організації є 193 країни. З осені 2020 року очолює ВОІВ Дарен Танг. Як згадувалося, саме ця організація адмініструє ключові міжнародні конвенції у сфері інтелектуальної власності. Як зазначено на офіційному сайті ВОІВ, вона забезпечує глобальний політичний форум, де питання ІС вирішуються за допомогою спільного обговорення урядами, представниками громадянського суспільства та ініціативних груп [204] на благо всіх та кожного. Повноваження організації, принципи функціонування її керівних органів та подібне викладені у Конвенції ВОІВ 1967 р., яка й заснувала Всесвітню організацію інтелектуальної власності.

Сучасні технології створили безмежні можливості для обміну інформацією та знаннями незалежно від геолокації суб'єктів такої взаємодії, а значить, окремим національним відомствам не впоратися поодиночі, тому роль організації дуже важлива. Можна сказати, що всі, і традиційні, і нетрадиційні об'єкти інтелектуальної власності - це предмет ведення ВОІВ. Так, РСТ, Мадридська, Гаазька, Лісабонська системи дозволяють окремим новаторам та цілим компаніям обмежитися подачею однієї єдиної міжнародної патентної заявки або міжнародної заявки на реєстрацію ТЗ, найменування місця походження, промислового зразка, щоб їхні права охоронялися у всіх країнах-учасниках. Спори за доменними іменами, ключовим об'єктом інтелектуальної власності в кіберпросторі, можуть бути вирішені альтернативними методами через Центр арбітражу та посередництва, і це - відмінна альтернатива витратним судовим розглядом.

Багато відомств ІВ у різних державах об'єднують свої зусилля, обмінюються даними про патенти та інші об'єкти охорони. І щоб така спільна робота проходила успішно, зазначені відомства повинні

дотримуватися єдиних (загальних) технічних стандартів, тільки тоді ІТ-системи цих країн зможуть якісно взаємодіяти. У зв'язку із цим дуже важливо забезпечувати належну інтернет-взаємодію, а всі необхідні для цього інструменти повинні бути у вільному доступі. Тому організація здійснює координацію своїх активностей із державними відомствами ІВ з метою розробки та впровадження глобально інтероперабельних інструментів та техстандартів, що дозволить полегшити доступ до технологічної інформації людям по всій земній кулі.

Міжнародна патентна система отримала істотну перевагу у зв'язку зі створенням в рамках ВОІВ так званого PATENTSCOPE, де зібрана майже вся патентна документація, адже тепер усі користувачі Інтернету отримали доступ до такої інформації з будь-якої точки світу за допомогою пари кліків комп'ютерної миші.

Також ВОІВ допомагає країнам, що розвиваються, в їх нарощуванні ІВ-потенціалу, проводячи консультації щодо інкорпорування відповідних політик у національні стратегії розвитку та створення якісної сучасної законодавчої бази у сфері інтелектуальної власності.

Організація намагається об'єднати зацікавлені сторони у відповідних питаннях, для чого формуються державно-приватні партнерства, створюються спеціальні спільні платформи. Все це робиться для того, щоб змусити інновації працювати над пошуком рішень глобальних проблем, таких як продовольча безпека та зміни клімату. ВОІВ проводить різні емпіричні дослідження відомостей та статистики, на підставі яких надалі надає владі та компаніям-гегемонам зважені та корисні дані, без яких не обійтися у процесі прийняття рішень про використання інтелектуальної власності. Співробітники організації, держави-члени та інші зацікавлені сторони мають єдину мету - впровадити ефективну та доступну систему інтелектуальної власності, яка працює на благо всіх [210].

Організаційна структура цієї Всесвітньої організації включає вісім секторів, очолюваних заступниками та помічниками Генерального директора, під чийм керівництвом вони і функціонують. При цьому кожен сектор складається з кількох відділів чи департаментів, які відповідають за реалізацію окремих програм та спеціальних заходів. Так, сектор авторського права та творчих галузей має відділи як безпосередньо по АП, так і окремий відділ поширення інформації та цифрового контенту. Сектор брендів і зразків включає департамент товарних знаків, промислових зразків і географічних зазначень, а також Гаазький і Мадридський реєстри. Також діють сектор регіонального та національного розвитку, сектор адміністрації, фінансів та управління, у складі якого виділяється департамент інформаційно-комунікаційних технологій, сектор патентів та технологій, сектор глобальних завдань та партнерств. Окремо відзначимо сектор екосистем ІВ та інновацій, до складу якого входять також департамент економічної інформації та аналізу даних, департамент ІВ для новаторів, а також Центр ВОІВ з арбітражу та посередництва та Судовий інститут Організації.

ВОІВ сьогодні - загальноприйнятий координатор, який очолює активності щодо формування збалансованої та ефективної системи ІВ, що забезпечить сприятливі умови для інновацій та творчості на благо кожного. І у зв'язку із зазначеним не оминула організація своєю увагою й питання захисту ІВ у кіберпросторі.

У цьому питанні особливу роль відіграє служба цифрового доступу ВОІВ (англ. *WIPO Digital Access Service, DAS*), особлива електронна система для безпечного обміну документами між відомствами з інтелектуальної власності. Це сприяє виконанню заявниками та іншими суб'єктами вимог Паризької конвенції щодо сертифікації в електронному середовищі.

Також була введена в дію онлайн-платформа *WIPO ALERT*, куди держави-члени організації завантажують дані про веб-ресурси, які порушують авторське право згідно із національним законодавством. Такий сервіс особливо популярний серед суб'єктів реклами, адже отримана на платформі інформація допомагає їм уникнути розміщення на сайтах-порушниках реклами автоматизованим способом. В іншому випадку таке могло б призвести до порушення авторських прав і заподіяння шкоди репутації клієнтів таких рекламних суб'єктів.

Онлайн-платформа *WIPO Match* допомагає налагодженню взаємодії із потенційними постачальниками ІВ, тим самим використовуючи потенціал промисловості та приватного сектора для економічного, соціального та культурного розвитку держав із перехідною економікою та подібних їм. Суть платформи – у сприянні здобувачам технічної допомоги у сфері інтелектуальної власності шляхом пошуку донорів для реалізації відповідних проектів.

Обмін технологіями у боротьбі зі зміною клімату здійснюється за допомогою онлайн-платформи *WIPO GREEN*. У ній беруть участь постачальники та шукачі екологічно безпечних технологій. *WIPO Re:Search* допомагає обміну даними та ноу-хау (на безоплатній основі) між організаціями та кваліфікованими дослідниками по всій земній кулі з метою боротьби із тропічними хворобами та туберкульозом.

Не менш важливими є документи ВОІВ у сфері, що розглядається. І такими насамперед є "Інтернет-договори ВОІВ" (англ. *WIPO Internet Treaties*), а саме: Договір з авторського права (ДАП) від 20 грудня 1996 р. (чинний з 6 березня 2002 р.) та Договір про виконання та фонограми (ДВФ) від 20 грудня 1996 р. (чинний з 20 серпня 2002). Ці два нормативно-правові акти стали відправною точкою формування міжнародного законодавства з ІВ у кіберпросторі. Так, у 1996 р. була скликана Дипломатична конференція ВОІВ, основною темою якої був пошук рішень у зв'язку зі зростаючою

кількістю випадків неправомірного використання цифрових об'єктів інтелектуальної власності у цифровому ж середовищі. В рамках заходу і було прийнято два зазначені документи.

На переконання деяких спеціалістів, ці договори показали себе досить суперечливими і такими, що не змогли радикально змінити ситуацію на користь правовласників [309; 194, с. 192]. Але все ж таки відповідним суб'єктам вдалося хоч трохи обмежити вільне відтворення та розповсюдження цифрових інтелектуальних об'єктів, адже країни-учасниці договорів включили окремі їхні положення до свого законодавчого масиву, визнавши неправомірним розміщення захищених об'єктів у всесвітній мережі без дозволу правовласників [194, с. 227-239]. Головне протиріччя ДАП та ДІФ, на нашу думку, полягає у тому, що охорона технічного захисту інтелектуального об'єкта не дозволяє його використання у випадку, якщо таке використання дозволено, наприклад, трирівневим критерієм. Таким чином, спочатку треба зняти захист з об'єкта, а це заборонено.

Варто розглянути детальніше основні положення зазначених договорів щодо використання інтелектуальної власності у кіберпросторі. Норми обох документів можна умовно класифікувати за трьома групами:

- охорона "сучасних" авторсько-правових об'єктів (комп'ютерні програми, бази даних);
- охорона авторських та суміжних прав у цифрових мережах;
- охорона "нових" прав відповідних суб'єктів (право на поширення та на прокат).

Тепер більш детально розглянемо конкретні норми. Договір ВОІВ про виконання та фонограми поширює свою дію на два типи суб'єктів - виконавців та виробників фонограм. Глава II ДВФ присвячена правомочності перших, наділяючи їх особистими немайновими правами (бути визнаним виконавцем конкретного твору та забороняти будь-яке його спотворення - Стаття 5), а також майновими, як то: дозволяти ефірне

мовлення та повідомлення, а також запис своїх незаписаних об'єктів (Стаття 6); право на відтворення (Стаття 7); на розповсюдження (Стаття 8); на прокат (Стаття 9) та право робити записані виконання доступними (Стаття 10). Глава III ДВФ (статті 11-14) наділяють виробників фонограми правом зробити фонограми доступними, а також правами на прокат, розповсюдження та відтворення.

Так, у статті 7 ДВФ, присвяченій праву на відтворення, декларується виключне право виконавців дозволяти відтворення своїх виконань-фонограм "будь-яким чином і в будь-якій формі". Аналогічним правом Статтею 11 наділені виробники фонограм. Стаття 16 дозволяє країнам-учасникам приписувати у своєму національному законодавстві обмежувальні норми для захисту прав виконавців та виробників фонограм, аналогічні нормам із охорони авторського права на твори. А обмежувальні норми ДВФ будуть включені у національні закони лише без шкоди "нормальному використанню виконання або фонограми" без обмеження інтересів відповідних суб'єктів. При цьому право на відтворення за змістом статей 7 і 11 та винятки щодо цього права за статтею 16 в рівній мірі повинні застосовуватися у цифровому середовищі та щодо використання об'єктів у цифровій формі. Відтворенням в такому випадку вважається і зберігання контенту, що охороняється, у цифровій формі на (в) електронному пристрої. Стаття 18 зобов'язує сторони Договору передбачати належну "правову охорону та ефективні засоби правового захисту від обходу існуючих технічних засобів", які правосуб'єкти використовують з метою здійснення своїх прав по ДВФ для обмеження протиправних дій щодо їх інтелектуальних об'єктів. Строк охорони на об'єкти регулювання становить щонайменше 50 років, відповідно до Статті 17 [23]. Але варто відмітити, що якихось конкретних обмежень щодо використання об'єктів творчості в цифровому середовищі Договір про виконання і фонограм не встановлює,

вказуючи лише на заборону протиріччя виключення із охорони "нормальному використанню".

Договір ВОІВ з авторського права зобов'язує країну-учасницю, навіть якщо вона не пов'язана зобов'язаннями за Бернською конвенцією 1886 р, дотримуватися основних положень Паризького Акту 1971 р. цієї конвенції. ДАП регулює відносини з охорони авторсько-правових об'єктів та прав авторів у цифровому домені. Крім стандартних художніх та літературних творів Договір поширюється на комп'ютерні програми (Стаття 4) та бази даних (Стаття 5), якщо компіляція таких є результатом інтелектуальної творчості. Згідно зі статтями 6-8 ДАП, автори наділені правами на розповсюдження, прокат та доведення до загального відома (це крім тих прав, що декларує Бернська конвенція). Варто зазначити, що зазначене право на повідомлення для загальної інформації надає автору правомочність дозволити таке повідомлення по проводах та бездротовим способом, у т.ч. таким, «при якому представники публіки можуть мати доступ до таких творів з будь-якого місця та у будь-який час на їхній власний вибір», відповідно йдеться про передачу через всесвітню мережу. Стаття 10, як і стаття 16 ДВФ, містить норму про так звану «триступеневу перевірку» про застосовність обмежень у контексті статті 9(2) Бернської конвенції. Узгоджена заява до цього Договору декларує можливість поширення обмежень та вилучень за національним законодавством на цифрове середовище, при цьому країни-учасниці мають право встановлювати інші обмеження, які можуть бути використані у цифровій сфері. Зобов'язання щодо технічних заходів, аналогічні тим, що зазначені у статті 18 ДВФ, містяться й у статті 11 ДАП.

Зазначимо, що в Узгодженій заяві до статей 6 і 7 ДАП, так само як і в аналогічному документі до статей 2(е), 8-9, 12-13 ДВФ, чітко зазначено, що поняття «копія» у контексті права на поширення та прокат має на увазі виключно фізичну копію творчої роботи, яка знаходиться в обігу як

«відчутний» об'єкт. Відповідно, можна зробити висновок про те, що інтернет-договори не вважають два зазначені види прав застосовними у телекомунікаційних діджитал-мережах і сайтах, а, отже, і не відносять їх до прав у кіберсередовищі.

Окремі особливості в розумінні інтернет-договорів має і право на відтворення, яке логічно сприймається як найбільш застосовне у цифровому домені. Нагадаємо, що це право передбачає можливість створення копій наявного твору. Але, у разі, коли має місце інтернет-передача даних, завжди відбувається проміжне їх копіювання у пам'ять сервера, через який користувач виходить в Мережу. Але, якщо щоразу запитувати дозвіл автора на таке копіювання, то система просто "ляже", адже сервер буде перевантажений, а користувач - не отримає доступ до необхідної веб-сторінки. Обговорення з цього питання велися тривалий час, але будь-яких видимих результатів вони не принесли, тому в ДАП так і не були включені спеціальні положення щодо права автора на відтворення у цифровому полі.

На нашу думку, зміст ДВФ і ДАП логічно розглядати в більш широкому сенсі, ніж просто договори, що охоплюють «цифрове середовище». Такі НПА насправді ввели нові правові норми, які застосовуються до об'єктів у будь-якій формі, як то в діджитал чи аналоговій. Можна стверджувати, що інтернет-договори ВОІВ не наголошують на виділенні Всесвітньої мережі в особливу цифрову мережу серед собі подібних, відповідно, їх положення в рівній мірі будуть застосовані і в інших цифрових сферах.

Окремо варто звернути увагу на п.2 ст.5 ДАП, який дослівно повторює п.2 ст.5 Бернської конвенції. Відповідно до зазначеної норми, «...крім встановлених цією Конвенцією положень, обсяг охорони, а також засоби захисту, що забезпечують автору охорону його прав, регулюється виключно законодавством країни, в якій потрібна охорона» [22]. Таким

чином, має місце дублювання норми без включення до неї додаткових положень про право, яке застосовувалося б до відносин з використання творчого контенту в кіберсередовищі. Ця особлива тенденція у вигляді територіальності характеру авторських та суміжних прав у симбіозі з принципом національного режиму, який використовується як основний у ході міжнародної охорони прав авторів, нашоюхує нас на висновок про необхідність застосування судом у спірних ситуаціях свого локального права.

Незважаючи на очевидні недоліки, ДАП та ДВФ, все ж таки, є одними з перших міжнародних правових документів, які зобов'язали Договірні Сторони передбачити засоби правового захисту від обходу технічних засобів, що і зараз допомагає правовласникам у захисті своїх прав. На позитивну оцінку заслуговує і особлива гнучкість формулювань, що використовується в інтернет-договорах ВОІВ, наприклад, щодо права на доведення до загального відома, де така характеристика відчутно спрощує включення відповідних норм до національного законодавства держав-членів.

У подальших спробах покращити регулятивну ситуацію робочими групами було запропоновано різні основи та методики як на національному, так і на міжнародному рівнях, для забезпечення загального доступу до кібернетичного простору, метою чого було формування та забезпечення функціонування транспарентного, полікультурного інформаційного суспільства.

У контексті регулювання відношення інтелектуальної власності в кібернетичному просторі також важливо згадати про так званий Дослідницький процес ВОІВ, який мав місце в рамках Організації з 1998 у вигляді широкої міжнаціональної акції консультацій на підставі пропозиції уряду США. Метою даного заходу була розробка для Інтернет Корпорації з присвоєння імен та номерів (ICANN) відповідних рекомендацій у взаємодії

доменних імен та прав на інтелектуальну власність. В результаті великої кількості консультативних нарад було прийнято Єдину Політику Розгляду Спорів про доменні імена (англ. *Uniform Domain Name Dispute Resolution Policy, UDRP*) і Правила до неї. Дані акти відіграють особливу роль у вирішенні доменних суперечок між власниками товарних знаків та адміністраторами доменів, вони також були розроблені ВОІВ, а прийняті - ICANN. Вони будуть розглянуті далі, у Розділі 4.2.2 даного дисертаційного дослідження.

На закінчення зазначимо, що інтернет-договори ВОІВ і сьогодні залишаються важливими регулятивними інструментами у сфері захисту та охорони прав на об'єкти інтелектуальної власності в інтернеті та взагалі кіберпросторі. У подальших спробах покращити регулятивну ситуацію робочими групами було запропоновано різні основи та методики як на національному, так і на міжнародному рівнях, для забезпечення спільного доступу до кібернетичного простору, метою чого було формування та забезпечення функціонування транспарентного полікультурного інформаційного суспільства. Сьогодні основна регулятивна діяльність ВОІВ щодо кібернетичного домену націлена в більшості своїй саме на такий об'єкт ІВ як доменні імена.

4.2.2. Internet Corporation for Assigned Names and Numbers (ICANN)

Як було зазначено в попередньому Розділі 4.2.1 даного дисертаційного дослідження, особливе значення для розвитку регулювання кібер-відносин у контексті інтелектуальної власності мав дослідницький Процес ВОІВ, Заключний звіт по якому містив важливі рекомендації для ефективного вирішення особливо серйозних проблем між інтелектуальною власністю та доменними іменами. Також залишалася на той момент низка

невирішених питань, які вимагали додаткових консультацій. Серед них варто назвати:

- проблему несумлінності у сфері реєстрації доменних імен, які порушують права не тільки на ТМ, але й на географічні зазначення та подібні інтелектуально-правові об'єкти;
- аналогічну проблему недобросовісності з використанням під час реєстрації доменного імені акронімів міжнародних міжурядових організацій або міжнародних непатентованих імен, відібраних ВООЗ щодо деяких ліків за допомогою єдиних загальноновизнаних імен з метою захисту пацієнтів;
- введення в дію некомерційних доменів з обмеженим використанням, щодо яких контактні дані домено-власників обмежені у доступі для широкого загалу [77].

І тут на перший план виходить Інтернет-корпорація з присвоєння імен та номерів, також іменована Корпорацією з управління доменними іменами та IP-адресами (англ. *Internet Corporation for Assigned Names and Numbers, ICANN*), куди і був представлений зазначений вище Заключний звіт. До складу цієї некомерційної громадської корпорації увійшли люди з усього світу з єдиною метою - "забезпечити безпеку, стабільність та функціональну сумісність Інтернету" [214]. Ця організація активно розробляє та впроваджує політики щодо доменних імен як унікальних ідентифікаторів всесвітньої мережі, тим самим змушуючи Інтернет розширюватись та розвиватись.

Зазначені політики ґрунтуються на принципі "мультистейкхолдеризму", тобто моделі діяльності за участю багатьох зацікавлених сторін. Суть її в імітації структури всесвітньої мережі без фізичних кордонів і відкритої для кожного. Дана Інтернет-корпорація була сформована американським урядом та Міністерством торгівлі США. Її діяльність полягає в координації системи доменних імен в інтернет-мережі,

управлінні IP-адресами та номерами автономних систем, їх протоколами. На даному етапі функціонування ICANN вже управляється саме співтовариством, хоч і була спочатку створена урядом, вона активно співпрацює з диверсифікованими зацікавленими сторонами, а саме великими компаніями, цілими урядами та окремими фізособами, щоб Інтернет процвітав [200].

Щорічно в рамках Корпорації проводяться три зустрічі, в рамках яких обговорюється і затверджується майбутня глобальна політика, тенденції розвитку інтернет-мережі, приймаються важливі рішення. Авторка цього дисертаційного дослідження у 2017 році стала учасницею програми NextGen, а також двічі стипендіатом програми ICANN Fellowship (2017-2018 рр.).

Не варто думати, що Корпорація керує вмістом Інтернету, це не так. Організація не може, наприклад, перешкоджати поширенню спаму електронною поштою і надати доступ до всесвітньої мережі, вона саме координує систему присвоєння імен в ній. ICANN керує системою акредитації щодо реєстраторів доменних імен та адмініструє IP-адреси, у т.ч. для того, щоб не виявилось двох однакових IP-адрес, і є їх центральним репозиторієм. Таким чином, Корпорація швидше "спостерігає" за величезною мережею унікальних інтернет-ідентифікаторів.

У складі організації багато груп, що представляють різні сфери Інтернету. Так, у Корпорації є три "підтримуючі організації", це представники тих організацій, які працюють з доменами, з IP-адресами та менеджери країнових доменів вищого рівня. Також у складі ICANN чотири консультативні комітети, що надають їй консультації та рекомендації, до них входять уряди та міжнародні організації, організації-суб'єкти забезпечення безпеки Мережі, оператори корневих серверів та сама спільнота, тобто люди, кінцеві користувачі. Також є спеціальна Технічна група, яка співпрацює з організаціями з розробки протоколів для кібер-

технологій. Головні рішення ухвалює Рада директорів у складі 21 члена. Ще у Корпорації є Президент та Голова правління, а також у її рамках діє Відділ урегулювання спорів.

Важливим аспектом є питання зовнішньої відповідальності Корпорації. Так, вона є організацією, що підпорядковується законам штату Каліфорнія. Відповідно, організація підпорядковується законам США, проти неї можуть подаватися позови, і вона може бути притягнута до відповідальності судовою системою. Також, з урахуванням некомерційної форми, її директори несуть відповідальність за виконання своїх обов'язків у відповідності до законодавства про некомерційні організації. Також ICANN несе "внутрішню" відповідальність перед спільнотою відповідно до свого Статуту [307].

26 серпня 1999 р. в Чилі Радою директорів ICANN була прийнята Єдина політика вирішення спорів про доменні імена (скорочено - ЄПВС, англ. *Uniform Domain Name Dispute Resolution Policy, UDRP*), в основі якої і лежали раніше згадані рекомендації зі Звіту по дослідницькому процесу ВОІВ з питання доменних імен; були враховані також коментарі доменних реєстраторів та інших зацікавлених сторін. UDRP створила міцну правову основу для вирішення спорів між реєстрантами доменного імені (тобто власником реєстрації) та третіми сторонами. З того моменту всі акредитовані Корпорацією суб'єкти, уповноважені реєструвати загальні та національні домени верхнього рівня, що прийняли ЄПВС, висловили свою згоду дотримуватись та застосовувати цю Політику у спорах щодо зазначених типів доменів.

Єдина політика визначає процедури та інші вимоги для кожного з етапів проходження адміністративної процедури при вирішенні доменного спору, це, по суті, набір керівних принципів. Адмініструють процедуру акредитовані Корпорацією так звані постачальники послуг з вирішення спорів, до яких належить і Центр ВОІВ з арбітражу та посередництва. Саме

він, виступаючи технічним консультантом, розробив Додаткові правила ВОІВ до ЄПВС (Правила ЄПВС), що доповнили Політику та набули чинності з 14.12.2009 [298].

UDRP спочатку створювалася для захисту загальновідомих брендів та товарних знаків у разі неправомірної реєстрації сторонніми суб'єктами доменного імені, подібного до ступеня змішування, з метою отримання комерційної вигоди. Важливо відзначити, що Політика застосовна до всіх ccTLD і gTLD, які добровільно прийняли її. Додаткові правила ВОІВ застосовуються лише за певних обставин та до окремо взятих доменів вищого рівня.

Політика та Правила до неї поширюються на суперечки, що підлягають обов'язковому адміністративному розгляду, якщо у скарзі за ними вказується на такі умови:

- має місце завдання шкоди ТМ внаслідок реєстрації ідентичного або подібного до ступеня змішування доменного імені;
- власник такого ДІ недобросовісно його використовує;
- він також не має відповідних інтересів щодо цього доменного імені.

При цьому існує три основні обставини, що свідчать про несумлінну реєстрацію, а саме:

1. реєстрація ДІ провадиться із метою подальшого продажу, передачі в оренду спірного імені за велику суму грошей постраждалій стороні (зазвичай це власник відповідного товарного знака);
2. реєстрація ДІ провадиться з метою заподіяння шкоди бізнесу іншої сторони;
3. ДІ використовується для навмисного введення в оману та “приведення” потенційних клієнтів на електронний ресурс порушника або інші сайти з метою отримання комерційної вигоди [297].

Застосування Політики ЄПВС при виникненні спору про доменне ім'я здійснюється у простий та зрозумілий спосіб: спочатку власники доменних імен, з метою реєстрації такого об'єкта, укладають договір про реєстрацію з акредитованим Корпорацією реєстратором. У документі обов'язково вказується на застосовність Політики для врегулювання виникаючих доменних спорів. Рішення відповідно до ЄПВС далі приймають у відповідності до особливих процедурних правил, при цьому посилання на такі правила також обов'язково вказується у реєстраційному договорі. Таким чином, Політика є важливим елементом організації охорони електронних веб-ресурсів. Вона забезпечує якісне, швидке і не надто витратне вирішення спору про домен у позасудовому порядку. Більш детально процедура і особливості застосування Політики в умовах України будуть розглянуті у Розділі 5 даного дисертаційного дослідження.

Окремо варто вказати на методикау прийняття рішень щодо регулювання інтернету, як основи кіберпростору, в рамках ICANN. Так, якщо проблема потребує технічних змін у всесвітній мережі, то застосовуватиметься спрощена процедура за такою схемою:

1. Підтримуюча організація виносить відповідне питання на розгляд, зазвичай, на підставі звіту одного з консультативних комітетів.
2. Далі такий звіт доводять до відома громадськості. У випадку, якщо порушена проблема та відповідні зміни стосуються іншої групи в системі ICANN, то ця група, після ознайомлення із передбачуваними змінами, висловлює свою думку. Після цього досягнуті результати обговорення виносять на розгляд громадськості повторно.
3. Процес завершується передачею підсумкового звіту із рекомендаціями на розгляд Раді директорів ICANN. Цей орган схвалює зміни, або їхню частину, або відхиляє всі зміни, або повертає звіт організації-ініціатору із поясненням необхідності врегулювання певних моментів.

4. Тепер процес повторюється, доки всі зацікавлені сторони не погодяться зі змінами, і завершується їх прийняттям Радою директорів ICANN [307].

У контексті ICANN також важливо згадати Адміністрацію адресного простору Інтернет (англ. *Internet Assigned Numbers Authority, IANA*), відому ще з 1970-х років. Сьогодні її послуги надаються в рамках *Public Technical Identifiers* (далі - *PTI*), як підконтрольного Корпорації органа. У зв'язку із закінченням на 1 жовтня 2016 року терміну дії договору про виконання функцій адміністрації адресного простору всесвітньої мережі IANA й перейшла до рук ICANN. Адміністрація адресного простору виконувала функцію управління просторами IP-адрес та доменів верхнього рівня, була відповідальна за розподіл усіх зарезервованих доменних імен, які використовуються в протоколах, визначених у RFC. Разом із операторами ДВР вона керувала даними корневих серверів ДНС. Зараз РТІ відповідає за "операційні аспекти координації унікальних мережевих ідентифікаторів та підтримку довіри співтовариства до надання таких послуг безстороннім, відповідальним та ефективним чином" [130].

РТІ не встановлює політики своєї діяльності безпосередньо, а лише реалізує узгоджені політики та принципи на підставі принципу нейтральності. Корпорація ICANN надає спеціальні форуми для встановлення таких політик для операцій з доменними іменами та IP-адресації, до впровадження яких також залучаються інші зацікавлені сторони. До завдань РТІ віднесено й інформаційно-роз'яснювальну роботу з операторами TLD, регіональними інтернет-реєстратурами та іншими зацікавленими групами. Цей орган здійснить координацію із забезпечення безперебійної роботи Всесвітньої мережі, зокрема:

- управляє корневим DNS-сервером, доменами .int та .агра, ресурсом практики інтернаціоналізованих доменних імен;

- разом із органами стандартизації керує системами нумерації інтернет-протоколів;
- координує глобальний набір номерів IP та AS [307].

Отже, Корпорація ICANN відіграє важливу роль у захисті одного з основних об'єктів інтелектуальної власності в кіберпросторі - доменного імені. Завдяки діяльності даного суб'єкта як спостерігача за об'єднаною мережею унікальних ідентифікаторів, за допомогою яких комп'ютери в кібернетичному домені "знаходять" один одного, ми маємо можливість користуватись благами інтернет-мережі. А Політика вирішення доменних суперечок зараз дуже успішно застосовується у багатьох країнах, зокрема й в Україні.

4.2.3. Internet Society, World Wide Web Consortium та інші суб'єкти

У кіберпросторній екосистемі не менш важливу роль відіграє засноване в 1992 р. **Товариство (Суспільство) Інтернету** (англ. *Internet Society, ISOC*). Ця міжнародна професійна організація активно розвиває та забезпечує доступність Інтернету для всіх і кожного. ISOC стало основою та забезпечує організаційну інфраструктуру для широко ланцюга консультативних та дослідницьких груп, що також здійснюють активності з розвитку всесвітньої мережі. Товариство було створено для підтримки процедури розробки інтернет-стандартів та вирішення питань, що постають перед майбутнім інтернет-мережі. Планування інтернет-політики в Internet Society базується на таких поняттях як Кодекс поведінки в Інтернеті, Закон про Інтернет та інтернет-Екосистема [265].

Виступаючи за наскрізне шифрування, ISOC здійснює публікацію звітів про глобальні проблеми всесвітньої мережі, а також виробляє інструменти, розробляє кодекси та рекомендації для покращення її використання. Діяльність Товариства пов'язана також з *MANRS* (від англ. *Mutually Agreed Norms for Routing Security* – Взаємно узгодженими нормами

безпеки маршрутизації), ці норми розпочали свою дію у 2014 році з метою виправлення проблем, спричинених поширенням загроз інфраструктурі маршрутизації Інтернету. ISOC веде активну діяльність у всьому світі. Так, ним було організовано Африканський форум з пірингу та взаємодії (англ. *Africa Peering and Interconnection Forum, AfPIF*) для розвитку африканської інтернет-інфраструктури. Ще воно сформувало Реєстр громадських інтересів (англ. *Public Interest Registry, PIR*) з метою управління та використання реєстру .org [129].

У складі Товариства – понад 100 організацій-членів практично з кожної держави, а також не менше ніж 20 тисяч індивідуальних членів. Internet Society - некомерційна освітня організація, що забезпечує доступність Інтернету у світовому масштабі. Крім інформаційно-освітньої активності, Товариство також координує та фінансує громадські ініціативи з питань Інтернету, а також веде мережеву статистику, проводить опитування та маркетингові дослідження.

Управляє Internet Society опікунська рада, члени якої призначаються департаментами (англ. *Chapters*) Товариства, безпосередніми його членами та робочою групою IETF (аббр. від англ. *Internet Engineering Task Force*). Останній суб'єкт представляє собою відкрите міжнародне співтовариство провайдерів, вчених, проектувальників, учених та мережевих операторів, в його функції входять активності з розвитку протоколів та архітектури всесвітньої мережі. Його співробітники займаються виявленням та наданням пропозицій щодо рішень в технічних аспектах організації Інтернету, розробкою угод та стандартів щодо загальних архітектурних принципів протоколів Мережі, а також рекомендацій щодо стандартизації таких протоколів тощо. Місія даної робочої групи - покращення Інтернету саме з інженерної точки зору.

Товариства разом з IETF наприкінці 2020 р. оголосили про нову стратегічну угоду для підтримки поточної роботи над відкритими

стандартами на довгостроковій основі. Така угода має забезпечити безперервність критичної роботи IETF у процесі розробки стандартів для покращення роботи Всесвітньої мережі. Документ набув чинності з 01.01.2021 р. і діятиме до 31.12.2026 [286].

ISOC також надає свої рекомендації з міжнародних договорів, у тому числі щодо інтелектуальної власності у кібернетичному домені. Так, на Торговельну угоду проти контрафакту (англ. *Anti-Counterfeiting Trade Agreement, ACTA*) 2011 р. Товариство надало свій висновок, який зводився до стурбованості потенційним впливом угоди на розвиток та законне використання Всесвітньої мережі. Окремо спікери наголосили на необхідності підтримання прозорості та справжньої участі багатьох зацікавлених сторін АСТА. Адже Інтернет, як унікальна платформа для інновацій, має бути відкритим, щоб і надалі розвиватися успішно; тільки так можна забезпечити постійні інновації та інвестиції в нього, а разом з ним - і до пов'язаних економічних, соціальних і культурних переваг. Представники Товариства наполягали на тому, що рішення відносно методик захисту права інтелектуальної власності в онлайн-середовищі актуальне рівною мірою для всієї інтернет-спільноти, а не тільки для урядових структур та власників інтернет-контенту [218].

В рамках Workshop 146, організованого ISOC заходу, було піднято важливе питання щодо сумісності "класичних" прав інтелектуальної власності з обміном та перерозподілом контенту та інтелектуальних товарів через Всесвітню мережу. Під час обговорень виділилися два підходи. Прихильники першого виступали за суворе дотримання прав ІВ з метою захисту від піратства результатів творчості авторів та правовласників. Послідовники другого підходу наполягали на скасуванні прав на ІВ та за впровадження альтернатив для врівноваження прав творців та кінцевих користувачів таких інтелектуальних творів. Вони наполягали на законному обміні файлами, але рішуче виступали проти "драконівських" методів

захисту відповідних прав. Основною ідеєю такого було неминуче придушення інновацій у разі запровадження суворих покарань за доступ до захищеного контенту, а з ним - і прогрес соціальної несправедливості, наприклад, через відсутність доступу до необхідних медикаментів у малозабезпеченого населення. У ході обговорень було досягнуто розуміння щодо непопулярності жорсткого правозастосування та необхідності пошуку альтернативних бізнес-моделей, наприклад, за типом Creative Commons і Open Source [242].

Також Інтернет-спільнота висловила занепокоєння можливим заподіянням шкоди всесвітній мережі у разі прийняття Угоди про транстихоокеанське партнерство (англ. *Trans-Pacific Partnership (TPP)*, *Trans-Pacific Partnership Agreement*) 2016 р. Цей акт містив у собі норми щодо тарифних та нетарифних бар'єрів у торгівлі та розробки механізму врегулювання суперечок між інвесторами та державами. У ній також містилося особливе Положення про права інтелектуальної власності. Представники ISOC наполягали на тому, що його положення не узгоджуються із основними принципами верховенства права, прозорості, пропорційності, належної правової процедури та підзвітності. Окрім зазначеного, прийняття Угоди могло б призвести до негативних наслідків для конфіденційності в Інтернеті, що важливо для безпеки кінцевих користувачів. Так, у відношенні відповідальності посередників, норми декларують нові рівні відповідальності для приватних осіб та створюють основу для жорсткої фільтрації контенту; у разі блокування таких матеріалів буде порушено право на онлайн-вираз. Все зазначене безсумнівно негативно вплинуло б на інновації, гальмувало б творчість, процвітання та економічну взаємодію [216].

Також для Товариства важливо, щоб суб'єкти, що визначають політику, розвивали політичні підходи у відповідності із принципами ефективності. Як приклад такого пропонується те, що рішення щодо

захисту прав ІВ не повинні суперечити базовій архітектурі всесвітньої мережі, оскільки технології можуть сприяти захисту таких прав іншими способами, але до таких не належить правозастосування. У цьому контексті згадуються одіозні акти SOPA, PIPA та ACTA, внаслідок яких позначився суттєвий розкол між технологічною, політичною та мультистейкхолдерною сторонами.

У зв'язку із зазначеним ISOC запропонував розробити набір мінімальних стандартів для вирішення питань інтелектуальної власності. При цьому важливо під час дискусій встановити міру впливу Інтернету на права інтелектуальної власності та місце такого права в його екосистемі. Участь та залучення багатьох зацікавлених сторін, прозорість, верховенство закону, повага до архітектури Інтернету та підтримка його відкритих стандартів є тими рішеннями, які мають бути встановлені в управлінні інтелектуальною власністю. Має місце відсутність інклюзивних структур для взаємодії із зацікавленими сторонами в галузі інтелектуальної власності. Не менше інклюзивності, для розвитку у зазначеному питанні, важливі транспарентність, дотримання верховенства права та поваги до архітектурного дизайну Всесвітньої мережі [230].

При створенні зазначеного документа для Товариства постало розуміння того, що обговорення інтелектуальної власності, незалежно від конкретного об'єкта, є частиною загального обговорення управління всією мережею Інтернет. Тому ISOC закликав зацікавлених суб'єктів впроваджувати політики щодо ІВ, які підпорядковувалися б таким мінімальним стандартам (принципам):

- **верховенство закону** - за розумінням Товариства до цього принципу включені рівноправність, правова визначеність, справедливість, належна правова процедура та право бути почутим кожного;
- **транспарентність** - про необхідність прозорості сказано у Женевських принципах (мається на увазі *Declaration of Principles*:

building the information society: a global challenge in the new millennium) і *Open Government Paradigm*, при цьому Товариство наполягає на включенні даного принципу в АСТА, ТРР і Всеосяжну угоду між Канадою та Європою (англ. *EU-Canada Comprehensive Economic and Trade Agreement, CETA*);

- **мультистейкхолдеризм** - у всіх дискусіях щодо питання ІВ беруть участь багато зацікавлених сторін;
- **"інновації без дозволу"** - при розробці та впровадженні нових політик та НПА у сфері ІВ основою має стати сучасна парадигма стандартів, що базується на принципах взаємної співпраці, балансу, консенсусу, доступності та подібних;
- **дотримання інтернет-архітектури** - протидія порушенням прав ІВ не має порушувати глобальну архітектуру або будь-яким чином обмежувати міжнародно визнані права [217, с. 1-2].

Як зазначалося раніше, Інтернет-спільнотою було створено **Реєстр громадських інтересів (PIR)**. Ця некомерційна організація була заснована в 2002 році для управління, покращення та розширення домену .org, головною ж її метою є служіння громадським інтересам в Інтернеті. Вона також – активний учасник ICANN. PIR запропонував надійну платформу та необхідні ресурси для створення безпечної та надійної інтернет-присутності. З січня 2003 р. організація стала офіційною відповідальною за експлуатацію домену .ORG з одночасним веденням офіційної бази даних усіх доменних імен у цьому домені [92].

Стандарти Інтернету - це також основа діяльності **Консорціуму Всесвітньої павутини (World Wide Web Consortium, також W3C)**. Дане міжнародне співтовариство залучає до розробки технічних веб-стандартів (протоколів та посібників) організації та громадськість задля досягнення своєї головної мети – повне розкриття потенціалу Світової мережі,

забезпечення її довгострокового зростання. Свою діяльність Консорціум здійснює на основі принципів відкритих стандартів та дизайну:

- інтернет для всіх - забезпечення можливості спілкуватися та вести діяльність у Мережі для кожного, незалежно від наявного ПЗ, обладнання, локації, мовної приналежності, фізичних чи розумових здібностей тощо;
- інтернет у всьому – від комп'ютера до побутової техніки [213].

15 вересня 2020 р. Консорціум ухвалив Патентну політику, яка регламентує використання патентів у процесі створення веб-стандартів. Мета її запровадження - гарантувати реалізацію Специфікацій на безоплатній основі (англ. *Royalty-Free*). Документи W3C мають ліцензії. Так, авторські права на документи Консорціуму належать первісним авторам документації. Ліцензія на програмне забезпечення W3C дозволяє модифікувати відповідні програми практично всім бажаючим [213].

Організація номерних ресурсів (англ. *Number Resource Organization, NRO*) - це некорпоративна організація, що об'єднує у собі 5 регіональних інтернет-реєстрів (англ. *Regional Internet registry, RIR*). Започаткована вона 24 жовтня 2003 р., коли 4 RIR, що існували на той момент, підписали Меморандум про взаєморозуміння з метою вести спільну діяльність, у тому числі шляхом координації відповідних політик. Організація номерних ресурсів надає захист нерозподіленим ресурсам IP-адрес, виступає за розробку інтернет-політик і виступає як координаційний центр для всієї інтернет-спільноти.

Регіональні Інтернет-реєстри - це особливі незалежні організації, що управляють розподілом та реєстрацією ресурсів інтернет-нумерації та технічно координують Інтернет-інфраструктуру у певних регіонах Землі. Членами RIR зазвичай є інтернет-провайдери, великі корпорації та телекомунікаційні структури. Сьогодні по всьому світу діють п'ять таких реєстрів:

- AFRINIC – країни Африки;
- APNIC – Східна Азія, Океанія, Південна та Південно-Східна Азія;
- ARIN - Сполучені Штати, Канада, Антарктида та частина Карибського басейну;
- LACNIC - велика частина Карибського басейну та Латинська Америка;
- Réseaux IP Européens (RIPE NCC) – Європа, Центральна та Західна Азія [254].

Отже, не можна не відзначити, що в останні десятиліття ідея узгодження прав інтелектуальної власності з вимогами та потребами кіберпростору, особливо Інтернету та пов'язаних технологій, займає особливе місце у ході більшості дискусій з управління Всесвітньою Мережею. Ми можемо спостерігати, як все частіше урядові структури використовують термін «цифровий суверенітет» з метою виправдати свої політики та дії щодо контролю за роботою Інтернету. На жаль, дедалі частіше помітні їхні спроби “накласти” географічні кордони на глобальний кібердомен. Саме тому роль неурядових організацій настільки велика, так само як і роль громадськості, яка активно “мешкає” в кіберпросторі. Ми щодня завантажуємо файли, що відносяться до об'єктів інтелектуальної власності, пересилаємо їх іншим респондентам, відвідуємо веб-сайти під певними доменними іменами і робимо подібне, саме тому важливо говорити і брати участь у розробці стандартів і політик у відношенні інтернет-мережі.

Безумовно, з появою Всесвітньої мережі як глобального засобу комунікації, творчості та інноваційної діяльності, так само як і зі зростанням ступеня доступності інформації (даних) традиційні концепції інтелектуальної власності сприймаються сучасним інформаційним суспільством як архаїчні та не особливо застосовні в кібердомені, де інформація є демократизованою, а людина отримала великі можливості для

творчості. Тому ще раз наголосимо на важливості обговорення політик та технологій, що зачіпають сферу інтелектуальної власності та її взаємодії з Мережею не лише на урядовому, а й на міжнародному рівні. Не менш актуальним залишається питання розробки стратегії щодо створення збалансованого зв'язку між інтернет-платформами та режимами інтелектуальної власності, чому б послужило створення та впровадження мінімальних уніфікованих стандартів у цій сфері.

Висновки до Розділу 4

У даному розділі дисертації на основі методу компаративістики було ретельно досліджено правові основи регулювання відносин дотримання права інтелектуальної власності у кібернетичному просторі в Сполучених Штатах Америки, країнах Європи та Співдружності Незалежних Держав. Окремо було проаналізовано та співставлено особливості діяльності суб'єктів міжнародно-правової охорони права інтелектуальної власності у кібернетичному домені. Отримані результати відповідного дослідження дали змогу дійти наступних висновків:

1. В світі існує загальна практика поділу авторського права на дві окремі системи - загальну, характерну для Великої Британії та Сполучених Штатів Америки, та систему цивільного права, якій слідує країни континентальної системи права. У першому випадку гарантуються тільки майнові права, авторське право прирівняно до форми власності; у другому - охорона розповсюджується і на майнові, і на немайнові ("моральні") права, адже творча діяльність творця вважається невід'ємною від його особистості, є її відображенням, а тому і потребує охорони на основі природної справедливості. Все це в рівній мірі стосується і об'єктів авторського права, що використовуються у кіберсередовищі.

2. В американському праві є чотири головні типи об'єктів інтелектуальної власності - патенти, авторські права, комерційні таємниці та товарні знаки, їх створення та використання врегульовані як федеральним законодавством, так і законодавством штатів, на них також поширює свою дію система загальноновизнаних міжнародних конвенцій. Таке законодавство передбачає традиційні цивільну та кримінальну охорону, а також прикордонний захист прав інтелектуальної власності. Саме правовласник в США несе відповідальність за цивільне правозастосування своїх прав інтелектуальної власності та може повідомити про її крадіжку в режимі онлайн шляхом звернення до веб-ресурсу Національного координаційного центру з прав інтелектуальної власності. Вважається за доцільне для українських нормотворців перейняти відповідний досвід у регулюванні правовідносин, пов'язаних із захистом та здійсненням прав власників інтелектуальної власності в кібернетичному просторі та інкорпорувати деякі відповідні положення американських нормативно-правових актів у національне законодавство.
3. Вважається за необхідне гармонізувати національне законодавство до більшості Директив ЄС, що стосуються захисту інтелектуальної власності в кіберпросторі. Також слід запозичити європейську методику превентивного захисту прав власників відповідних об'єктів інтелектуальної власності, яка передбачає відправку вимоги про видалення нелегального контенту з веб-ресурсу його власнику, а оператору зв'язку - про необхідність здійснити технічні заходи щодо закриття доступу до таких матеріалів. Правомірність відповідних дій вирішуватимуть українські суди.
4. Запропоновано, з метою подолання прогалів у законодавстві з інтелектуальної власності країн СНД, наступне: прийняти

одноманітний закон, який врегулює відносини інтелектуальної власності в кібернетичному домені, і який поширюватиме свою дію на всі держави-члени СНД. Також доцільно встановити та впровадити спеціальну підвідомчість спорів про захист виняткових прав при використанні контенту у кібернетичному просторі арбітражним судам. У системі цих органів для формування одноманітної практики у справах буде доречним створити Суд з інтелектуальних прав.

5. Визначено, що на міжнародному та регіональному рівнях функціонують різні організації, які займаються питаннями інтелектуальної особливості взагалі, та в кібернетичному домені зокрема. Регламентації відповідних відносин на міжнародному рівні певною мірою забезпечується "Інтернет-договорами" Всесвітньої організації інтелектуальної власності. Наразі вони є застарілими та такими, що не забезпечують всебічне регулювання відносин інтелектуальної власності у кібрдомені, але саме вони вважаються відправною точкою формування міжнародного законодавства про інтелектуальну власність у Всесвітній Мережі. Відповідно, на їх основі ЄС розробляє своє Директиви, і такі НПА стають прикладом для розробки законодавства в інших державах, зокрема, в Україні.
6. Зазначено, що Політика вирішення доменних суперечок (UDRP), що втілена в життя спільними діями BOIB та ICANN, показала себе як найбільш вдалий спосіб вирішення доменних суперечок через свою невисока затратність та процедурну легкість, зокрема в Україні.
7. Наголошено на важливості обговорення політик та технологій, що зачіпають сферу інтелектуальної власності та її взаємодії з Інтернетом не лише на урядовому, а й на міжнародному рівні задля недопущення спекулювання «цифровим суверенітетом» і обмеження кіберпростору географічними кордонами.

8. Вказано на актуальність розробки стратегії створення збалансованого зв'язку між інтернет-платформами та режимами інтелектуальної власності, для чого вважається за необхідне створити та впровадити (на глобальному рівні) мінімальних уніфікованих стандартів у відповідній сфері.

Результати дослідження, викладені у Розділі 4, відображено у таких публікаціях автора: [144]; [146]; [323]; [345]; [161]; [166]; [4228].

РОЗДІЛ 5. НАУКОВО-ПРАКТИЧНА ОСНОВА ФОРМУВАННЯ ЕФЕКТИВНОГО ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ДОТРИМАННЯ ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ У КІБЕРПРОСТОРИ

5.1. Нові підходи до формування правового забезпечення дотримання права інтелектуальної власності у кіберпросторі в Україні

Як вже було зазначено у попередніх розділах даного дисертаційного дослідження, в Україні простежується позитивна динаміка у формуванні правового забезпечення дотримання права інтелектуальної власності взагалі та безпосередньо у кіберпросторі, розробляються та втілюються в життя нові підходи до такого, правова база реформується з урахуванням сьогоденних викликів. І одним з проявів вказаного слід вважати вже зазначене у Розділі 3 набрання з 1 січня 2023 року чинності новою редакцією ЗУ № 2811-ІХ «Про авторське право і суміжні права» (від 01.12.2022). Слід більш детально розглянути новації даного НПА, особливо в розрізі саме кібернетичного середовища.

Так, внесення змін до Закону про авторське право 1993 року було зумовлене євроінтеграційним спрямуванням України, зокрема у частині імплементації положень НПА Євросоюзу у наше вітчизняне законодавство. Далі варто дослідити основні новели Закону про АП 2022 р. як загалом, так і щодо їх застосування при взаємодії із кібердоменом.

І першими слід розглянути ті, що містяться у Статті 1 Закону 2022 р., яка має назву "Визначення термінів" (Розділ I "Загальні положення". Так, з'явилося поняття музичного кліпу, яким, відповідно до п. 29 зазначеної статті, слід вважати аудіовізуальний твір, де "втілена візуальна інтерпретація музичного твору з текстом або без тексту, звуковий ряд якого містить запис виконання зазначеного музичного твору" [66]. Це допоможе більш якісно деталізувати перелік відповідних об'єктів АП.

Взагалі, відповідно до п. 56 Статті 1, твором слід вважати авторське творіння, у галузі мистецтва, науки, літератури, яке є оригінальним та втіленим в об'єктивну форму [66]. Попередній Закон, хоч і вказував на необхідність надання твору такої форми, але не мав конкретного визначення твору загалом. Також підкреслимо, що Стаття 1 у пункті 35 зазначає критерій охороноздатності твору - його оригінальність, яка характеризує відповідний твір "як результат власної інтелектуальної творчої діяльності автора та відображає творчі рішення, прийняті автором під час створення твору" [66]. Як відомо, Закон 1993 року такого критерію до робіт чітко не висував, натомість вимагалися творчий характер і об'єктивна форма вираження [67]. Тепер же можна говорити про заміну законодавцем творчого характеру на оригінальність.

В цьому зв'язку є вартою уваги справа *Eva-Maria Painer v. Standard VerlagsGmbH and others*. До Суду з позовом звернулася фотограф-фрилансерка, яка багато років поспіль заробляла на життя фотографуванням дітей (реалістичні портретні фото). Одну з її моделей, Наташу К. було викрадено, в ході розслідування чого було використано фото дитини, зроблене фотографкою. Коли Наташа К. змогла втекти з полону, багато ЗМІ використали спірні фото дівчини для висвітлення відповідних новин, в тому числі використовувався фоторобот, що був зроблений на основі спірного фото. Позивачка, крім іншого, вимагала, щоб ЗМІ, які використали її роботу, припинили відтворення та розповсюдження її творінь, а також виплатили їй винагороду за таке використання. Суд своїм рішенням надав тлумачення Статті 6 Директиви Ради 93/98/ЄЕС стосовно уніфікації термінів захисту авторського права і деяких суміжних прав від 29 жовтня 1993 року. Так, фотографію слід вважати фотографічним твором, а отже і об'єктом АП, якщо за її створення автором було використано оригінальні й унікальні прийоми фотографування, постановки або унікальні техзасоби. Фото буде вважатися оригінальним, якщо воно є власним

інтелектуальним творінням фізичної особи-автора, тим самим відображаючи його особистість, незалежно від мети тощо [226].

Щодо української практики, то унікальним є спір, що мав місце задовго до появи Закону 2022 р. Так, своєю постановою у справі № 918/5/14 від 19 серпня 2014 р. ВГСУ визнав самотійним об'єктом АП назву персонажа Капітошка, посилаючись на те, що така назва має оригінальний характер, відповідно, є результатом творчої діяльності фізичної особи-автора. І відтоді назва "Капітошка" може використовуватися окремо від зображення відповідного персонажа [64].

Є й інші нововведення у термінологічному апараті. Так, відеограмою, згідно п. 13 Статті 1 за новим Законом, є "вироблений (кінцевий) відеозапис виконання або інших зображень (із звуковим супроводом або без нього), крім відеозапису, що використовується у складі аудіовізуального твору" [66], в той час як старий Закон 1993 р. під цим терміном мав на увазі "відеозапис на відповідному матеріальному носії (магнітній стрічці, магнітному диску, компакт-диску тощо) виконання або будь-яких рухомих зображень (із звуковим супроводом чи без нього), крім зображень у вигляді запису, що входить до аудіовізуального твору" [67]. Таким чином, було збільшено перелік вірогідних творів-отримувачів правової охорони, бо тепер до них входить і відеозапис нерухомих зображень. Відповідний перелік біло збільшено і за рахунок включення до нього текстів перекладів для "озвучення, субтитрування аудіовізуальних творів іншими мовами" [66]. Стаття 8 попереднього Закону в п. 16 зазначала тільки тексти перекладів, що використовувалися для роботи із іноземними аудіовізуальними роботами [67].

П. 58 розширює поняття твору образотворчого мистецтва, а саме художнього дизайну, включивши сюди й накреслення (дизайн) шрифтів.

П. 55 Статті 1 надає визначення службовим творам, якими є ті, що були створені працівником у зв'язку із виконанням ним своїх трудових

обов'язків, тобто визначених у трудовому договорі (контракті) із ним. Раніше ж мова йшла про "твір, створений автором у порядку виконання службових обов'язків відповідно до службового завдання чи трудового договору (контракту) між ним і роботодавцем". Тепер же, Відповідно до ч. 3 Статті 14 роботодавець також може доручити іншій особі завершити незавершене службове творіння, або змінити уже готове, додати до нього перед- та післямову, графічні матеріали.

Щодо суб'єктів відповідних правовідносин, то варто відмітити, що за попереднім Законом автором визнавалася фізособа, що створила твір "своєю творчою працею" [67], у Новому ж Законі слово "праця" замінено на "діяльність" [66]. Якщо звернутися до Словника української мови 1980-80 рр., то працею вважається людська діяльність як сукупність цілеспрямованих дій, що потребують розумової енергії і націлені, крім іншого, на створення духовних цінностей [99, с. 522]. Діяльністю ж є "застосування своєї праці до чого-небудь" [98, с. 311].

Також на цікаву новелу вказує адвокат О. Мисенко. Так, п. 7 Статті 1 Закону 2022 р. не включає до категорії виконавців осіб, які виконують "циркові, естрадні, лялькові номери, пантоміми тощо", як то приписував Закон 1993 р. Однак артистів естради, цирку до виконавців зараховує Стаття 9 Римської конвенції про охорону інтересів виконавців, виробників фонограм і організацій мовлення 1961 року. Одночасно п.4 ч.1 Статті 6 Закону № 2811-ІХ такі об'єкти як циркові номери та пантоміми включені до об'єктів АП (п.4 ч.1 ст.6), тому логічно, що і виконавці вказаного будуть вважатися відповідними виконавцями за суттю Закону 2022 р. Тим не менш, статус виконавців естрадних й лялькових номерів не встановлено, а, отже, за новим Законом вони не є суб'єктами суміжних прав, що, на думку вказаного правознавця, є "звуження змісту та обсягу існуючих прав і свобод" відповідно до Статті 22 Основного закону нашої держави.

Натомість до переліку виконавців додано особу, що виконує "художній образ" (без визначення суті такого терміну) [53].

Додано і визначення сирітського твору, що не було відомо попередньому Закону. Таким, за п. 51 Статті 1 є оприлюднені в нашій державі творіння, фоно- та відеограми й виконання, щодо яких або не було ідентифіковано суб'єкта майнових прав, або місцезнаходження такого суб'єкта не вдалося встановити. Статус сирітського може отримати лише аудіовізуальне або творіння, що публікувалося у книзі, другоквантій пресі, письмових виданнях, яке "міститься в колекціях бібліотек, музеїв з відкритим доступом для відвідувачів, в архівах або організаціях із збереження фондів аудіо-, відеозаписів". Тобто, сирітські роботи вправі використовувати лише музеї, архіви тощо після невдачі у спробах ідентифікувати автора. Тим не менш, якщо автор сирітського твору з'явиться, то зможе відновити свої на нього права. Важливо також розуміти, що сирітський твір не є суспільним надбанням, і строк дії АП на нього не сплинув. Порядок ведення реєстру таких робіт, їх використання, ідентифікації потенційних авторів має визначити Кабмін [66].

Також Закон 1993 року у п. 10 Статті 8 серед об'єктів авторсько-правової охорони називав фотографічні твори і ті, що створені подібним способом, але конкретного визначення відповідного твору не надавав [67]. Відповідно ж до п. 63 Статті 1 Закону 2022 р. фотографічним вважатиметься "твір, статично відображений (зафіксований) із застосуванням аналогових, цифрових фотографічних технологій на матеріальному носії чи в електронній (цифровій) формі або із застосуванням лазерних технологій у вигляді об'ємного тривимірного зображення". Але, як конкретизує новий НПА, під охорону АП не підпадають фото без ознак оригінальності [66]. Останнє свідчить про те, що фотографія має бути зроблена з застосуванням авторського творчого підходу із залученням особливих технологій, про які зазначено в попередньому визначенні.

В контексті даного дисертаційного дослідження особливої уваги потребує п. 65 розглянутої статті, що надає визначення цифровому контенту ("електронна (цифрова) інформація"). Під таким слід розуміти дані та відомості, які містять об'єкти АП, суміжних прав у цифровій, електронній формі. Відповідний вміст можна зберігати й поширювати у зрозумілій користувачам цифрового простору формі файлів або їх частин, а також записів у базах даних на зберігаючих пристроях ПК, серверах чи у Всесвітній Мережі [66]. Варто взагалі відзначити, що новий Закон чітко деталізує можливість існування літературних творів не тільки в письмовій, але й в електронній, тобто цифровій та інших формах. Тобто надання авторській роботі електронної форми вважається створенням твору. Раніше такі відповідні твори теж охоронялися, але конкретної деталізації не було, натомість нині, через значну розповсюдженість робіт саме у цифровій формі, їм надали окреме місце серед об'єктів авторського права *de jure*, а не тільки *de facto*.

Цікавим є і доповнення, що міститься у п. 25 щодо інтерактивного надання доступу публіки до об'єкта АП й суміжних прав. Ним вважається поширення відповідних робіт по кабелю чи без його використання, в тому числі в Інтернеті та інших інтерактивних мережах. Відповідним поширенням буде також вважатися розміщення гіперпосилань чи цифрового вмісту одного веб-ресурса на іншому без його відтворення (тобто йдеться про так званий фреймінг, суть якого була розкрита у Розділі 3 даного дисертаційного дослідження). Уточнюється, що користувачі відповідного контенту мають отримати відповідний доступ з місця та у час за своїм власним вподобанням (індивідуально). При цьому у п. 19, присвяченому доведенню об'єктів АП та суміжних прав до загального відома, йдеться про те, що таким слід вважати поширення творів шляхом публічних виконань, показів, демонстрування чи сповіщення, а також зазначеного інтерактивного надання доступу тощо. У зв'язку із зазначеним наголосимо

й на наданому п. 44 визначенні терміну "публіка" як сукупності фізосіб, що не входять до кола сім'ї чи близьких знайомих користувачів об'єктів АП та суміжних прав [66].

Торкнувся новий Закон і такого електронного об'єкту як бази даних. Стаття 1 Закону 1993 р. містила відповідне визначення бази (компіляції) даних - сукупність творів, а Стаття 8 відносила її до відповідних об'єктів охорони АП [67]. Тим не менш, новий Закон у п. 17 Статті 6 уточнює, що об'єктом авторського права є саме "бази даних (компіляції даних), якщо вони за добром або упорядкуванням їх складових частин є результатом інтелектуальної діяльності" [66].

У п. 26 йдеться про комп'ютерну програму, яка тепер не просто є набором інструкцій у формі, придатній для зчитування комп'ютером, але й "настільним комп'ютером, ноутбуком, смартфоном, ігровою приставкою, смарт-телевізором тощо". Також стаття уточнює, що такою КП може бути операційна система, прикладна програма, виражені у вихідному або об'єктному кодах" [66]. До даного поняття так і не було включено попередні дослідні матеріали, як те зазначено у ч.1 Статті 180 Угоди про асоціацію між Україною та Євросоюзом, як не було зазначено, що КП має отримати охорону аналогічну тій, що отримують літературні твори [108]. У зв'язку із програмами варто вказати й на ч. 2 Статті 15 Закону 2022 р., в якій згадується об'єкт образотворчого мистецтва, створений за замовленням, як елемент КП комп'ютерної програми), належать його автору, якщо інше не встановлено договором або законом.

Є ще одна норма у новому законі, що стосується комп'ютерних програм, у якій йдеться про твір образотворчого мистецтва, спеціально створений як елемент комп'ютерної програми. Адвокат О. Мисенко роз'яснює, що мова йде про графічний користувацький інтерфейс. Він не вважається формою вираження комп'ютерної програми, а тому не захищається АП у якості КП. Тим не менш, даний інтерфейс може стати

об'єктом авторсько-правової охорони, якщо буде визнаний "результатом власної інтелектуальної творчої діяльності автора". Таким чином, майнові права на твір образотворчого мистецтва (яким є в даному прикладі малюнок на екрані комп'ютера), який особа сприймає внаслідок функціонування ЕОМ, що приводиться у дію створеною за замовленням КП, перейдуть на користь замовника, якщо інше не передбачено відповідним договором [53].

Важливо також відмітити, що раніше відтворенням вважалося тиражування, виготовлення копій, примірників творчого об'єкта в матеріальній формі й запис для зберігання в електронній, оптичній тощо формі. Нині ж, відповідно до п. 14 Статті 1 Закону 2022 р. ним вважатиметься також і "створення тривимірного твору з двовимірного і навпаки та створення тривимірного твору на основі набору інструкцій, який зчитується комп'ютером для виготовлення тривимірного твору" [66]. Зазначені зміни нормотворці аргументували тим, що такі дії не вважатимуться переробкою, бо не матимуть творчого характеру, але будуть вважатися використанням [63, с. 24-25].

Загалом, підсумовуючи аналіз Статті 1, зазначимо, що у попередньому Законі також не містилося визначень таких понять як законний користувач бази даних та комп'ютерної програми, мовлення, аудіодискрипція (тифлокоментування), копія та приватне копіювання, особа з обмеженими можливостями сприйняття друкованої інформації, піратський примірник твору, цитата тощо. Але в Новому Законі вони уже містяться; в ньому також були вдосконалені визначення вже наявних термінів як от комп'ютерна програма, твір та твір образотворчого мистецтва, компіляція даних, відтворення та публічне виконання й показ, розкриття публіці, розповсюдження й репродукування та інші.

Розглянемо й інші новели та важливі особливості норм Нового Закону про АП. Його Стаття 5 опікується питанням цивільно-правового захисту АП та суміжних прав, а також дає змогу отримати його правам особливого

роду (*sui generis*). Останнє, як зазначає О. Штефан, це результат імплементації Директиви 96/9/ЄС «Про правову охорону баз даних» (від 11.03.1996 р.), що надала відповідну правову охорону й захист виробнику неоригінальної бази даних. Так, у главі III, п саме в ч. 1 Статті 7 зазначеної Директиви вказано, що такий розробник, продемонструвавши вливання "якісно та/чи кількісно" значних інвестицій в "отримання, перевірку чи представлення вмісту бази", отримує право запобігати витягненню та/чи повторному використанню всього вмісту бази даних чи значної її частини у якісному чи кількісному вимірі». О. Штефан підкреслює, що вказане право виникає із завершенням створення бази даних та припиняється зі спливом 15 років з 01.01. року, який настає після дня такого завершення, а також має застосовуватися незалежно від того, чи підлягає розглянутий інтелектуально-правовий об'єкт захисту АП чи іншими правами. Як результат, п. 5 ч. 1 Статті 55 Закону 2022 р. зазначає серед суб'єктів, які вправі звертатися за захистом своїх АП та суміжних прав також і осіб з правом особливого роду *sui generis* [122, с. 65]. Окремо підкреслимо, за суттю зазначеної норми, що у разі, якщо компіляції даних надано охорону по *sui generis*, це ні в якому разі не спричиняє перешкоди здійсненню прав, що існують щодо наповнення даної бази.

Також звернемо увагу на Статтю 33, присвячену *sui generis* на неоригінальні об'єкти, згенеровані КП, за якою слід вважати неоригінальним об'єкт, який "відрізняється від існуючих подібних об'єктів та утворений у результаті функціонування комп'ютерної програми без безпосередньої участі фізичної особи в утворенні цього об'єкта". При цьому, якщо відповідний твір створили фізичні особи шляхом використання комп'ютерних технологій, то він не буде вважатися неоригінальним, згенерованим комп'ютерною програмою [66].

Зазвичай, коли йдеться про об'єкти, згенеровані комп'ютерною програмою, мають на увазі технології штучного інтелекту. Використання

штучного його як такого, що може створювати нові інтелектуальні продукти в процесі збору та пошуку даних та їх безпосереднього дослідження і компіляції, тим не менш, результують у формуванні неоригінального об'єкту, який можна використовувати для досліджень, розробки інфографіки тощо. Забігаючи наперед, відмітимо, що таке використання творчості комп'ютерних програм і подібних "творців" варто застосовувати, слідуючи таким настановам (щоб уберегти себе від подальших спорів):

- вказати інформацію про суб'єктів, які користуються *sui generis*;
- вказати джерело запозичення, в контексті використання у кібернетичному просторі - бажано зазначити гіперпосилання;
- використовувати об'єкт лише в тому обсязі, що обумовлений метою такого використання.

Нині все частіше з'являються позови, що стосуються саме використання ШІ у подібному контексті. Так, у справі *Andersen v. Stability AI Lt.* троє художників на чолі С. Андерсен позиваються проти компаній *Stability AI*, *Midjourney* і *DeviantArt*, що створили та впровадили артгенератори із застосуванням технологій штучного інтелекту. Митці вбачають порушення порушення своїх авторських прав у зв'язку із використанням робіт художників у генеративних системах ШІ. Натомість, відповідачі впевнені, що створені такими системами зображення, не схожі на роботи митців, а також посилаються на відсутність у позові проти них зазначення конкретних арт-об'єктів, які було використано в порушенні АП. Розгляд справи все ще триває [304].

Стаття 6, що містить перелік авторсько-правових об'єктів, тепер також включає й твори художнього дизайну (п. 12). Також категорія сценічних творів доповнилася музично-світловими шоу та цирковими виставами (п. 4 Статті 6), містобудування - ландшафтними утвореннями (п. 11), категорія ужиткового мистецтва - художньою ковкою (п. 10), збірників

- збірками обробок нематеріальної культурної спадщини (п. 14). Також з'явилася і така група об'єктів АП як "театральні постановки, сценічні переробки літературних творів белетристичного, публіцистичного, наукового, технічного або іншого характеру, і обробки нематеріальної культурної спадщини, придатні для сценічного показу" (п. 5 Статті 6)." Натомість із конкретного переліку об'єктів АП в новому Законі нормотворці прибрати сценічні обробки творів та фольклору, що є придатними для показу на сцені, які містилися у п. 13 Статті 8 Закону 1993 року [66, 67].

Стаття 7 до об'єктів охорони Закону 2022 р. відносить, крім іншого, й частини творінь, якщо такі можна використовувати самостійно. До них, зокрема, включають оригінальні назви творів та їх персонажів. Відмітно, що при їх використанні окремо від оригінальної роботи, такі частини є окремим твором [66].

Зміни торкнулися і норм відносно об'єктів, які не підлягають охороні авторським правом. Так, Стаття 10 Закону 1993 року до таких відносила "повідомлення про новини дня або поточні події" [67], натомість Стаття 8 Закону 2022 р. замінила дане формулювання на "повідомлення про новини або інші факти" [66]. Таким чином, поняття новин тепер охоплює не лише події, що сталися саме сьогодні (на поточний час), а й інші, що відбулися дещо раніше. Також є вказівка на ознаку факту у таких новин, тобто вони мають бути достовірним, "фактичними".

Щодо фольклору, то формулювання відносно нього тепер звучить як "вираження народної творчості" [66], а не "твори народної творчості", як було раніше. Щодо офіційних документів органів влади, то їх відповідні проекти тепер теж не є об'єктами АП [66]. Але в цьому контексті варто звернутися до Статті 91 Регламенту ВРУ (ЗУ № 1861-VI від 10.02.2010), згідно якої проекти законів та інших актів подаються на реєстрацію у комплекті із проектом постанови, переліком авторів, пояснювальною запискою та пропозицією по доповідачу на пленарне засідання [86]. Із цієї

норми слідує, що до реєстрації проект нормативного акту буде вважатися твором, у якого є автор, відповідно - і об'єктом АП. Але із моментом реєстрації над даним об'єктом починають працювати й інші особи-спеціалісти з відповідного напрямку роботи, вони вносять правки до колишнього твору, але до авторів віднесені бути не можуть.

Вище вже згадувалися неоригінальні роботи, які були згенеровані комп'ютерними програмами. У ч. 4 Статті 8 нового Закону вказано на надання їм охорони правом особливого роду. Фізична особа як автор не приймає участі у створенні таких об'єктів (вони генеруються КП), а отже немає і авторського творчого підходу, відповідно в процесі їх створення не виникають немайнові права [66].

Категорія державних символів та нагород, які не є авторсько-правовими об'єктами, доповнена знаками та емблемами "державної влади, Збройних Сил України та інших військових формувань України, затверджені органами державної влади". Також перелік об'єктів, не віднесених до відання авторського права, доповнено аббревіатурами й вищезгаданими неоригінальними фото [66].

У попередньому Законі містилася Стаття 12 щодо АП та права власності на матеріальний об'єкт, в якому втілено твір, які не залежали одне від одного та не передбачали відчуження обох при відчуженні одного з них. Також власник відповідного матеріального об'єкта, якщо в ньому було втілено творіння образотворчого мистецтва чи архітектури мав, перш ніж знищувати його, запропонувати творцю викупити його. або дозволити скопіювати у відповідній формі [67]. За Статтею 10 Закону 2022 р., яка розширює межі регулювання не тільки на матеріальні об'єкти, в яких втілені твори, але й на електронні (цифрові), в якому роботи були зафіксовані. Зазначена норма зберегла незалежність АП та права власності на такі об'єкти, як і незалежність відчуження їх. Тим не менш, пункт про знищення тепер стосується лише творів образотворчого мистецтва і не

забороняє власникові архітектурного об'єкту знищувати його без попередження творця. Також ч. 3 та 4 наділяють автора правом доступу до свого творіння задля його відтворення й забороняють власнику такого об'єкта відмовити творцеві у цьому [66].

Особливої уваги потребує питання особистих немайнових та майнових прав автора. Закон 2022 року доповнив перелік перших правом надати роботі назву або взагалі залишити її без такої, також у автора тепер є право присвятити твір певним особам, датам або подіям. Стаття 11, що містить відповідні положення, також зазначає серед так званих "моральних" прав автора вже відомі Закону 1993 р. право авторства, право на ім'я (псевдонім, залишатися анонімом) та на цілісність твору. Як і раніше, даний набір прав є невідчужуваним та не може бути переданий у спадщину [66]. Тарасенко Л.Л. пропонує доповнити список особистих немайнових прав автора тими, які містяться у законодавствах інших країн, зокрема правом на доопрацювання роботи, на її першу публікацію (оприлюднення), на збереження конфіденційності певних фотографічних творів та правом на заперечення проти знищення або видалення роботи [281, с. 173].

Також, щодо особистих немайнових прав, варто вказати на твердження К. Зерова про те, що у разі ускладненості відповідних правовідносин іноземним елементом, і при наявності бажання замовника застосувати до договору концепцію Work for Hire, дана умова буде нікчемною [35]. Зазначемо, що вказана концепція є офіційно закріплена в авторсько-правовому законодавстві США, і полягає в тому, що коли твір створено "за наймом", то його законним автором є роботодавець, а не творець-працівник [143].

Щодо майнових прав інтелектуальної власності на твір (так звучить назва відповідної Статті 12 Нового Закону, яка замінила собою відповідну Статтю 15 Закону 1993 р. із назвою "Майнові права автора"), то ними є стандартне право використовувати твір будь-яким способом та дозволяти

чи забороняти його використання іншими особами. Відповідний невичерпний перелік шляхів такого використання включає відтворення, переклад твору, його переробку та подібні модифікації, публічні виконання, сповіщення, покази, демонстрування, та інтерактивне надання доступу публіці, й доведення до загального відома публіки іншими способами, а також включення роботи до складеного чи іншого твору, імпортування, здавання в найм чи позичку та розповсюдження його примірників [66].

Не буде вважатися використанням авторсько-правового об'єкту розміщення гіперпосилань та фреймінг, якщо вказане вчиняється щодо твору, який було правомірно розміщено без обмеження доступу на веб-ресурсі, куди йде відповідне перенаправлення, таким чином, щоб люди могли отримати доступ до такого вмісту у час та з місця, обраних за їх бажанням. Якщо ж має місце легальне розміщення твору у цифровому просторі, але з обмеженнями доступу, а лінк (тобто посилання) чи фрейм дозволяє обійти відповідні обмеження доступу, то відповідні дії будуть вважатися використанням захищеного об'єкту шляхом інтерактивного надання доступу [281, с. 173], про який було зазначено вище. Тобто лінкування (розміщення гіперпосилань) та фреймінг щодо стороннього вмісту можуть бути абсолютно легальними, якщо відповідний матеріал був попередньо правомірно доступний і без посилання чи фреймінгу. А порушення матиме місце у випадку, коли, наприклад, автор фотографії обмежив загальний доступ до свого творіння (наприклад, такий доступ надається за певний кошт), але через лінкінг чи фреймінг ці обмеження можна обійти, тим самим порушивши авторські права.

Є у Законі 2022 р. вказівка й на майнове право на справедливую винагороду. Частина 3 Статтей 12, 38-40 пожиттєво наділяють авторів, виконавців та виробників відео- та фонограм правом на справедливую винагороду в незалежності від відчуження ними виключних майнових прав. Воно є невідчужуваним, переходить у спадщину та діє весь час, поки чинне

АП, також правочини і ліцензування щодо такого права є нікчемними, відповідно до Статті 48. В цьому контексті варто вказати на те, що майнові права на аудіовізуальний об'єкт переходять від автора до продюсера з того самого моменту, як твір створено. Але творець музичного твору, якщо такий було створено спеціально для аудіовізуальної роботи, залишає за собою майнові права на її публічне виконання та сповіщення окремо від аудіовізуального об'єкту. Договір про спільне виробництво фільму між продюсером й виробником такого твору не буде вважатися договором про спільну діяльність, а вихідні матеріали та копії роботи належать виробнику й іншим особам. При цьому суб'єктами права власності на вихідні матеріали й фільмокопії можуть стати як юридичні та фізичні особи, так і держава [66]. Таким чином, право на справедливу винагороду як невідчужуване - це спосіб, у який законодавці захищають творців від недобросовісних дій інших осіб, а також від умов договорів,, які могли б позбавити авторів такого права.

Взагалі, за Законом 1993 р. саме на Кабмін було покладено обов'язок затверджувати мінімальні ставки авторської винагороди [67], за Законом 2022 р. таке централізоване регулювання не передбачено. Останній НПА надає більшої ваги саме організаціям колективного управління (далі - ОКУ). Вказані суб'єкти формують тарифи на використання об'єктів АП, що є під їх управлінням, і діють вони на засадах самоорганізації і самоврядування [66].

Строк дії авторського права (як те було зазначено у Статті 28 попереднього закону) тепер замінено на "Строк чинності.." (Стаття 31 Закону 2022 р.), який складає (щодо майнових прав ІВ) 70 років, які обчислюються з 01.01 року, що слідує за роком смерті автора. Особисті немайнові права, як і раніше, охороняються безстроково [66].

Стаття 13 присвячена співавторству і передбачає, що майнові права на твір у співавторстві належать спільно всім таким співавторам і

здійснюються за погодженням між ними, якщо відповідна робота становить нерозривне ціле. У вказаному випадку також жоден із співавторів не може без достатніх підстав відмовляти іншим членам авторського колективу у наданні дозволу на опублікування чи переробку такого спільного об'єкту. Якщо ж мова йде про окремо створені авторами частини єдиного твору, то кожен автор здійснює майнові права щодо своєї частини твору відповідно до Статті 47 Закону 2022 р., тобто особисто, через представника, уповноважену особу або ОКУ. Відповідно, такі дії не повинні завдавати шкоди звичайному використанню авторсько-правового об'єкту чи безпідставно обмежувати законні інтереси суб'єктів АП. Щодо розподілу винагороди за використання створеної у співавторстві роботи, то він здійснюється у рівних частинах або у частинах, які співавтори погодять у відповідному договорі [66].

Зазначена Стаття 47 входить до Розділу IV Закону 2022 р., який присвячено здійсненню майнових прав і на об'єкти АП, і на об'єкти суміжних прав. Особливості правочинів щодо розпорядження майновими правами на відповідні об'єкти також врегульовані у вказаному Розділі, відповідно, передання майнових прав на об'єкти АП чи суміжних прав можливе:

- за договором - іншій особі у будь-якій державі повністю або частково на всі або окремі способи використання (Стаття 49);
- за ліцензійним договором - в цьому випадку ліцензіар надає ліцензіату дозвіл на використання відповідного об'єкту визначеним способом на певний строк, на певній території, за що ліцензіат буде оплачувати певну суму грошей (Стаття 50);
- за публічною ліцензією - шляхом оприлюднення умов такої ліцензії із наданням можливості дистанційного ознайомлення із творчим об'єктом необмеженому колу осіб з використанням інформаційно-телекомунікаційних систем. Така ліцензія може бути безвідкличною,

відповідно, діятиме протягом усього строку чинності майнових прав і буде достроково припинена тільки у разі порушення умов. Підкреселемо, що такі ліцензії є невиключними (Стаття 51);

- на користь ОКУ (Стаття 52) [66].

При цьому предметом договору про передання майнових прав не можуть стати об'єкти чи майнові права, яких не існувало на момент укладання відповідної угоди. Також, якщо в документі міститься умова щодо передання майнових прав на інший термін, ніж встановлено законом, або якщо умови погіршують становище автора чи його нащадків, або обмежують право творця на створення інших робіт, то відповідні умови будуть визнані нікчемними. Щодо ліцензування, то ліцензіат неправе використовувати відповідний об'єкт ІВ в сфері іншій, ніж передбаченій такою ліцензією [66]

Треба вказати на те, що автор чи виконавець вправі, відповідно до ч. 7 Статті 50 вимагати від іншої сторони договору виплатити йому додаткову пропорційну винагороду за використання твору (виконання), у разі, коли розмір винагороди за використання за укладеним між сторонами договором став непропорційно низьким [66]. Отже, якщо має місце безоплатний правочин, то зазначена винагорода буде автоматично непропорційною доходам іншої сторони, відповідно, автор (виконавець) отримає право вимагати від респондента оплати.

Щодо зазначеної Статті 51, окремо зазначимо про її застосовуваність у випадку з так званими “інтернет-мемами” (тобто зображення, відео чи подібний контент, зазвичай пародійного характеру). Так, на думку, медіа юриста М. Гринишака, такий твір за своїми характеристиками є карикатурним твором, і, відповідно, його використання регулюється законодавством, а тому без дозволу суб'єкта АП може використовуватися і безоплатно, якщо тільки було вказано ім'я автора, а також джерело

запозичення. Тим не менш творець мему може скористатись правом щодо надання публічної ліцензії на використання своєї роботи [65].

Також Закон 2022 р. оновив підходи до визначення дій, що порушують особисті немайнові та майнові права, зокрема Стаття 53 присвячена підставам для захисту АП та суміжних прав, якими є їх порушення, невизнання чи оспорювання і створення загрози відповідного порушення. Так, до порушень відносяться камкординг, плагіат, обхід технологічного захисту інтелектуальних об'єктів тощо. Серед іншого норма розкриває й суть зазначених загроз, якими слід вважати:

- ввезення в нашу державу та розповсюдження обладнання чи техпристроїв, що включає КП та надає доступ юзерам до об'єктів АП чи суміжних прав без відповідного дозволу;
- налаштування КП, застосунків та інших технологій, які надають зазначений доступ;
- надання інструкцій щодо налаштування таких КП й технологій без відповідного дозволу задля отримання комерційної вигоди за таке інструктування [66].

Статті 14 та 15 офіційно розділили авторські права на твори службові та створені за замовленням. Загалом же діє загальне правило, що майнові права на зазначені твори переходять до роботодавця (чи замовника відповідно), якщо договір чи законодавство не передбачає інакше. Також відмітно, що такі права на творіння образотворчого мистецтва, створеного на замовленням (якщо це не складова частина КП), належать його творцю [66].

Закон 2022 р. оновив та конкретизував випадки вільного використання об'єктів АП та суміжних прав. Так, Стаття 22 дозволяє відтворювати твір, якщо обсяг такого відповідає поставленій меті, в рамках демонстрування обладнання, його налаштування чи ремонту, якщо таке неможливо здійснити без відповідного використання, у вигляді макета,

креслення або плану капітальної споруди, будівлі задля її реконструкції, а також для забезпечення провадження (судового, адміністративного, чи кримінального), нормотворчої діяльності державних органів, вчинення нотаріальних дій, забезпечення суспільної безпеки. У вказаних випадках можна використовувати твір на безоплатній основі, без дозволу суб'єктів АП та зазначення авторства і джерел запозичення. Аналогічна норма діє і щодо публічного виконання музичних робіт в ході релігійних чи офіційних церемоній, що організували органи державної влади чи місцевого самоврядування. Без дозволу та на безоплатній основі, але з обов'язковою вказівкою авторства та джерела запозичення можна вільно:

- використовувати цитати та їх переклад з правомірно опублікованих робіт;
- відтворювати (і в електронній формі) та надавати (інтерактивно) доступу до правомірно опублікованих статей, уривків та невеликих за обсягом робіт, фото, аудіовізуальних та творів образотворчого мистецтва задля забезпечення й реалізації освітнього процесу чи проведення наукових досліджень, якщо таку активність здійснює суб'єкт освітньої чи наукової діяльності у місцях у призначених для цього місцях або через захищене цифрове середовище, доступ до якого мають тільки здобувачі освіти та освітяни. При цьому об'єм запозичення має відповідати поставленій меті, а сама діяльність не має самостійного економічного значення;
- відтворювати твори репрографічно з освітньою метою, якщо таке здійснюється суб'єктами освітньої діяльності, у відповідному меті обсязі та несистематично;
- відтворювати в електронному вигляді чи інтерактивно надавати доступ до статей, невеликих творів, уривків для цілей дистанційного навчання, але з обов'язковим вжиттям відповідних заходів для

недопущення отримання несанкціонованого доступу до такого контенту;

- відтворювати у каталогах охоронювані об'єкти якщо такі було виставлено на аукціонах, у колекціях, на виставках тощо задля інформування про відповідні заходи та без мети отримання комерційної вигоди;
- відтворювати, доводити до загального відома публічно виголошених промов, доповідей тощо у виправданому метою обсязі;
- відтворювати, доводити до загального відома та розповсюджувати у ЗМІ попередньо опублікованих статей, якщо такі дії не були попередньо прямо заборонені автором;
- відтворювати в Держреєстрі свідоцтв про реєстрацію АП на твір та Держреєстрі договорів, що стосуються права автора на твір;
- доводити до загального відома робіт з метою висвітлення подій та у відповідному інформаційній меті об'ємі;
- використання об'єктів як основи для створення попури, пародійних творів, карикатур;
- створювати зображення архітектурних чи творів образотворчого мистецтва, які знаходяться у доступних для громадськості місцях і використовувати їх в подальшому без самостійного економічного значення;
- робити аудіодискрипції (тифлокоментування) аудіовізуальних робіт;
- записувати роботу задля недовгого користування, якщо таке здійснює організація мовлення своїми засобами для своїх програм, але з подальшим знищення такого запису протягом тридцяти днів; вказаний строк можна збільшити за погодженням із відповідним суб'єктом АП.авторського права чи не встановлено законом. Такий запис може бути збережено в державних архівних установах у зв'язку з його виключно документальним характером;

- створювати копії об'єктів АП задля пошуку даних у наукових джерелах для дослідницьких цілей, якщо використання таких робіт прямо не заборонено суб'єктами АП, в тому числі шляхом зчитування комп'ютером з цифрового контенту, який розміщено у Всесвітній мережі [66].

В. Коноваленко вказує на катастрофічність скасування новим Законом можливості вільного використання літературних і художніх творів як ілюстрації у друкованих навчальних виданнях. Він посилається на відповідні норми п. 2 ч. 2 Статті 22 Закону 2022 р. Так, він зазначає, що нині передбачено тільки два варіанти використання об'єктів ІВ у якості ілюстрації у навчальних виданнях: відтворення та надання інтерактивного доступу. Але друковані навчальні видання прийнято розповсюджувати способом першого продажу чи іншого першого відчуження примірників відповідного об'єкта, який п. 2 ч. 2 Статті 22 Закону не передбачає. Справа в тому, що велика кількість видавців не володіє знаннями про зміни норм щодо вільного використання творів у виданнях навчального характеру, а тому й далі ілюструє підручники у спосіб, що є порушенням АП. Уникнути такого можна лише двома шляхами, на думку В. Коноваленка: використовуючи неохоронювані АП роботи, а саме фольклор та ті, що стали частиною суспільного надбання, та використовуючи твори, що АП охороняються, але із попереднім отриманням дозволу від автора або інших власників майнових прав на твір. Варіантом останнього є отримання ліцензії, укладення ліцензійного договору з такими особами. Також можна використовувати твори з вільною публічною ліцензією Creative Commons та об'єкти зі стокових веб-ресурсів, як от freepik.com та ua.depositphotos.com [43].

Статті 23-24 присвячені вільному використанню робіт в інтересах інвалідів та бібліотеками, музеями, архівами, організаціями із збереження фондів відео- та аудіозаписів. Щодо КП, то її законний користувач, за

Статтею 25, без дозволу і безоплатно може зробити резервну копію програми, декомпілювати та досліджувати її функціонування тощо; тобто копіювати програму можна з ціллю її збереження, а декомпілювати - з навчальною та дослідницькою ціллю [66].

Стаття 26 опікується вільним використанням баз даних, розширюючи межі такого використання, встановлені Статтею 22. Так, без дозволу та на безоплатній основі також можна вчиняти дії, що потрібні для забезпечення доступу до контенту відповідної бази з ціллю правомірного отримання такої копії законним юзером; відтворювати неелектронні БД в особистих цілях або для членів сім'ї та для ілюстрації в освітній й науковій діяльності, звісно без самостійного економічного значення та із зазначенням джерела запозичення, у відповідному меті обсязі і несистематично. Стаття також врегульовує питання вилучення баз даних [66].

Новий Закон додав і так зване тимчасове вільне відтворення творів, чим опікується Стаття 27. Відповідно до неї вказані дії можливі тільки задля правомірному використанню об'єкта охорони або сприяння переданню посередником його електронної (цифрової) копії у мережі між третіми особами. Якщо така мета дотримана, то відповідна активність дозволена без отримання дозволу суб'єктів АП та на безоплатній основі, а саме таке тимчасове відтворення має проміжний або випадковий (додатковий) характер та є обов'язковим як частина технологічного процесу [66].

Стаття 28 Закону 2022 року замінила та конкретизувала норми Статті 25 попереднього Закону, що присвячені вільному відтворенню робіт в своїх особистих цілях. Зокрема, тепер без дозволу та безкоштовно можна скопіювати твори за виключенням, крім іншого, баз даних (крім випадків за Статтею 26), творів образотворчого мистецтва (крім випадків за Статтею 24). Також можна зробити репрографічні копії об'єкта АП з виплатою справедливої винагороди відповідним суб'єктам, але суто в особистих цілях або для кола сім'ї [66].

Стаття 30 уніфікує норми щодо права слідування з тими, що діють в Євросоюзі з 2001 року. Кожного разу, коли має місце перепродаж об'єкту АП, автор вправі отримати відсоток від ціни (від 0,25% до 6% в залежності від вартості наступного продажу), але не більше як 12,5 тисяч євро. З точки зору даного дисертаційного дослідження важливим є те, що дана норма розповсюджується не тільки на спеціалізовані організації, які здійснюють професійну діяльність з торгівлі творами мистецтва, а й на приватних осіб, якщо вони продають відповідні об'єкти в Інтернеті [66].

Відповідно до раніше згаданої Статті 31 нового Закону, АП починає діяти з того моменту, як автор створив твір, у попередньому акті (Стаття 28) була вказівка саме на день створення роботи, до того ж у цьому документі зазначено, що таке право діє протягом строку життя творця і 70 років після його смерті, а у новому йдеться тільки про сплив чинності майнових інтелектуальних прав через ті ж 70 років. Якщо ж автор захотів залишитися анонімом чи видав твір під своїм псевдонімом, то по суті норма залишилась аналогічною - тут строк чинності майнових прав становить 70 років з оприлюднення роботи з урахуванням аналогічних правил обчислення, як і у випадку зі звичайним, оприлюдненим під ім'ям автора твором. Відповідно і якщо по псевдоніму особу автора можливо встановити, то діють правила аналогічні [66; 67].

Щодо співавторства та строку дії майнових прав в цьому випадку, то останній залишився незмінним - 70 років з дня смерті останнього зі співтворців (окрім положення про дію "протягом життя співавторів" та про правила обчислення, як і у випадку звичайного авторства), але цю норму було також додано положенням про строк дії ППВ на аудіовізуальні праці - також 70 років зі смерті останнього творця. Щодо неодночасного оприлюднення повного обсягу твору (у попередньому законі - "весь твір"), то окрім старої норми про строк чинності майнових прав ІВ (раніше - "строк дії АП"), що визначається окремо по кожній з частин, вказано, що цей

термін рахується з дати легального оприлюднення роботи. Щодо творів реабілітованих авторів, це положення було доповнене вже зазначеними правилами обчислення. Із нового Закону прибрана норма про АП на творіння, яке опубліковано вперше протягом 30 років зі смерті творця, але передбачено, що для твору, чий строк чинності прав рахується не від смерті авторів, така чинність припиняється, якщо відповідна робота не була законно оприлюднена в термін 70 років зі смерті творця. Також особа, що оприлюднить твір вперше і правомірно закінчення строку чинності майнових прав, користуватиметься охороною, аналогічною типовій охороні (стандартній), а сам такий строк складатиме 25 років для всіх творів, окрім творів науки та творів критичного характеру, де строк встановлено на рівні 30 років [66; 67].

Стаття 32 Закону 2022 р. замінила собою дві статті (29, 30) попереднього закону щодо питань спадкування та переходу творіння у суспільне надбання. Відповідно до вказаної норми, майнові права є складовою частиною спадщини, особисті немайнові - ні. В такому випадку спадкоємці спільно або спадкоємець (якщо він один) отримують відповідні права у повному обсязі, зокрема, і право отримувати винагороду за використання відповідного творіння. При спадкуванні за законом, нащадки однієї черги, за відсутності між ними відповідного договору, спадкують у рівних частках, а за заповітом - аналогічно, при відсутності у заповіті іншої волі заповідача. Спадкувальна норма доповнена положенням про те, що у спадкоємців є право на оприлюднення неоприлюдненого твору, якщо тільки автор не заборонив відповідні дії. Положення ч. 2 Ст. 29 попереднього закону про право нащадків на захист авторства та протидію перекручування роботи також присутнє у новому акті. Щодо суспільного надбання, то перехід до нього роботи відбувається із закінченням строку чинності майнових прав, раніше йшлося про "закінчення строку дії авторського права", при цьому така робота може використовуватися вільно,

без сплати винагороди (раніше було "без виплати авторської винагороди") [66; 67].

Стаття 55, присвячена цивільно-правовому захисту АП й суміжних прав, за яким, відповідно до її ч.1, вправі звернутися безпосередні суб'єкти таких прав, ті, кому належить вже згадані вище *sui generis*, акредитовані та ОКУ за дорученням правовласників-контрагентів з добровільного колективного управління, а також ті, хто володіють виключним право на використання відповідних або наділені правом отримання частки винагороди за їх використання. Ч. 2 даної Статті конкретизує, з яким вимогами вказані особи можуть звертатися до суду за захистом своїх інтелектуальних прав, а саме: визнати відповідні АП чи суміжні права, припинити й заборонити відповідні дії, що є порушенням вказаних прав, а також підготовчих до порушення дій (в т.ч. призупинити митні процедури, якщо є загроза ввезення примірників робіт із порушенням), поновити становище, що існувало до порушення, стягнути винагороду, за рахунок порушників опублікувати в ЗМІ інформацію про такі порушення та судові рішення з цього питання, відшкодувати моральну та матеріальну шкоду тощо [66].

На останніх вимогах треба наголосити особливо. Так, посилаючись на п.4 ч.3 розглянутої статті, відмітимо, що законотворці удосконалили інститут компенсації замість відшкодування збитків або стягнення доходу. Можемо говорити про поділ компенсаційних виплат за суб'єктивною ознакою на загальну і спеціальну. До першої слід віднести суб'єктів АП та суміжних прав, всіх інших, що зазначені вище - до суб'єктів спеціальної компенсації. Для першої групи осіб можливе (за їх вибором), замість відшкодування збитків або стягнення доходу, стягнення компенсації в об'ємі від 2 до 200 прожиткових мінімумів для працездатних осіб або фіксованої подвоєної суми винагороди, що мали б сплатити добросовісні отримувачі дозволу на використання спірної роботи, у випадку ж умисного

порушення така фіксована сума потроюється. Щодо випадків спеціальної компенсації, то тут передбачено лише можливість стягнення такої фіксованої подвоєної чи потроєної суми винагороди. Ця ж норма вимагає, щоб розмір компенсації був ефективним, співрозмірним і стримуючим", він також має бути націлений на відновлення порушених прав й використовуватися без "створення перешкод законній діяльності користувача і водночас забезпечити захист від зловживань користувача". При визначенні відповідного розміру суд має зважати на обсяг, тривалість та систематичність порушень, наміри та сферу господарювання порушників, їх вину та інші об'єктивні чинники [66].

Як наголошує з цього питання О. Мисенко, Новий Закон повернув оціночну компенсацію, залишивши одночасно і компенсацію штрафну. Тобто тепер компенсація альтернативна, але це стосується лише суб'єктів АП та суміжних прав. Він також підіймає важливе питання про те, яким же чином із виключною ліцензією, що не наділені правомочностями надавати іншим особам дозвіл на використання інтелектуального об'єкту, зможуть довести вірогідний розмір передбачуваної винагороди. Аналогічна дилема постала й перед тими, хто має право претендувати на частку винагороди за використання спірного твору, право на що також не обов'язкової наявності виключного права надання дозволу на використання. Відповідне доведення вбачається легкою справою лише для ОКУ, які вправі укладати відповідні договори із користувачами на умовах затверджених тарифів [52].

Спеціаліст також наголошує на неможливості застосування так званої штрафної компенсації, з урахуванням вимоги співрозмірності. Справа в тому, що така подвійна чи потрійна компенсація більша за передбачувану суму винагороди, яку опонент мав би сплатити. Це свідчить неспіврозмірність штрафних санкцій наслідкам порушення права у разі, якщо втрати постраждалого суб'єкту через порушення його прав дорівнюють передбачуваній сумі винагороди. Тому О. Мисенко радить

використовувати вимогу про співрозмірність тільки до оціночної компенсації. Так, вона разом із вимогою спрямованості компенсації на відновлення порушених прав означає, що судовий орган має встановити об'єм втрат позивача від порушення його прав, щоб чітко визначити розмір компенсації. Також слід розуміти, що за відсутності розміру втрат і самі підстави для стягнення оціночної компенсації будуть відсутні, бо "немає чому бути співрозмірною". Ще, обираючи оціночний вид компенсації, позивач має не тільки довести належність йому відповідних прав та факт протиправного використання належного йому спірного об'єкту, але й обґрунтувати співрозмірність суми оціночних компенсаційних виплат тим наслідкам, до яких призвело відповідне порушення. У випадку ж вибору штрафного виду позивач не буде обґрунтовувати вказане, але має довести розмір суми винагороди [52].

Вже зазначена раніше Стаття 56 нового Закону, що має особливе значення для даного дисертаційного дослідження, вдосконалила порядок припинення порушень АП та суміжних прав з використанням Всесвітньої мережі. Так, при вчиненні відповідного порушення з використанням Інтернету суб'єкт АП чи суміжних прав (у даному випадку він - заявник) вправі звертатися із заявою про припинення такого порушення до власника сайту і (або) власника веб-сторінки, на ресурсі яких і міститься спірний контент. Оригінал такої заяви надсилають власникові веб-сайту/веб-сторінки, а її копію постачальнику послуг хостингу (хостеру) для даного веб-ресурсу. До заяви висувуються наступні вимоги щодо наявного в ній змісту:

- дані про заявника, що його ідентифікують. Такими, для фізособи, є її ім'я (або найменування), місце проживання, перебування чи знаходження, поштова та e-mail адреса для направлення релятивної інформації направляти інформацію. у випадку із юрособою

знадобляться її дані про реєстрацію у країні місцезнаходження та реєстраційний номер;

- дані про спірний об'єкт - його вид, назва та інші ідентифікуючі його відомості;
- вмотивоване твердження щодо наявності у заявника майнових прав на відповідний об'єкт, а також посилання на підстави виникнення у нього таких прав. Останнє не вимагається у разі, коли вказана особа є первинним суб'єктом цих майнових прав;
- гіперпосилання на спірний цифровий вміст;
- вимога до власника ресурсу щодо вчинення дій для унеможливлення доступу до спірного контенту на сайті, і, за необхідності, вимогу до власника сайту і провайдера щодо недопущення ними розміщення такого вмісту в майбутньому;
- дані про хостера (його найменування; e-mail або поштова адреса для направлення релятивної інформації). При цьому зазначається, що постачальником хостингу буде вважатися власник сайту, який розміщує його на власних ресурсах чи (і) сам забезпечує доступ до нього через Інтернет, завдяки чому інші користувачі мають змогу розміщувати цифровий вміст на його ресурсі;
- твердження заявника про достовірність інформації в заяві і про те, що адвокат чи патентний повірений перевірили наявність й нього відповідних прав, які заявлено як порушені [66].

Слід звернути увагу на випадки, коли заявником виступає юридична особа. В такому разі вона може звертатися із вказаною заявою лише через представника - адвоката чи патентного повіреного, додавши до основного пакету документів копію посвідчення повноважень такого представника [66].

Власник веб-ресурсу може відмовити у задоволенні заяви, якщо та оформлена з порушенням вимог, або коли він наділений правом

використовувати спірний вміст, що підтверджується наданням відповідних документів про таке. У разі наявності основ для відмови, власник веб-ресурсу протягом 48 годин з моменту отримання заяви має повідомити заявника про відмову заявнику та хостера. У відповідному повідомленні зазначаються:

- дані про власника інтернет-ресурсу в об'ємі, що є достатнім для пред'явлення позову (його ім'я чи найменування, місце проживання чи місцезнаходження, поштова та адреса електронної пошти - для фізичних осіб; ідентифікаційні реєстраційні дані, реєстраційний номер - для юридичних осіб);
- спірний цифровий вміст, по якому відмовлено у обмеженні доступу;
- підстави для такої відмови [66].

Якщо ж адресат заяви не має підстав для відмови, то він зобов'язується не пізніше 48 годин з моменту отримання заяви унеможливити доступ до спірного цифрового контенту, а також надати заявнику і хостеру відомості про вжиті ним заходи. У випадку, якщо отримувач заяви - власник веб-сайту - не є власником сторінки, де міститься спірний вміст, то він має протягом 24 годин перенаправити копію заяви власнику відповідної веб-сторінки по електронній пошті або через систему повідомлень даного веб-ресурсу, а також надіслати заявникові повідомлення про відповідні дії і свій статус. Якщо ж за 48 годин з моменту направлення власнику веб-сторінки заяви той не направив власнику сайту повідомлення про відмову, то останній самостійно унеможлиблює доступ до спірних матеріалів, про що відповідно повідомляє заявника та хостера протягом 96 годин з моменту отримання заяви. Аналогічний термін в 4 доби є у власника сайту на те, щоб, у разі представлення власником сторінки відмови, надіслати копію такої відмови заявнику [66].

Заявник, за посередництвом адвоката чи представника у справах ІВ, може звернутися із зазначеною заявою, також напряму до хостера, якщо у зазначені строки власник сайту не вчинив (або не в повному обсязі) зазначені вище дії) або на самому сайті чи базі WHOIS не міститься відомостей про власника веб-сайту в обсязі, достатньому для звернення до нього із заявою (цими даними є e-mail адреса тощо). Така заява має містити відомості про заявника, гіперпосилання на спірні матеріали, вимогу до власника веб-сайту про унеможливлення доступу та твердження про достовірність інформації, а також додатково - документ про повноваження представника. Постачальник послуг хостингу, якщо немає підстав для відмови у задоволенні вимог заявника, не пізніше 24 годин з моменту отримання заяви надсилає її копію власникові сайту, а також пояснює адресату його права та обов'язки щодо цієї заяви і відповідні правові наслідки невчинення ним відповідних дій. Останній має добу (24 години) на вчинення цих дій, про що далі інформує хостера. Якщо ж відповідні дії не були вчинені у зазначений термін, хостер має самостійно унеможливити доступ до спірного цифрового контенту, про що потім, протягом 48 годин, повідомляє заявника та власника веб-ресурсу. Якщо ж неможливо встановити адресата заяви, заявник має право звернутися безпосередньо до Установи для сприяння у визначенні власника сайту чи хостера [66].

У хостера також є змога залишити без розгляду заяву, належним чином повідомивши про таке заявника протягом 24 годин, але зазначивши правові підстави для такого. Ними вважаються наступні:

- заява не відповідає вимогам;
- хостер не надає послуги чи ресурси щодо розміщення веб-ресурсу із спірним контентом;
- заявник не має відповідних підстав для звернення до хостера [66].

Якщо ж заявник, виконавши всі умови, не отримав відповідь від хостера, то він має право на звернення до Установи щодо питання про ініціювання притягнення до відповідальності відповідних власника сайту чи хостера, представивши для цього копії та підтвердні документи у свою пользу [66].

Таким чином, в порядку позасудової процедури припинення порушення АП, як зазначає Л.Л. Тарасенко, тепер можна вимагати припинення незаконного використання будь-яких об'єктів АП, а не тільки деяких, як було передбачено за Законом 1993 р. Нині хостери мають передбачити у договорі про надання хостинг-сервісу умови, що забороняють замовникам послуг публікувати електронний вміст з порушенням АП і наділяють їх обов'язком зазначати достовірні відомості про себе (і негайно інформувати про зміни в них). Щодо провайдерів послуг обміну контентом, то вони теж тепер відповідальні за порушення відповідних прав, але будуть звільнені від відповідальності при доведенні ними факту вжиття всіх можливих заходів для унеможливлення обміну спірним контентом і повторного його розміщення на сайті [281, с. 173]. Про такі вимоги щодо хостерів зазначено у Статті 57 Закону 2022 р. [66].

В контексті кіберпростору особливої уваги потребує і Стаття 58, що опікується питаннями відповідальності провайдерів послуг обміну контентом за порушення АП та суміжних прав. Дана норма в основі своїй містить положення Директиви Європейського Парламенту і Ради (ЄС) 2019/790 від 17 квітня 2019 року про авторське право і суміжні права на Єдиному цифровому ринку та про внесення змін до директив 96/9/ЄС та 2001/29/ЄС. Відповідні положення зачіпають провайдерів послуг обміну контентом (далі - ППОК). Вони мають нести відповідальність за порушення авторських, суміжних прав при відсутності у них дозволу на використання відповідних охоронюваних об'єктів "шляхом інтерактивного надання доступу та/або публічного сповіщення" відповідних творів. Тобто зазвичай

мова йде про нелегальне розміщення користувачького вмісту на веб-ресурсі без дозволу на те правовласників. Тим не менш, згідно ч. 3 зазначеної статті, ППОК не буде нести відповідальність, якщо доведе:

- факти вжиття ним всіх можливих заходів задля отримання такого дозволу;
- факти вжиття ним всіх можливих заходів задля унеможливлення обміну спірним контентом, попередньо отримавши заяву від правовласників про необхідність такого;
- факти вжиття ним заходів з метою припинення відповідних порушень у Всесвітній мережі та недопущення повторного завантаження спірного вмісту [66].

Варто звернути увагу на те, що законотворці не деталізують вміст поняття «всі можливі заходи» [66]. В тей же час Стаття 58 містить винятки, що стосуються стартапів та молодих компаній, що здійснюють діяльність менше 3 років, і чий обсяг річного доходу не перевищує 10 млн гривень, а місячна середня кількість унікальних відвідувачів його сайту менша за 5 млн осіб. Цим комерційним діячам треба тільки вжити всіх можливих заходів для отримання дозволу на використання відповідних матеріалів - контенту [66].

При цьому вказані вимоги не стосуються онлайн-енциклопедій, ринків електронної комерції, звичайних та хмарних сервісів B2B для особистого використання фізичними особами. Більше того, від компанії, яка жодного разу не отримала скарги щодо порушення АП по конкретним інтелектуально-правовим об'єктам, не вимагається робити моніторинг усього наявного цифрового вмісту, шукаючи порушення [55].

Новий Закон про авторське право передбачив й інші важливі новації. Отже, можна зробити висновок про те, що новий Закон про авторське право і суміжні права є проривом у царині АП. Тим не менш, не дивлячись на його

суттєві переваги у порівнянні з попереднім НПА, він має і наступні недоліки:

- відсутність визначення поняття «виключне право», яке в тексті НПА використовується, у поточній редакції Закону 1993 р. це визначення було наведене;
- використання терміну «суб'єкт майнових авторських прав» відбувається поруч із терміном «суб'єкт авторського права». Із формулювання ч. 2 Статті 5 прямо не випливає, що друге поняття включає в себе і перше, хоча Закон 1993 р. відносить суб'єктів майнових АП до суб'єктів АП;
- наявність юридичної колізії у питанні розподілу майнових прав на твір, створений за замовленням; вони, за відсутністю відповідних положень у договорі замовлення, перейти до замовника коли твір створено. За ч. 2 Статті 430 Цивільного кодексу, ці права належать обом сторонам договору спільно [116];
- приватне копіювання як спосіб використання твору, передбачає "відтворення в особистих цілях особи...чи близьких знайомих такої сім'ї". Але відповідного визначення таких "знайомих" немає, а, отже, ними може бути необмежена кількість осіб, відповідно, є ризик зловживань;
- перелік способів використання творів, за новим Законом, є вичерпним, хоча Закон 1993 р. передбачав те, що він не є вичерпним. Останнє вважається обґрунтованим, адже в контексті сучасних технологій, особливо застосування Всесвітньої мережі, практично неможливо передбачити всі можливі способи використання твору.

Отже, прийняття Закону 2022 р. стало відмітним кроком на шляху до вдосконалення законодавства у відповідній сфері з урахуванням реалій сьогодення та європейського вектору спрямування України. Даний НПА чимало уваги приділяє саме захисту АП у цифровому середовищі, де

сьогодні найчастіше здійснюються відповідні права, надаючи творцям не тільки відповідні права, але й механізми та інструменти для їх відповідного захисту в кіберсередовищі. Нині в Україні законом захищаються всі оригінальні творіння, що використовуються у цифровому середовищі, як от комп'ютерні програми, веб-сайти, та навіть меми тощо. Так, новий Закон про АП визначив порядок надання правової охорони об'єктам в рамках sui generis та особливості набуття, користування й захисту (зокрема, в позасудовому порядку) прав щодо об'єктів АП в Інтернеті. Водночас, даний акт став об'єктом критики та дискусій, які законотворцям ще знадобиться вирішити у майбутньому, адже їх вирішення важливе для підтримки правового порядку у кібернетичному середовищі, де контент створюється і поширюється досить легко.

5.2. Ефективність правового забезпечення дотримання права інтелектуальної власності у кіберпросторі в Україні і світі: шляхи впровадження найкращих світових практик

Захист прав інтелектуальної власності в кіберсередовищі є дуже важливим для всіх країн, адже нині світ живе в високорозвинену цифрову еру, де створення й розповсюдження цифрової ІВ є невід'ємною частиною повсякденного життя більшості людей. Сьогодні інформація передається без особливих зусиль, а кордони стають дедалі прозорішими, і тому захищати свій цифровий контент від посягань стає дедалі складніше. Захист відповідних прав досить часто ускладнюється через несанкціоноване копіювання та легкість отримання спільного доступу до цифрового контенту, простоту його тиражування та розповсюдження. На руку порушникам грає й те, що у різних державах - різний підхід до регулювання відповідних питань: різняться законодавчий масив, механізми захисту таких прав та притягнення до відповідальності за їх порушення.

В результаті страждають як окремі люди-творці, так і юридичні особи, що володіють майновими правами інтелектуальної власності на твори у цифровому середовищі. Також стрімкий розвиток інформаційних технологій не дає змогу нормотворцям вчасно реагувати на нові інцеденти та потенційні ризики. Саме тому в даному розділі дисертаційного дослідження будуть розглянуті найбільш дієві практики країн щодо захисту інтелектуальної власності в цифрову еру у кіберпросторі.

Але для початку варто згадати, які саме перешкоди постають на шляху здійснення відповідного захисту:

- світ змінюється, велика частина життя людей тепер має місце саме в кібернетичному середовищі, де, відповідно, постійно з'являються нові типи ІВ, а законотворці не встигають за трендами цифрових трансформацій;
- доступність відтворення об'єктів ІВ та легкість їх розповсюдження через цифрові мережі значно посилює відповідні проблеми типу онлайн-піратства;
- відсутність або недостатність напрацьованих та дієвих заходів кібербезпеки, що має місце, зокрема, через зростаючу частоту та складність кіберзагроз;
- нерегульованість захисту даних і конфіденційності, чому сприяє, зокрема, великі обсяги оброблюваних даних;
- розвиток технології блокчейну із її децентралізованою архітектурою змінює способи управління правами ІВ;
- поява смарт-контрактів, що базуються на попередній технології і може забезпечити прозорість угод, тим не менш, є недостатньо врегульованою.
- відсутність уніфікованого правового регулювання, що є важливим з точки зору транскордонного захисту ПІВ тощо.

Даний перелік не є вичерпним, а тому важливо розробляти та впроваджувати в дію відповідні механізми та засоби, які б допомогли подолати вказані проблеми. Далі варто розглянути конкретні приклади окремих країн, що вважаються нам за позитивні.

Так, наприклад, захист інтелектуальної власності в епоху цифрових технологій у В'єтнамі, як зазначає юрист Ф. Зітер, є частиною бізнес-стратегії в умовах процвітаючої цифрової економіки його країни та заснований на наступних положеннях:

- **стійке розуміння суті та впливу цифрової ери.** Ця ера змінила кардинально спосіб створення, споживання інтелектуальної власності та її розповсюдження, а тому традиційні методи захисту часто не відповідають вимогам кіберсередовища. Це, в свою чергу, має своїм наслідком розквіт онлайн піратства та недозволеного використання відповідних об'єктів;
- **визнання важливості такого захисту.** ІВ - це актив, який не тільки є каталізатором творчої активності, але й конкурентоспроможності та інноваційної діяльності відповідних суб'єктів. Відповідно захист останніх, зокрема, в цифровому середовищі - це засіб для залучення інвестицій та економічного зростання суб'єктів, і в'єтнамські компанії це чудово розуміють;
- **активне залучення фахівців з права.** Професіонали своєї справи, вони допоможуть у розробці дієвих стратегій, наприклад, проактивного моніторингу, подальшого втілення механізму сповіщення про видалення тощо, а також у застосуванні судових засобів захисту. Також в'єтнамські організації активно взаємодіють в цьому питанні із місцевими правоохоронними органами;
- **здійснення безпосереднього захисту ІВ.** Щодо АП, то у захист відповідним суб'єктам надається автоматично після створення твору, тим не менш, реєстрація АП у Національному відомстві авторських

прав В'єтнаму відіграє важливу роль, адже таким чином створюється юридичний запис. Патентний захист у даній країні здійснюється через Національне відомство інтелектуальної власності шляхом попередньої подачі патентної заявки. Захист ТМ відбувається також через вказаний орган шляхом відповідної реєстрації. Захистити комерційну таємницю можна шляхом застосування проактивного підходу, зокрема, заходів конфіденційності, NDA й протоколів обмеженого доступу [316].

Представниця Індії, Н. Сансаре, радить застосовувати наступні стратегії для захисту інтелектуальної власності в цифровому світі:

- **реєстрація авторського права на твір.** В багатьох країнах така реєстрація не вимагається як основа для виникнення авторських прав, але вона є бажаною, бо надає додаткові юридичні переваги у разі порушення (зокрема, з досвіду України - доведення авторства у разі виникнення спору буде здійснюватися на основі свідoctва про реєстрацію відповідних прав);
- **використання засобів міжнародного захисту інтелектуальної власності.** Фахівчиня радить звернутися до Бернської конвенції 1886 р. та Паризької конвенції 1883 р. Також можна додати в цей перелік процедуру реєстрації торгових марок за Мадридською системою, що базується на застосуванні Мадридської угоди про міжнародну реєстрацію знаків та Протоколу до неї тощо;
- **управління цифровими правами** (англ. - *Digital Rights Management, DRM*). Такі технології допомагають контролювати розповсюдження та використання цифрових матеріалів, обмежуючи неавторизоване копіювання, спільний доступ або модифікацію цифрових активів. Але застосування DRM може мати й негативні наслідки, зокрема, у вигляді обмеження свободи користувачів;

- **умови використання** (*англ. Terms of Use*) і ліцензійні угоди. Такі Угоди та Умови мають бути чіткими та максимально зрозумілими для звичайної людини, щоб кожен міг легко зрозуміти, в яких формах можна взаємодіяти з наявними матеріалами, за яких умов, зокрема, чи можна, і в якому об'ємі копіювати контент, розповсюджувати, модифікувати його;
- **"водяні знаки" (або т.зв. ватермарки) та шифрування.** Так, застосовуючи першу методику, власник контенту додасть до нього відмітний (або навіть непомітний) знак. Щодо другої методики, то вона захистить інформацію, зробивши її непридатною для читання кожному, хто не має відповідного ключа розшифровки;
- **моніторинг і забезпечення виконання.** Правовласникам бажано періодично перевіряти цифровий простір на предмет будь-яких несанкціонованих дій із належним їм контентом, для чого можна використовувати спеціальні інструменти та послуги служб для ідентифікації наявних порушень. Якщо ж таке порушення було виявлено, то треба застосовувати всі наявні можливості досудового вирішення відповідних спорів, інакше - звертатися з позовом в суд;
- **підвищення обізнаності про важливість дотримання ПІВ.** Необхідно формувати серед користувачів кіберпростору культуру поваги до цифрової інтелектуальної власності [269].

Щодо викликів в сфері інтелектуальної власності та цифрової економіки Сінгапуру, то Європейська комісія (далі - ЄК) як вищий орган виконавчої влади ЄС, радить європейським підприємствам знати не тільки про основні проблеми галузі, але й застосовувати різноманітні наявні інструменти для ефективного управління своєю ІВ, що сприятиме їх економічному розвитку в названій країні. Зокрема, мова про:

- надання пріоритету онлайн-досвіду. ІТ-інтеграція відмітно змінює способи підходу до клієнтів під час ведення бізнесу, а тому, задля

уникнення проблем, треба застосовувати стратегії ліцензування та синтезу захисту відповідних об'єктів ІВ, бо відповідні права оскільки права ІВ будуть уразливими в невідомому середовищі;

- впровадження заходів кібербезпеки, а також всебічне регулювання взаємодії із даними задля їх захисту на онлайн-платформах. Останні стали звичним середовищем для розвитку цифрової економіки. ЄК наголошує на ризиках зазнати порушення ПІВ і можливості бути притягнутим до відповідальності за те, що певним чином надали змогу порушникам через вашу платформу порушувати права інших;
- адаптація до нових реалій у зв'язку із використанням технології штучного інтелекту. Щодо володіння ПІВ на об'єкти, створені ШІ, сінгапурське законодавство вимагає залучення до створення відповідних робіт хоча б однієї живої людини (автора), тоді і створений твір буде користуватися захистом ПІВ. Також використання вказаних технологій пов'язане з великим ризиком втрати компанією бізнес-інформації і порушенню прав інших осіб через використання ШІ великого масиву даних. Представникам бізнесу радять постійно працювати над підвищенням рівня захисту інтелектуальної власності, відстежувати нові потенційні загрози, протидіяти проблемам, що виникають при транскордонному правозастосуванні. Задля реалізації Сінгапурської національної стратегії штучного інтелекту Офіс інтелектуальної власності Сінгапуру опублікував Записку (англ. IP and Artificial Intelligence Information Note), в якій йдеться про ключові питання ІВ і доступні форми захисту відповідних прав в контексті ШІ;
- застосування практичних рішень, запропонованих урядом країни. Офісом інтелектуальної власності Сінгапуру було опубліковано Сінгапурську стратегію інтелектуальної власності 2030 (англ. Singapore IP Strategy 2030, SIPS), що націлена на підтримку

комерційної діяльності, орієнтованої на взаємодію із ІВ та використання штучного інтелекту;

- використання «Програм прискорення». Серед таких названо PCT-Patent Prosecution Highway, ASEAN Patent Examination Cooperation, SG IP Fast Track, які допоможуть прискорити процедуру патентного захисту та зробити її дешевшою. Результати патентної експертизи, отримані за допомогою таких програм можна використовувати як довідкові матеріали в процесі експертизи;
- реєстрація торгових марок через мобільний застосунок IPOS MOBILE GO. Це перша в світі мобільна платформа, через яку можна подати заявку на відповідну реєстрацію напряму і досить швидко (процедура триває близько 10 хвилин). Також в цій програмі можна подати заявку на продовження своїх прав промислової власності й здійснити пошук по вже наявним об'єктам [177].

Американські юристи, що працюють із фондовими ринками, задля захисту своїх ПІВ радять наступне:

- використовувати авторське право, бо це єдиний тип захисту ІВ, який можна набути автоматично в момент компіляції чи написання вихідного коду ПЗ. Також варто зареєструвати своє творіння у Бюро авторських прав США чи в іншому бюро авторських прав в тій державі, де об'єкт буде використовуватися. При цьому слід пам'ятати, що сама заявка на реєстрацію може бути подана онлайн - і досить швидко, але її розгляд триватиме близько 4 місяців. Захист в рамках АП можна застосовувати до всього коду програми, при цьому деякі його частини можна зазначити як комерційну таємницю, зробивши інші частини доступними в бібліотеках з відкритим кодом;
- щоб захистити комерційну таємницю, варто використовувати Угоди про нерозголошення та конфіденційність при розробці ПЗ, задля збереження бізнес-логіки проєктів, при цьому юристи наголошують,

що захист комерційної таємниці є безстроковим та значно дешевшим, ніж отримання відповідного патенту;

- слідувати не тільки місцевому законодавству, але й загальноприйнятим юридичним практикам, зокрема, Європейського Союзу щодо захисту ІВ (наприклад, Директиві 2009/24/ЕС щодо правового захисту комп'ютерних програм) [136].

Окрема увага далі буде приділена європейським країнам та ефективності правового забезпечення дотримання права інтелектуальної власності у кіберпросторі в них, із зазначенням шляхів впровадження найкращих світових практик у даній сфері.

Так, щодо Великобританії, що здійснила Брексіт, та уже не є членом ЄС, Б. Хітченс та інші вказують на зв'язок між захистом ІВ та сталим розвитком економічного зростання країни, а також безпосередньо Цілями сталого розвитку ООН (серед яких, зокрема, зазначаються промисловість, інновації та інфраструктура). Саме тому технологічні інновації, що спрямовані на забезпечення стійкості відповідних факторів (умовно названих «зеленими» технологіями), мають ключове значення для досягнення цілей вказаної організації. Щодо АП, то важливим є наявність у творів відповідної стійкості (в контексті сталого розвитку). Діджитал-технологічність життя вимагає, щоб більшість технологій керувалася саме комп'ютерами. Відповідно, АП може захищати ПЗ та алгоритми, що здатні аналізувати й сприяти розробці більш стійких промислових процесів [198, с. 387].

Таким чином, ПЗ, захищене авторським правом, можна комерціалізувати в рамках моделі ліцензування, що, відповідно, принесе дохід своїм авторам, тим самим стимулюючи людей до розробки нових або покращення вже наявних технологічних інноваційних продуктів. АП також допоможе боротьбі із несправедливим використанням своїх прав правовласниками для запобігання конкуренції й залучення інвестицій у

подібних або тотожних сферах. Нинішній набір інструментів прав інтелектуальної власності у Сполученому Королівстві є якісним й достатнім для забезпечення захисту технологій у цифровій сфері, а сьогоденні тенденції тяготіють до активного залучення технологій штучного інтелекту та великих даних. Зокрема, щодо ІІІ, зараз впроваджуються два сценарії:

1. творіння та розробки у відповідній сфері користуються «звичайним» захистом (патентування, захист комерційних таємниць, АП),
2. система штучного інтелекту сама створює об'єкти, що підпадають під відповідний захист. І тут уже виходять із трьох підходів:
 - a. АП захищає творіння, яке створено навіть без втручання людини, або
 - b. вимагається хоча б мінімальна участь людини у створенні об'єкта (наприклад, фізична особа натискає кнопку для запуску операції), або
 - c. АП не розповсюджується на твори, що були створені без участі людини [198, с. 393-394].

У зв'язку із вищезазначеним, звернемося до британського Закону про АП (англ. *Copyright, Designs and Patents Act 1988*), відповідно до п. 9 (3) Ч. 1 якого, автором твору літератури, музики тощо, якщо він створений за допомогою комп'ютера, буде особа, що вжила заходів, необхідних для його створення [151]. При цьому у справі *C-5/08 Infopaq International A/S v Danske Dagbaldes Forening* суд постановив, що АП поширюється тільки на твори, у яких є оригінальність, що, в свою чергу, є проявом власного інтелектуального творіння автора [198, с. 394].

Щодо країн ЄС, то Європейська рада з інновацій разом з Виконавчим агентством з питань малого та середнього бізнесу, звертає особливу увагу на так зване "цифрове мистецтво" (англ. *digital art*). Воно залежить від технологій як невіддільної частини творчого процесу та створюється авторами із використанням ПЗ та цифрових пристроїв (це, наприклад,

пiксельне мистецтво, цифровий живопис тощо). Також до уваги взято криптомистецтво (англ. *crypto art*), яке використовує технологiю блокчейн у питаннях власності та аутентифікації. Також цифрове мистецтво iснує виключно в цифровій сфері, а криптографічне - завдяки невзаємозамінним токенам (англ. *non-fungible tokens, NFT*), i воно не підлягає відтворенню без оригінального файлу. У випадку з цифровим мистецтвом, по строку захисту, воно діє 70 років після смерті творця (або останнього з співавторів). Майнові права забезпечують контроль над відповідним об'єктом, який можна продати, використовувати по ліцензії та розповсюджувати на онлайн-платформах, а особисті права автора дають йому змогу називатися творцем та протидіяти будь-яким перетворенням [178]. Останнє особливо важливе у зв'язку з легкістю модифікації твору у цифровому середовищі.

Для захисту своїх робіт, авторам радять:

- офіційно зазначити своє авторство, зокрема, шляхом зазначення із використанням символу копірайту;
- зареєструвати АП через національне відомство інтелектуальної власності, що стане у нагоді при доведенні презумпції авторства, власності та дати створення спірного об'єкту. Так, Бюро патентів і торгових марок Іспанії веде офіційний реєстр авторських прав. Механізми *i-Depot* під керівництвом Офісу ІВ Бенілюксу та *e-Soleau* (Франція) надають послуги із встановлення дати створення роботи. При цьому слід зважати на те, що на сьогодні не існує єдиної європейської реєстрації АП. ;
- укладати ліцензійні угоди, в яких чітко визначені положення та умови використання творів чи скористатися послугами спеціалізованих онлайн-платформ для розповсюдження та ліцензування цифрового контенту;

- зауважити на захищеність авторським правом ПЗ та його назви, графічного інтерфейсу тощо, тобто того, що є необхідними для втілення творчості людини у цифровій формі. Слід також пам'ятати, що сам код може бути захищений незалежно від об'єкта АП, який створюється з його використанням. Але алгоритми, мови програмування та функції ПЗ в розумінні законотворців - це ідеї, а тому вони не охороняються АП, але підпадають під охоплення конфіденційністю;
- використовувати DRM - керування цифровими правами, що використовує шифрування та контроль доступу задля недопущення піратства чи несанкціонованого розповсюдження твору;
- проставляти на своїх творах цифрові водяні знаки, які діють як підписи на об'єктах цифрового мистецтва. Такі вотермарки не можуть бути легко видалені неавторизованою особою без згоди правовласника.
- використовувати шифрування, і твір буде недоступним для розшифровки без відповідного ключа;
- застосування технології блокчейн (що особливо важливе у сенсі криптомистецтва), із внесенням інформації про права власності та транзакції щодо робіт в децентралізовану та незмінну книгу із призначенням унікального цифрового маркера кожному матеріалу [178].

Не можна оминати увагою і такого світового гегемона як Китай. Вчені наголошують на особливій бінарній природі «приватних прав» та «прав людини» щодо ПІВ. У першому випадку йдеться про інтелектуальну власність як форму «влади» для нематеріальної власності, відповідно, власник отримує «владу» над власністю щодо приватних правна ТМ, АП, ім'я, патенти тощо. Щодо прав людини, то мається на увазі право

суспільства на участь у вигодах від творчо-інтелектуальної діяльності [288, с. 791-792]. Тобто має бути баланс між обома типами прав.

Країна постійно веде діяльність у галузі удосконалення системи інтелектуальної власності та посилення її захисту. І це стосується не лише законотворців. Так, права інтелектуальної власності інноваційних суб'єктів в Китаї визнається нематеріальним активом, тому місцеві банки почали фінансувати застави інтелектуальної власності, забезпечивши тим самим фінансову підтримку інноваційним підприємствам. Щодо нормативно-правового масиву, то у 2019 році був прийнятий Закон про товарні знаки КНР, який періодично переглядається. Зокрема, врегульовано питання заходів для обмеження зловмисних реєстрацій ТМ із одночасним заохоченням реальних інновацій. Компаніям надано змогу інвестувати в дослідження та розробки, що дало поштовх для ведення більш активної творчо-інноваційної діяльності. Труднощі виникають щодо підтримки вже зазначеного балансу між інтересами власників ІВ та загальних інтересів суспільства. Тому було впроваджено особливий механізм балансування вигод, в рамках якого забезпечується основа для розподілу прибутку в технологічній інноваційній діяльності. Тим не менш, проблема захисту інтелектуальної власності в Китаї та способи реагування на неї все ще є наріжним каменем і веде до певних обмежень, зокрема, недостатня врегульованість окремих питань, низька ефективність судової системи, слабе правозастосування [311, с. 111-112].

Тому для посилення захисту ІВ в країні вчені та практики радять наступне:

- подолання недоліків побудови системи ІВ. Для цього варто скоріше розробити більш конкретні норми задля недопущення різнорідного трактування положень та уникнення неоднозначності у їх практичному застосуванні та розумінні. Для цього можна застосовувати уніфіковані стандарти захисту ПІВ;

- налагодження співпраці між різними відомствами. Це сприятиме формуванню інтегрованої правоохоронної мережі для безперервного захисту ІВ;
- підвищення ефективності судочинства. Наразі термін розгляду справ категорії ПІВ є довшим за відповідний розгляд звичайних цивільних справ, до того ж сама судова процедура є складнішою, відповідно, ускладнюється і отримання належного правового захисту правовласниками. Тому китайському уряду бажано прискорити судову реформу, в рамках чого створити спеціалізовані окружні суди або судові групи для розгляду справ щодо питань ІВ. Також варто постійно проводити підвищення кваліфікації суддів та прокурорів у відповідній сфері;
- посилення нагляду та контролю за правоохоронними органами з боку уряду. Хоча місцеве законодавство є всеосяжними, але воно не виконується належним чином на рівні правозастосування. Подолання такої перешкоди допоможе забезпечити ефективне впровадження захисту ІВ на практиці;
- продовження всебічного вдосконалення системи захисту ІВ. Не тільки реформування нормативно-правового інструментарію, але й роз'яснювальна діяльність щодо прав та обов'язків в контексті ПІВ, а також посилення санкцій за відповідні порушення сприятиме досягненню поставленої мети;
- посилення міжнародного співробітництва. Це сприятиме обміну практичним досвідом, а також колективній боротьбі з транснаціональними порушеннями ІВ [311, с. 112].

Щодо захисту баз даних в Китаї, то тут здебільшого використовується стаття 14 місцевого Закону про АП, Закон про товарні знаки, Закон про недобросовісну конкуренцію, Закон про патенти. Так, у справі щодо нематеріальної культурної спадщини *Hainan Jingtian Company v. Shanghai*

Хіхі, відповідач скопіював та поширив через сайт створену позивачем «велику базу даних нормативних документів і запитів». Суд спочатку сумнівався у питанні надання охорони даних базі даних, але зрештою відмітив її оригінальність у відповідність іншим умовам захисту АП. Але він наголосив на тому, що даний об'єкт являє собою структуроване вираження інформації для запитів та аналізу, що наділене функціями зручності та практичності у користуванні. Суд постановив, що захист АП в даному випадку застосовується до структури, а не до вмісту бази даних, тобто має місце так званий «м'який захист». А, отже, самі дані нематеріальної культурної спадщини не можуть бути захищені авторським правом [288, с. 794-795]. Таким чином, у КНР простежується позитивний рух щодо поступового підвищення рівня захисту інтелектуальної власності, вбачається суттєва підтримка інноваційно-економічному розвитку, але все ще відчувається необхідність у перебудові та покращенні системи захисту, із реформуванням судової системи та посиленням правозастосування.

Щодо Японії, яка також серед лідерів ІТ-індустрії світу, то місцевий Відділ авторських прав (англ. *Japan Copyright Office, JCO*) активно проводить політики щодо АП, як от розробка й удосконалення законодавства та систем оформлення прав в галузі діджиталізації. Також ведеться нагляд за колективними товариствами й впроваджуються освітні заходи для експертів і широкої громадськості. Також в країні діє Агентство з питань культури (англ. *Agency for Cultural Affairs, ACA*) як орган в складі Міністерства освіти. Будучи членом Інтернет-договорів ВОІВ, Бернської та Римської конвенцій, Пекінського договору про аудіовізуальні виконання, Всесвітньої конвенції про АП та Угоди TRIPS тощо, держава прийняла та неодноразово переглядала закон про авторське право. Питання, що стосуються захисту немайнових прав та тривалості часу захисту віднесені до відання національного права країни витребовування захисту. Так, наприклад, дії користувача із об'єктом АП, якщо вони суперечать намірам

автора, вважатимуться протиправними, навіть якщо зміна твору іншою особою є вигідною для автора. Тобто в японському законодавстві упор зроблено саме на нематеріальні ("моральні") права автора. Загалом же АП країни тяжіє до континентально-європейської концепції у цьому відношенні, але з поєднанням норм права США. Японський Закон про авторське право нині, у відповідь на стрімкий розвиток цифрового та мережевого суспільства, зазнав деяких поправок, в тому числі, з метою зобов'язання міноритарних зацікавлених сторін вживати всіх необхідних засобів для захисту своїх законні інтересів [306, с. 28-30].

Цікавим з точки зору кібернетичного середовища та ПІВ є положення ст. 10 Закону про авторське право Японії про "твори комп'ютерного програмування" (саме в такій термінології). Так, вони, відповідно до п. їх ч. 1, є твором у розумінні вказаного НПА, але у ч. 3 даної статті зазначено, що охорона "не поширюється на мову програмування, кодування або алгоритми, які використовуються для створення твору" [148]. Таке уточнення було б дуже вдалим, якщо його інкорпорувати в українське законодавство, тим самим роз'яснивши правовласникам межі захисту.

Також, відповідно до ч. 2 Статті 15 вказаного НПА, автором твору комп'ютерного програмування, якщо він був створений працівником корпорації і за її ініціативою під час виконання службових обов'язків, якщо інше не передбачено договором, трудовими правилами тощо [148]. Саме автором вважається компанія, що не корелює із загальнопоширеним розумінням автора як фізичної особи.

Як уже зазначалося японський автор наділений нематеріальним право щодо збереження цілісності роботи та її назви, а тому її модифікації, якщо вони суперечать намірам автора, заборонені. Але дане положення не буде застосовано, відповідно до п. ііі ч. 2 Статті 20, якщо подібні модифікації КП потрібні для її виконання на конкретному комп'ютері або для її більш ефективного використання на комп'ютері. Стаття 76-2(1) Автор КП може

zareєстровати дату створення такого об'єкта (і тоді робота вважається створеною у дату реєстрації); але із сплином 6 місяців від дати створення, таке положення не застосовується. Згідно Статті 119 (v), особа, що надала для громадськості доступ або саму КП, яка сприяє використанню твору, що порушує АП, понесе відповідальність у вигляді позбавлення волі на строк до 5 років, й (або) штрафу в розмірі до 5 мільйонів ієн [148].

Цікавим є те, що згідно з місцевим прецедентним правом до кінематографічних творів належать комп'ютерні ігри (тобто КП), і за Законом про АП строк їх охорони складає 70 років. Щодо використання ШІ, то попередньо підготовлені моделі та навчальні набори даних можуть отримати захист в рамках АП, якщо в їх створенні була використана творчість і не вважаються створеними ШІ, натомість є власним інтелектуальним твором людини-творця [306, с. 30-32].

Проблеми захисту ПІВ в Японії особливо часто виникають саме у цифровій сфері, адже відповідні об'єкти потребують дещо іншого захисту аніж традиційні твори. В даній країні захисти відповідних прав здійснюється в судовому порядку в незалежному (паралельному) режимі. І в цьому контексті слід зауважити на важливості поділу порушень ПІВ на пряме і непряме.

Як зазначає на прикладі винаходів Й. Фолкнер, дана концепція поділу схожа із підходом США, відповідно, якщо має місце конкретний акт порушення, що зачіпає всі елементи заявленого винаходу, то мова йде про пряме порушення. Якщо ж порушення зазнають не всі елементи об'єкта, але має місце така поведінка порушника, що спонукатиме або сприятиме їх порушенню іншою особою, то це - непряме порушення [33].

Відповідно, якщо відбувається явне (пряме) порушення, то розпочинається основний судовий розгляд. Його супроводжує попереднє судове провадження. У разі ухвали рішення про наявність порушення, має бути подано позов про сплату застави - і тільки тоді буде розпочато

основний судовий процес. Щодо непрямих порушень, то в державі прийнято, що воно тягне за собою лише відшкодування збитків, й не надає правовласникам право на судовий захист. І відповідно до місцевого законодавства судові заборони на непряме порушення не дозволяються. Така практика б не мала особливо негативних наслідків, якщо б ІТ не посприяло можливості миттєво створювати копії творів [180, с. 34].

Щодо прямих та непрямих порушень, варто також згадати про так звану Доктрину Караоке. Початком її формування слід вважати справу караоке-закладу Club Cat's Eye, по якій у 1988 році було винесено рішення Верховного суду Японії. Власника закладу було визнано порушником АП, бо він використовував музику без сплати ліцензійних зборів. Здавалося б, що порушниками є самі співаки, але за визначенням суду, саме власник клубу безпосередньо вчиняв правопорушні дії, керуючи і контролюючи караоке-активності з метою отримання прибутку. Підкреслимо, що справа стосувалася не самого акту програвання записаних на програвач композицій, адже будь-яка людина могла повторити виконання захищеного твору. Але відвідувачі співали без мети отримання прибутку за виконання, натомість власник пропонував клієнтам заспівати, надавав відповідні караоке-касети й інше обладнання для цього. Відповідно, відвідувачі співали під контролем та адмініструванням власника, а сам заклад «створив свою атмосферу частково на основі співу клієнтів» і намагався отримати прибуток шляхом задоволення такою атмосферою людей. Суд, як наслідок, постановив, що спів клієнтів, з точки зору законодавства про АП, є таким же як "спів власника бару". Зрештою, таке одіозне рішення породило Доктрину Караоке, що нині застосовується, зокрема, у справах щодо обміну з використанням однорангової технології (P2P) та служб обміну відео (TV Break Case) [305, с. 4-5], відповідно у сфері використання цифрового простору.

Сьогодні дана доктрина дозволяє надавати судові заборони щодо деяких види непрямих порушень АП, тим не менш все частіше виникають несправедливі ситуації, коли відтворення є законним, але спонукання або допомога в ньому вважатимуться незаконними. Також японська судова система іноді відмовляється від юрисдикції на основі «доктрини особливих обставин» у разі, коли оголошення юрисдикції суперечить принципам справедливості між сторонами. Це дає певну гнучкість судам, бо вони можуть відмовитися від юрисдикції, застосовуючи певні підстави юрисдикції до кожної справи окремо. Тим не менш, таке нерідко призводить до правової невизначеності. А тому слід намагатися уникнути загального положення, яке встановлює «доктрину особливих обставин» задля встановлення балансу між ефективним забезпеченням ПІВ та правами відповідача [231, с. 74].

Таким чином, в Японії вживають наступних заходів у галузі захисту ПІВ:

- ведення нагляду за колективним управлінням АП (на основі Закону про бізнес-управління авторським правом та суміжними правами 2001 р. - англ. Law on Management Business of Copyright and Related Rights);
- використання набору правил для збору плати за використання виконань. Розвиток цифрових технологій значно полегшивши взаємодію із творами, а тому і різноманітність варіантів їх використання значно зросла;
- застосування жорсткого тлумачення діючого законодавства значно обмежило коло дій користувачів у пункті їх законності, навіть коли шкода автору не завдається;
- застосування принципу презумпції мовчазної згоди та вичерпання прав, розширення тлумачення окремих положень щодо обмежень задля "пом'якшення" такого жорсткого тлумачення;

- активна розробка засобів протидії порушенням ПІВ у кіберпросторі з використанням ІІІ (на основі законодавства про захист прав на товарні знаки й недобросовісної конкуренції). Зокрема, виходять із визнання правовласником тієї організації, яка створила алгоритм ІІІ;
- обговорення нових правил регулювання спорів між коспеєрами (людина, одягнена як певний персонаж твору) та власниками інтернет-адреси, за якою матеріали за участю коспеєрів розміщуються. Нині виходять із того, що якщо коспеєр не заробляє на цьому прибутку, то він не є порушником. Але у разі продажу або поширення через Інтернет матеріалів з відповідно вдягненим коспеєром порушення АП має місце;
- визнання незаконним опублікування в Мережі (зокрема, на YouTube) скорочених версій кінотворів із супровідним текстом з описом сюжету відео-матеріалу;
- врегулювання питання інтелектуального аналізу тексту та даних (англ. *Text and data mining, TDM*). Мова про метод комп'ютерного аналізу тексту та даних, що застосовує у своїй діяльності великий об'єм даних і тексту, які створені і є доступними у цифровому середовищі. Наразі в країні дозволено використовувати твір будь-яким способом і в будь-якому обсязі, якщо користувач не має на меті особисто "насолоджуватися думками чи почуттями, висловленими в цьому творі" та його дії не завдають необґрунтованої шкоди інтересам правовласника. Але метою таких дії має бути, альтернативно, використання для тестування при розробці технології для запису звуку чи зображення твору тощо; використання в аналізі даних; використання з метою обробки комп'ютерних даних. При цьому TDM може вчинятися навіть з метою отримання прибутку [306, с. 35-39].

І наостанок слід дослідити захист прав ІВ і, зокрема, АП, в Польщі, куди наші співвітчизники найчастіше прямують, обираючи країну для переїзду. Так, як відзначає М. Лукан, місцева система є менш формалізованою, рівень захисту АП в цій країні подібний до інших правових систем і, по суті, аналогічний рівню в країнах Євросоюзу. Так, дана центрально-європейська республіка імплементувала всі директиви ЄС в галузі АП та є учасницею ТРІПС, ДАП, Бернської конвенції, Женевської та Парижської конвенцій про АП. Місцевий закон про АП (*пол. Ustawa o prawie autorskim i prawach pokrewnych*) 1994 р. у Статті 1 проголошує принцип автоматичного захисту, охороняючи, відповідно, творчі здобутки з моменту їх створення безвідносно до виконання будь-яких формальностей.

В країні не ведеться офіційний авторсько-правовий реєстр, а реєстрація відповідних прав не передбачена через офіційний владний орган (хоча й є можливою через спеціалізовані недержавні установи, тоді відповідний документ буде оцінений судом як звичайний доказ). У Статті 8 зазначеного акту проголошується і принцип презумпції авторства, тобто творцем є людина, чиє ім'я зазначено на примірнику відповідної роботи допоки інше не буде доведено [235, с. 68-69].

Тим не менш, така ситуація іноді призводить до спростування авторства через суд, і, задля недопущення вказаного, місцеві юристи радять вчинити наступних кроків:

1. зарезервувати своє АП нотаріально;
2. надіслати рекомендованим листом примірник твору на адресу правовласника (із отриманням повідомлення про вручення);
3. працюючи над творінням, фотографувати та фільмувати весь творчий процес із зазначенням дати зйомки;
4. при розгляді спору в суді залучати свідків, яким твір та його автор знайомий;

5. зареєструвати свої права у Бюро авторських прав Сполучених Штатів [232].

Також бажано скористатися послугами вже згаданих установ для фіксації свого авторства та дати створення роботи. Для цього можна звернутися в The Copyright Index (визнана в усьому світі як орган, що забезпечує офіційну реєстрацію АП) онлайн та отримати відповідний офіційний сертифікат. Тривалий час послуги з колективного управління АП в країні надає і платформа ZAiKS, приймаючи заявки і особисто і через цифрові засоби, а також OKU SAiW COPYRIGHT POLSKA [235, с. 69].

Таким чином, Україні є чому повчитися у інших країн, адже ефективність правового забезпечення дотримання права інтелектуальної власності у кіберпросторі, в більшості випадків, є доведеною. Підсумовуючи їх досвід, можна радити українським правовласникам наступні шляхи впровадження найкращих світових практик:

- зробити захист інтелектуальної власності частиною бізнес-стратегії компанії, що включатиме, зокрема, стійке розуміння суті та впливу цифрової ери, визнання важливості захисту інтелектуальних цифрових активів, активне залучення фахівців з права, зокрема, для розробки дієвих стратегій та взаємодії із місцевими правоохоронними органами, здійснення безпосереднього захисту ІВ як це прийнято у В'єтнамі;
- завжди реєструвати свої АП, навіть з урахуванням того, що ця процедура не є обов'язковою для отримання відповідного захисту, як радять представники Індії та Євросоюзу;
- використовувати цифрові платформи для реєстрації своїх АП шляхом подання онлайн-заявки. Зокрема, в зв'язку із повномасштабним вторгненням РФ в нашу державу, УКРНОІВІ, що функціонує як нацорган ІВ - НОІВ, з 2022 року приймає електронні заявки на відповідну реєстрацію;

- компаніям слід розробити стратегії для захисту своїх ПІВ в контексті кіберсередовища. Зокрема, бажано укласти угоди про конфіденційність та неконкуренцію із своїми працівникам і, тим паче, незалежними підрядниками, як радять американські та європейські правознавці, а також використовувати системи відстеження активів задля недопущення витоку важливої інформації;
- впроваджувати та використовувати системи керування цифровими правами та (або) укласти із користувачами ліцензійні угоди та Terms of Use, що допоможе контролювати в якому обсязі та яким чином останні отримують доступ до контенту, як практикують в Індії, Сінгапуру, ЄС;
- для комп'ютерних програм та подібних активів слід використовувати не лише захист в рамках АП, але й патентування, а також, за можливості захист комерційної таємниці щодо конфіденційних даних та, наприклад, процесів, як це практикується в США та деяких країнах Європи;
- застосовувати технології відстеження активів, що характерно для Індії та Європи, зокрема, шляхом використання технології блокчейн та ШІ тощо для нагляду за використанням відповідних активів та IP-адрес правовласників. Також ШІ допоможе аналізувати значні обсяги даних, завдяки чому можна буде виявляти потенційні випадки порушення. При цьому, розробляючи та впроваджуючи технології штучного інтелекту, слід залучати до їх створення живих людей, як це прийнято в Сінгапурі;
- використовувати платформи безпечного обміну при обміні користувачами конфіденційними даними, як це втілено в сінгапурській практиці;
- відстежувати використання своїх ТМ та пов'язаних із ними доменних імен, також обов'язково проходити відповідну процедуру реєстрації

торгових марок за (бажано) Мадридською системою, як радять індійські та інші юристи;

- для своїх творів використовувати ватермарки та шифрування для захисту відповідного контенту і даних, як це радять представники Індії, Європи та інших країн;
- проводити тренінги та майстер-класи для співробітників з навчанням їх передовим практикам по поводженню з цифровими активами та їх захистом.

Щодо участі держави у відповідних ініціативах з покращення правового забезпечення дотримання прав ІВ у кіберпросторі, то, з огляду на практику проаналізованих країн, мають бути вчинені наступні заходи:

- розробити та впровадити стратегію інтелектуальної власності строком на найближчі 10 років, як це реалізовано в Сінгапурі, задля надання підтримки бізнесу і стимулювання творчо-інноваційної діяльності;
- використовувати при розробці правових інструментів та механізмів загальноприйнятні юридичні практики, зокрема, європейські;
- усіляко сприяти поширенню розуміння необхідності реєструвати свої АП, а також, відповідно, втілювати практики для полегшення даної процедури, наприклад, за моделлю США та європейських країн;
- аналогічні дії вчинити і щодо реєстрації торгових марок, зокрема, впровадити можливість робити це через спеціалізовані мобільні застосунки (за приклад може бути взятий сінгапурський IPOS MOBILE GO);
- розробити та впровадити "програми прискорення" (за сінгапурським моделлю), що допоможуть пришвидшити та здешевити патентування відповідних активів;
- для запобігання зловживанням у сфері використання ІІІ імплементувати британський, японський та сінгапурський досвід,

зокрема у частині вимоги про хоча б мінімальну участь людини у створенні активу;

- детально врегулювати на законодавчому рівні питання захисту об'єктів "цифрового мистецтва" та криптомистецтва (за основу бажано взяти досвід ЄС);
- при розробці законодавства у галузі ПІВ застосовувати уніфіковані стандарти захисту з метою недопущення різноманітного трактування положень та уникнення неоднозначності у їх практичному застосуванні;
- впровадити механізм балансування вигод при розподілі прибутку в технологічній інноваційній діяльності (як це робить Китай);
- спростити судові процедури при розгляді відповідних спорів та нарешті де-факто почати роботу Вищого суду з питань інтелектуальної власності (ІР-суду);
- активно співпрацювати при розробці правових норм із технологічними експертами для кращої відповідності таких норм технічним реаліям у галузі використання ІВ в цифровому середовищі;
- налагоджувати та усіляко сприяти співпраці між різними відомствами задля недопущення інцидентів у сфері порушення ПІВ у цифровому домені, а також, як це зробив Китай, посилювати контроль за правоохоронними органами;
- розвивати міжнародне співробітництво задля обміну практичним досвідом й спільній протидії транснаціональним порушенням.

Отже, вирішення проблем у сфері ПІВ, зокрема, у кіберпросторі вимагає багатогранного підходу, що передбачає правові, технологічні й соціальні рішення і взаємодію. Наявні практики зарубіжних країн можуть стати у нагоді при розробці відповідних стратегій та інструментів в Україні. Важливо також забезпечити дотримання ПІВ в різних юрисдикціях, що

наразі є великою проблемою з огляду на глобальний характер цифрового середовища.

5.3. Концептуальні засади побудови ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі

Як було зазначено в минулих розділах даного дисертаційного дослідження, цифрова революція, зокрема в контексті переведення основних видів діяльності в кіберпростір, має своїм результатом значні наслідки для прав інтелектуальної власності. Так, нині створено нові великі можливості для творчості та інноваційної активності, але разом з тим постійно виникають відчутні перешкоди й труднощі, які вимагають особливого правового регулювання, зокрема, досить гнучкого, яке б урахувало і реалії сьогодення, і стійку необхідність у забезпеченні надійного захисту відповідним об'єктам та їх правовласникам. Тому законотворцям настійно рекомендовано співпрацювати як із юридичними експертами, так і представниками комерційних кіл, а також кіл академічних, бо доктрина, хоч і не є джерелом права безпосередньо в нашій країні, але може стати міцним підґрунтям у цьому питанні для розвитку нормативно-правового інструментарію, що б відповідав викликам мінливого кіберсередовища.

Як відомо, уже багато років Росія веде проти України, зокрема, і інформаційну війну, використовуючи обширні важелі інформаційної зброї, вчиняючи акти кібертероризму, наслідки чого, за своєю суттю, можна порівняти з наслідками використання зброї масового знищення. Адже незаконне злонамісні дії з інформацією - її збирання з інших джерел чи створення, подальше зберігання, використання, розповсюдження тощо - можуть призвести не тільки до фінансових втрат, але й до репутаційних та навіть до втрат здоров'я та життя людей. Дійсно, кіберзлочини як

транснаціональна проблема може зашкодити усім трьом основним суб'єктом інформаційних відносин - людині, суспільству та державі загалом. І це в рівній мірі стосується й питання прав інтелектуальної власності у кіберпросторі, адже відповідні об'єкти досить часто є носіями інформації не лише творчого характеру, але й передових інновацій, зокрема, тих, що можуть бути використані у військовій сфері (а це нині є особливо актуальним для України). Як приклад, креслення і загалом розробки дронів - це одночасно і результат творчо-інноваційної активності людини (людей), і засіб якщо не перелому ходу війни, то, хоча б, впливу на нього.

Таким чином, взаємозв'язок між інтелектуальною власністю та кіберсередовищем нині є явним та нерозривним. Кіберпростір — це нефізичний світ, він усіляко сприяє безперервному перебігу торгівлі, дає змогу нам, живим людям, спілкуватися та обмінюватися даними, зокрема тими, що являють собою об'єкти інтелектуальної власності. Але таки стан речей сприяє і збільшенню кількості кібератак, коли інформація може бути скомпроментована та використана у інший, ніж визначений правовласником, способом, а це, відповідно, створює додатковий тиск на інтелектуальну власність та потребує вироблення нових концепцій для її надійного захисту.

Для детального вивчення концептуальних засад побудови ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі важливо володіти понятійними категоріями, і, зокрема, розуміти, що є концептуальними засадами. Так, під ними, О. Дніпров має на увазі основоположне розуміння певного феномену, "сукупність поглядів на певний процес, діяльність, явище" [20, с. 37]. Завдяки логіці дослідника, як множинне упорядковане утворення, дане поняття набуває ознак систематизації. Саме вказаний суб'єкт відбирає серед різноорідних наукових положень та засад необхідні, і робить це "цілеспрямовано, аналітично і конструктивно" [14, с. 167].

Таким чином, *концептуальні засади побудови ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі можна визначити як основоположне розуміння відповідної побудови ефективного правового забезпечення, сукупність поглядів на неї вчених та практиків, а також нормотворців, що втілюють відповідні ідеї та концепції у нормативно-правове регулювання щодо права інтелектуальної власності у кіберпросторі.* Отже, для виконання поставленого завдання, необхідно дослідити наявні погляди та підходи щодо побудови ефективного правового забезпечення дотримання ПІВ у кібернетичному просторі, і конструктивно їх систематизувати.

На думку більшості вчених, саме авторсько-правове регулювання є сьогодні основоположним у питанні побудови ефективного правового забезпечення дотримання ПІВ у кіберпросторі. Але, за Р. Фатіма, ефективність законів про авторське право з точки зору незаконного копіювання викликає великі сумніви через швидкий розвиток та прогрес у технологіях копіювання, а також невисоку вартість тиражування творів і легкість їх оцифрування. Зазвичай, у випадку вказаного порушення, використовуються цивільні, кримінальні та адміністративні засоби правового захисту [179, с. 1165-1167].

Але їх недостатньо, бо транснаціональність ІТ сприяє ускладненню відстеження порушень авторських прав у кіберпросторі. Також негативними факторами є відсутність єдиного нормотворчого органу, який би "домінував над Інтернетом", політичних зобов'язань, достатніх всеосяжних нормативних механізмів. Сприяє погіршенню ситуації і погане виконання наявного законодавства у відповідній сфері. І ці проблеми мають бути вирішені якнайшвидше, зважаючи на швидкі темпи технологічних змін. Світова спільнота має співпрацювати задля пошуку регуляторних формул для вирішення вказаних проблем, що залишаються в кіберпросторі, адже відповідні інтелектуально-правові об'єкти не захищені

загальноприйнятими стандартами як звичайні (тобто нецифрові) твори [179, с. 1168-1169].

Г. І. Зекос також вказує на нездатність законодавства про авторське право забезпечити належний захист, що видно із конвергенції технологій та появи нових форм вираження мистецтва у формі додатків. На його думку АП стало "законом про втрачені можливості" [315, с. 330-331].

Аналізуючи Закон про захист авторських прав у цифрову епоху, вчений вказує на наявність процедури самопомоги для власників АП для контролю над своєю ІВ. В цьому контексті він наголошує на неефективності DRM та подібних технологічних заходів захисту. Як засіб зменшення споживання піратського цифрового контенту пропонується практика закриття (виключання) веб-сайтів-порушників АП, бо, відповідно, зменшується кількість випадків нелегального використання творів. Складність захисту АП у кіберпросторі ускладнюється ще і тим, що порушники, зазвичай, знаходяться за межами однієї країни і, відповідно, законодавство з цього питання може різнитися, як от коли законодавство країни постачальника послуг не вважає певний контент правопорушним [315, с. 337-338].

Дійсно, зауважена проблема транскордонності цифрового середовища також потребує вирішення в контексті побудови ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі. На цьому наголошує і К. Сарангі. Так, децентралізована структура Мережі у поєднанні із простотою транскордонного зв'язку породжують велику проблему у питанні визначення юрисдикції в кіберпросторі, адже незрозуміло, хто має повноваження щодо певного кібер-інциденту. Суперечність НПА у різних державах поглиблює дану проблему, адже кожна юрисдикція буде відстоювати свою владу над діяльністю в цифровому середовищі. Задля подолання виникаючих невизначеності та двозначності вбачається за необхідне створити

загально визнану систему юрисдикції в кібернетичному просторі шляхом активної міжнародної співпраці, гармонізації законів та інноваційних підходів. Тільки так можна буде ефективно боротися з кіберправопорушеннями, зокрема, у галузі ІВ, забезпечувати ефективне управління цифровим доменом та дійсно захищати права та інтереси фізичних і юридичних осіб. Як приклади правових інструментів для подолання проблеми екстериторіального охоплення та втамування потреби в гармонізації між юрисдикціями наводяться Каліфорнійський закон про конфіденційність споживачів (англ. *California Consumer Privacy Act, CCPA*) та Загальний регламент про захист даних (англ. *General Data Protection Regulation, GDPR*) [270]. Вважаємо, що GDPR та CCPA мають бути використані при формуванні національного законодавства в контексті кіберпросторової юрисдикції, адже вони підкреслюють важливість чіткої правової регламентації, підзвітності та захисту прав особи на конфіденційність у кіберсередовищі.

"Цифровою проблемою" Г. Мохан охрестив те, що відбувається у сфері АП через активне використання Інтернету та цифрових технологій. Можливість створювати необмежену кількість копій твору, а після - швидко розповсюджувати їх по всьому робить кожного користувача потенційним "мережевим видавцем", бо цифровий всесвіт не обмежений географічними рамками, а редагування матеріалів є відносно простим. І відповідні правопорушні дії можуть взагалі не залишати слідів оригіналу твору. Розвиток численних способів спілкування та обміну вмістом через Інтернет, таких як торренти, однорангові системи обміну файлами тощо, полегшив порушникам поширення піратського вмісту та фактично позбавив прав власників авторських прав в Інтернеті. Серед причин, які сприяють порушенню авторських прав у кіберпросторі, вчений зазначає, окрім вказаного, також можливість працювати анонімно, користувачами нерідко є люди, що не знають основ авторського права, негативно впливає ів

відсутність національних органів, що могли б ефективно керувати захистом відповідних прав у кібердоміні. Він також, як і більшість науковців вказує на проблему юрисдикції у випадку кіберпорушень. Складність ідентифікації злочинця серед величезної кількості Інтернет-юзерів теж негативно впливає на ефективну розбудову якісного правового забезпечення дотримання відповідних прав [239, с.67-68].

На думку дослідника, вирішенню означеної проблеми сприятиме:

- детальна вказівка в законодавстві на підсудність справ з цифрового порушення ПІВ, вчиненого представниками іншої країни, судам своєї держави;
- законодавче врегулювання визнання тимчасових копій, зроблених гаджетом користувача, відтворенням, а також визнання надання онлайн-доступу до матеріалів «повідомленням громадськості» [239, с.70];
- подолання технологічної необізнаності, зокрема, серед правоохоронних органів, які можуть якісно розслідувати офлайн-порушення, але не володіють відповідними знаннями та навичками щодо порушень цифрових. Також навіть при наявності технічно кваліфікованих агентів, слідчі органи нерідко використовуються у розслідуванні значних комп'ютерних злочинів типу кібер-атак, хакерства, залишаючи кіберправовпорушення щодо ІВ поза увагою [239, с.95];
- розробка і подальше законодавче впровадження положень щодо нового розширеного режиму обміну файлами і посилення відповідальності онлайн-посередників, адже наразі Інтернет надає майже відкритий доступ до контенту, можливість легкого його розповсюдження з практично нульовими витратами;

- зобов'язання інтернет-провайдерів (під загрозою значних штрафних санкцій) контролювати та фільтрувати сайти-порушники, щоб не стати співучасниками у порушенні АП;
- надання правового захисту технологічним методам охорони прав авторів та правовласників, введення в дію жорстких положень щодо відповідальності за обхід технологічних заходів. При включенні відповідних норм до національного законодавства слід орієнтуватися на вимоги Інтернет-договорів ВОІВ [239, с.96-99];
- забезпечення наявності та виконання правових заходів для зберігання даних і записів про використання Мережі шляхом введення журналів і реєстрів для її використання, що мають робити постачальники інтернет-послуг протягом розумного строку задля надання допомоги у відстеженні IP-адрес порушників;
- надання чіткішого тлумачення дій, які не є порушенням, мова про випадки, коли «несанкціоноване відтворення твору» трансформується у законне вільне використання творів;
- впровадження системи оповіщення про авторські права та моніторингу із можливістю дисциплінарного стягнення щодо Інтернет-передплатників для однорангового обміну файлами;
- створення та просування технологічно грамотних програм відстеження IP для виявлення спуфінгу тощо;
- визначити на законодавчому рівні поняття кіберсквотингу та шляхи покарання порушників і методи відшкодування шкоди;
- на міжнародному рівні (для досягнення глобальної правової одноманітності):
 - розробка універсального кіберзакону для захисту ПІВ в цифровому середовищі та врегулювання питання юрисдикції;
 - розробка типового закону для захисту цифрової ІВ для сприяння окремим країнам у співпраці з міжнародними

організаціями на кшталт ICANN, який визначить, зокрема, покарання, юрисдикцію тощо.

- заохочення правовласників до використання DRM;
- впровадження програм громадської освіти серед інтернет-користувачів із їх інформуванням про можливі правопорушні дії та засоби самостійного захисту від відповідних порушень ПІВ в кіберпросторі [239, с.100-103].

В контексті самостійного відстеження правопорушень в мережі, що стосуються інтелектуальної власності, вчені уже більше десятиліття наполягають на використанні засобів, що надає корпорація Google, а саме - "Повідомлення про контент у Google" [209, с. 22]. Дана послуга створена на вимогу і виконання ДМСА.

Розглянемо, як же працює дана послуга відповідно до правил корпорації [62]. Отже:

1. перш за все варто скористатися сайтом <http://www.copyscape.com/> (або іншим сервісом, що знаходить в Мережі аналогічний контент як на сайті запитувача) і, якщо порушення було виявлено, треба перейти за посиланням
<https://support.google.com/legal/troubleshooter/1114905?hl=uk>, це
сторінка "Повідомлення про контент у Google";
2. далі серед запропонованих варіантів слід обрати сервіс, на якому розміщено спірний контент, що і став причиною скарги (це можуть бути веб-сайти із пошукової видачі Google, блоги, Youtube тощо). Якщо таких сервісів ("продуктів") декілька - для кожного треба надіслати окрему скаргу;
3. форма, коли скаржник вказує на сайт-порушник, обов'язково запитає: "Чи стосується цей запит контенту, який штучний інтелект створив у продукті Google?" (це відносно нове питання, яке з'явилося у відповідь на реалії сьогодення, пов'язані із генерацією контенту ШІ;

4. наступним кроком є вказівка на причину скарги (пропонується 2 варіанти відповіді: юридичні причини та порушення правил корпорації щодо матеріалів і продуктів, зокрема в контексті спаму чи фішингу). І якщо обрано перший варіант, то сервіс розумітиме це як наявність порушення про конфіденційність чи інтелектуальну власність певної країни чи регіону;
5. серед подальших юридичних причин можна зазначити як ІВ, так і наявність виданої ухвала суду або інші (на кшталт, наявності в контексті ворожих висловлювань тощо);
6. при обранні варіанту ІВ, скаржнику треба буде додатково вказати, що ця скарга стосується АП (зокрема, незаконне використання твору), або зустрічного сповіщення (у разі потреби відновити матеріали, попередньо видалені через таку скаргу), або обходу технологічних засобів захисту АП, або підробки (рекламування чи реалізації контрафакту);
7. далі заявник скарги щодо АП має надати детальний опис спірного вмісту, зазначити URL-адреси сторінки із правочомно розміщеними творами та сторінки-порушника.
8. останнім кроком є натискання відповідної клавіші “Створити запит”.

При цьому сервіс попередить скаржника про можливість притягнення його до відповідальності за завдані збитки (судові витрати тощо) за необґрунтовані скарги на порушення АП. Також вимагається, щоб скарга надсилалася або правовласником, або його уповноваженим представником.

У разі правомочності скарги, Google застосує процедури видалення спірних матеріалів або обмеження доступу до них відповідно до місцевого нормативно-правового регулювання. Щодо останнього варіанту, то юзера попереджають про можливість різниці у правових нормах різних країн (тобто, не обов'язково контент, який порушує норми законодавства однієї держави, вважається порушним в іншій). В такому випадку, пошукова

система видалить спірний контент або обмежить доступ до нього лише в тому регіоні, де він не є законним. Аналогічні дії, але щодо всього світу, будуть вчинені щодо матеріалів, які порушують загальні контентні правила Google чи Умови використання його сервісів.

Коли скарга прийнята, Google надішле відповідне повідомлення передбачуваному порушникові або власникові веб-ресурсу із неправомірно розміщеними матеріалами. Після цього повідомлення про порушення документується й, іноді, відправляється спеціальної організації Chilling Effects, що публікує такі скарги без зазначення в них особистих відомостей. У відповідь на повідомлення передбачуваний порушник (постачальник контенту, адміністратор веб-ресурсу тощо) наділений правомочністю подати зустрічне сповіщення (із посиланням на розділи 512(g)(2) і (3) ДМСА. Таке зустрічне сповіщення може стати основою для відновлення спірного вмісту.

Окремо варто вказати на підхід деяких вчених, згідно якого цифрові твори, зокрема, комп'ютерні програми, мають розміщуватися з урахуванням принципу свободи використання програмного забезпечення і необхідності розкриття вихідного коду (на основі загальнодоступних ліцензій тощо). Так, вільним вважається ПЗ, що відповідає 4 свободам:

- свобода запуску КП задля будь-якої мети і як завгодно;
- свобода вивчення, як така КП функціонує, та свобода її зміни, щоб вона виконувала обчислення так, як хоче юзер;
- свобода розповсюджувати її примірники з метою допомогти іншим юзерам;
- свобода розповсюджувати копії змінених версій КП серед інших осіб, що сприятиме наданню всій спільноті можливості отримати користь від таких модифікацій [197].

Але, не тільки регулювання в сфері авторського права та суміжних прав, як відомо, є сьогодні важливим у питанні побудови ефективного

правового забезпечення дотримання ПІВ у кіберпросторі. Так, розширюючи комунікацію й створюючи комерційні можливості, цифрове середовище, одночасно, породжує транскордонні суперечки, зокрема, щодо торгових марок та інших аспектів ІВ, наприклад, у полі права промислової власності. Глобалізація комунікацій через Всесвітню Мережу нерідко є місцем, де товарні знаки та фірмові найменування стають способом комунікації через доменні імена.

В цьому контексті, Г. Зекос наголошує на поширеній практиці законодавчого надання виключних прав на ТМ, які не володіють в достатній мірі розрізняльною здатністю. Закон, на його думку, має заохочувати суб'єктів господарювання до реєстрації дійсно відмітних товарних знаків, що чітко б відрізняли товари та послуги одного суб'єкта від аналогічних товарів і послуг іншого. А тому важливо, щоб відповідні НПА позбулися зайвої "описовості" та надто широкого трактування й набули чітких норм [315, с. 346].

П. Чакаборті вказує також на інші проблеми в сфері ТМ, зокрема, пов'язані із недобросовісною конкуренцією, коли на сайт продукту під зареєстрованим товарним знаком технологічно обізнані порушники "вбудовують" гіпертекстові посилання на інші веб-ресурси, а також вмикають невидимий секретний код (мета-тег), доступний для зчитування пошуковими системами (відповідно людина, що шукає веб-сторінку певного бренду буде введена в оману і перейде на інший сайт) [142, с. 402]. На проблеми, що стосуються недобросовісної конкуренції щодо товарних знаків вказують й інші вчені [243].

М.Д. Мюррей вважає, що саме комерційне призначення торговельної марки є ключовим аспектом до її розуміння у порівнянні з іншими об'єктами ПІВ. Тобто коли знак використовується в абсолютно некомерційних цілях і не створює плутанину щодо ТМ на ринку, то такі випадки не мають вважатися позовними. Комерційним слід вважати таке

використання, за якого суб'єкта може отримати певну вигоду чи перевагу від нього. Відповідно, концепція побудови засад для захисту торговельних марок має будуватися на фундаменті загального права, що передбачає отримання відповідної охорони після проходження таких трьох кроків: створення марки; її постійне використання в комерційній діяльності, нанесення її на свої продукти, упаковку для них, в рекламі тощо. Але для розширення меж територіального захисту з локального на такий, що стосується більш ніж однієї країни, правовласник має довести, що його активна комерційна діяльність поширюється на більш ніж один штат (в контексті США) або державу [243]. Відповідно, якщо ми говоримо про використання у кіберпросторі, то суб'єкт має фактично вести бізнес-діяльність, пов'язану з цією ТМ, не локально.

Інші дослідники також наголошують на важливості відкритого і помітного використання ТМ щодо товарів, до яких вона відноситься, тоді споживачі будуть сприймати такі товари у єдності із відповідним знаком. Тобто, за будь-якої можливості має бути зроблене фізичне нанесення знака на товари, і це в рівній мірі стосується цифрових товарів і послуг. Законодавство про товарні знаки має прагнути не до стимуляції інноваційної діяльності, а до забезпечення якісної охорони символів, що ідентифікують джерело походження товару чи послуги і, відповідно, використовуються споживачами для доступу до інформації щодо якості продукції [315, с. 350].

Окрім зазначеного, для побудови ефективного правового забезпечення дотримання права інтелектуальної власності, зокрема, щодо ТМ, у кіберпросторі слід оновити національні законодавства, взявши за основу практики розвинутих країн.

Зокрема, варто гармонізувати національне законодавство із актами Євросоюзу про товарні знаки; воно надає обширний захист доброї волі та посилення контролю над номінативним використанням. Існує потреба в

широких правах на такі об'єкти, зокрема, використання ТМ слід вважати порушенням тільки, коли воно є явно несправедливим. Так як, знаки вказують на комерційне походження продукту і спрямовують доходи до належного комерційного джерела, то вони не є такими, що перешкоджають конкуренції на рівні виробництва. Відповідно, конкуруючі особи можуть вільно пропонувати той самий товар чи послугу, якщо використовують інший знак, який вказує на інше джерело походження [315, с. 350].

Із питанням захисту торгових марок у кіберпросторі нерозривно пов'язане питання управління доменними іменами, адже, щонайменше, обране ДІ зазвичай відповідають ТЗ суб'єкта господарювання. Суперечки щодо права власності на такі об'єкти виникають, зокрема через логічне бажання власників певних знаків для бізнесу в офлайн-житті, використовувати його в цифровому просторі, бо доменні імена - це цінне доповнення до брендингу продуктів.

Зазвичай, саме правова система держави реєстрації товарного знаку і захищала його від порушення, тому такий об'єкт нерідко отримував реєстрації одразу в декількох країнах, задля розширення територіальних меж охорони. На противагу цьому доменні імена є доступними незалежно від фізичного розташування користувача, адже кіберпростір не має географічних меж. Використання таких "адрес" у цифровому середовищі призвело до розширення суто територіального характеру ТМ, нині він є глобальним.

Права на товарні знаки, як зазначають вчені [315, с. 354; 303], визначено територіально, тому, на практиці, національні закони щодо торгових марок, зазвичай, служать визнанню прав місцевого виробника. Але глобальні ринки та сучасне кібержиття заохочують більш ефективно забезпечення прав на міжнародному рівні, а також мотивують до поширення транскордонної торгівлі. Тому торгові марки, як сигнал про джерело походження продукту, перешкоджають виробникам

(постачальникам) з інших країн використовувати пов'язану із певним знаком репутацію. Тому відповідна Директива ЄС в Статті обмежила обсяг територіального права задля збереження основної функції ТМ. У цифровому середовищі видимі просторові межі (географічні кордони) руйнуються, адже з технологічної точки зору може існувати лише одне ДД, і, відповідно, воно може вказувати лише на одного конкретного суб'єкта господарювання. З посиланням на справу *Panavision Int'l v Toerpen, G.* Зекос вказує на розширення географії законодавства про ТМ в контексті доменних імен, відповідно, таке національне законодавство не прив'язаний до фізичної точки на карті і, вірогідно, діятиме поза територією окремої держави. Але і в цьому випадку є нюанс: коли сторони позиватимуться в інших країнах щодо права на знак, то завдяки відмінностям у правовому регулюванні, кожна сторона може виграти справу. Відповідно, правозастосування ускладнюється, адже нормативно-правове регулювання товарних знаків стає все більш масштабним у цифровому просторі. Тим не менш, загальноприйнятий стандарт пересічного споживача має братися за основу і під час судових спорів щодо доменних імен [315, с. 354-355].

Р. Верма, в контексті доменних імен, зазначає такі вірогідні проблеми як фреймінг, метатегування, а також "розрідження" (коли для абсолютно іншого продукту використовується подібний до відомої ТМ, а омана споживача може й не мати місця). Проблему становить також часта неможливість під час пошуку товарних знаків із доменними іменами, виокремити торговельні марки, які фактично використовуються, тому саме власник відповідного об'єкта повинен продовжувати його контролювати, щоб запобігти втраті [303].

Є й інші проблеми, які вже було згадано у минулих розділах даного дисертаційного дослідження, зокрема, кіберсквотинг, домейнінг тощо. Спеціальні приватні трибунали та політики на кшталт вже згаданої у UDRP

можуть допомогти вирішити конфлікти, що виникають у зв'язку із використанням доменних імен.

Тим не менш, на думку Г. Зекоса, Єдина політика вирішення доменних спорів не надто сприяє юридичній визначеності та передбачуваності через відсутність достатньої кількості прецедентів та багатонаціональний склад експертних груп [315, с. 350].

Як вважає М. Зальнерюте, UDRP, як засіб вирішення спорів щодо ТМ та доменних імен та захисту економічних інтересів відповідних суб'єктів, є дієвим, але також впливає на здійснення основних прав людини, зокрема, щодо свободи асоціацій, рівності, недискримінації та свободи вираження поглядів. Дослідниця вбачає такий конфлікт і в самій процедурі Єдиної Політики в контексті права на справедливий суд. Вона наголошує на невідповідності системи UDRP «міжнародно визнаним правам людини» в контексті базової справедливості та неупередженості, а тому підлягає реформуванню. Якщо ж цього не зробити, ICANN (яку було детально розглянуто у Розділі 4.2.2. даного дисертаційного дослідження) не зможе виконати свою глобальну громадську роль і, відповідно, не забезпечить захист прав людини. Дослідниця також наголошує на відсутності чіткого формулювання та відображення цілей UDRP, що може стати причиною занадто широкого тлумачення основних елементів Політики. Підкреслено і те, що суб'єкти мають наділятися правом реєструвати ТМ як доменні імена тільки, коли використання відповідного об'єкта є добросовісним та не є зловживанням. Якщо ж особи не хочуть використовувати UDRP, то можуть спробувати отримати правовий захист через муніципальні суди [314, с. 67-69].

Аналізуючи підходи до вирішення спорів щодо доменних імен та пов'язаних із ними торговельних марок, можна дійти висновку про досить широке застосування саме Єдиної політики як найбільш комфортного інструменту. Тим не менш, якщо UDRP в своєму теперішньому вигляді (як

така, що призводить до порушень основних прав людини) буде використана для розробки глобальної політики щодо механізмів альтернативного вирішення суперечок по доменним іменам, то це призведе до відмітного обмеження вказаних основних прав людини та недостатнього їх захисту в цифрову епоху.

Щодо об'єктів патентування та інших об'єктів права інтелектуальної власності, розглянутих у попередніх розділах, можна підсумувати словами О. Світличного про недосконалість та інертність системи відповідного державного управління, наслідком чого є відсутність суттєвих зрушень в адаптації законодавчої бази до сучасних економічних та політичних умов. Дослідник підкреслює те, що якщо Мінекономіки забезпечує формування та реалізує держполітику у інтелектуально-правовій галузі, то НОІВ має забезпечувати виконання завдань відповідно до комплексу окремих повноважень у цій сфері. А, отже, ключовими факторами для побудови якісного правового забезпечення дотримання прав ІВ, зокрема, у цифровому середовищі, є, по-перше, реальне функціонування ІР-суду, по-друге, розробка та впровадження нового організаційно-правового механізму, по-третє, формування нових суб'єктів державного управління й одночасна побудова нових ланок у структурі управління. Тільки так наша країна матиме впорядковану й стабільну держсистему, що відповідатиме визнаним міжнародним стандартам і принципам забезпечення належного захисту ПІВ [280, с. 153, 155].

Отже, випадків порушення ПІВ в кіберпросторі стає більше з кожним днем. І їм треба протидіяти. Як зазначає др. А. К. Бабу в контексті побудови ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі, правопорушення в Інтернет-мережі впливають на кожного, хто користується комп'ютером, тому їм треба протидіяти всіма доступними засобами. Як один з найпоширеніших методів відстеження правопорушників у цифровому середовищі, дослідник визначає цифрову

криміналістику та онлайн-розслідування, що використовують інформацію з відкритим кодом (англ. *open-source intelligence*, OSINT). Технології для збору даних про зловмисника є різними, вони допомагають об'єднати отримані відомості для визначення особи порушника, щоб зрештою "побудувати" справу проти нього. Завдяки цифровій криміналістиці, що включає в себе аналіз носіїв інформації, мережеву та експертизу пам'яті, машинне навчання, штучний інтелект слідчі органи збирають докази та визначити послідовність подій у правопорушенні. Їх вірогідних додаткових співучасників правопорушних дій. Під час відповідних дій, органи досліджують три рівні цифрового простору, а саме відкритий Інтернет, глибоку мережу та т.з. "даркнет". Так, наприклад, на останньому рівні слідчі можуть знайти інформацію про операції з криптовалютою, викривши тим самим злочинну діяльність. Цифрову криміналістику умовно поділяють на 4 області, які надають органам різний тип відомостей, а саме:

- криміналістика хостів. Даний тип охоплює криміналістичні дії, виконані на «звичайних» пристроях типу серверів та комп'ютерів, а також метод зважування криміналістичних доказів у технології блокчейн. За допомогою цього методу можна підтвердити дійсність цифрових доказів, правильність їх обробки та неможливість підробки. До уваги під час розслідування береться операційна система відповідного гаджету. Основна проблема на даному етапі - це рандомізація адрес ядра, для її вирішення використовуються 4 підходи дерандомізації: виправлений та невиправлений коди, код перебору та дані ядра лише для читання;
- мобільна криміналістика. Вона відрізняється від інших видів по апаратному та програмному забезпеченні, енергоспоживанні та загальній мобільності. До того ж зазвичай мобільні пристрої є носіями особистих даних, що нерідко є критичними для ведення розслідування. На цьому етапі використовуються загальні методи

збору даних, т.зв. "вилучення даних" шляхом ручного, логічного методів, шістнадцяткового дампу, відщеплення та мікрочитування. Кожен з цих методів надає різні відомості та є різним за ступенем складності, так логічне вилучення та шістнадцяткові дампи є нескладними, а тому швидшими й ефективнішими;

- мережева криміналістика. Вона передбачає аналіз відомостей з хоста чи всієї мережі, інформація видобувається, зокрема, за допомогою журналів та записів трафіку. Проблема даного методу - це обсяг трафіку та журнальних даних, бо де-факто проаналізувати кожен окремий пакет даних практично нереально, бо це занадто ресурсоємко;
- хмарна криміналістика. Вона передбачає аналіз відомостей із хмарних служб за допомогою спеціального додатку, який збирає дані і пересилає їх в інше місце для експертизи. Даний метод передбачає дослідження, синхронізацію та безпеку [290, с. 2-19].

Цікавої, і, як вбачається перспективною, також була практика для захисту інтелектуальних активів, запроваджена ВОІВ, - послуга WIPO PROOF. Організація запустила її у травні 2020 року для надання заінтересованим суб'єктам можливість отримувати цифровий відбиток файлу в певний момент часу, до того ж воно було б захищене від несанкціонованого доступу. Дана практика відповідала світовим стандартам з безпеки та захисту даних клієнтів, а також вимогам Євросоюзу щодо постачальників довірчих послуг по видачі електронних часових позначок. Тим не менш, з початку 2022 р. отримати відповідний токен неможливо - програма перестала діяти. Хоча вбачається, що послуга буде сприяти транскордонній співпраці та значно полегшить роботу судів, представляючи відповідні докази існування цифрових файлів у певний момент часу, які були доступні десятима світовими мовами [244].

Отже, як свідчить іноземна практика, Україна має перед собою досить широкий спектр концептуальних засад побудови ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі. Деякі з них уже впроваджуються, інші, можливо, будуть удосконалені і теж застосовуватимуться.

Так, розпорядженням № 402-р від 01.06.2016 р. Кабмін схвалив Концепцію реформування державної системи правової охорони інтелектуальної власності в Україні та зобов'язав Міністерство економічного розвитку і торгівлі (далі - Мінекономрозвитку) й заінтересовані органи створити та представити на розгляд план заходів з її реалізації. Дана Концепція, в основі якої лежить Стратегія сталого розвитку "Україна-2020", передабачала, що наша держава має стати не лише економічно сильною, але й міжнародним суб'єктом із передовими інноваціями, завдяки чому буде створено умови для становлення національної інноваційної системи та ефективну транспарентну структуру державного управління сферою ІВ, забезпечено прозорість процедур набуття та розпорядження відповідними правами, підвищено ефективність роботи держорганів й якість охоронних документів у вказаній сфері, а також буде забезпечено введення в дію та робота ефективного механізму захисту ПІВ. Це все вбачалося досягнути через три наступні напрями реалізації Концепції. Так, було запропоновано впровадити дворівневу структуру державної системи правової охорони ІВ, в якій Мінекономрозвитку відповідатиме за створення й реалізацію держполітики у відповідній сфері, а спеціальний національний орган ІВ - виконуватиме окремі публічні функції для такої реалізації, із одночасною ліквідацією Держслужби ІВ (далі - ДСІВ). Також вбачалося за необхідне реорганізувати систему колективного управління (далі - СКУ) майновими авторськими та суміжними правами й вдосконалити та гармонізувати національне законодавство у відповідності до європейського [89].

Розпорядженням № 632-р від 23.08.2016 р. Кабмін затвердив вище згаданий план заходів з реалізації даної Концепції. Перший напрямок реалізації Концепції (запровадження транспарентної дворівневої структури) полягав, зокрема, у ліквідації ДСІВ, реорганізації ДП "Український інститут інтелектуальної власності", поданні на визначення державної організації, що виконуватиме функції НОІВ із затвердженням її положення, аналізі іноземного досвіду фінансування патентних тощо. Удосконалення та гармонізація законодавства полягала у розробці, супроводженні в ВРУ відповідних НПА щодо внесення змін до законів щодо захисту АП і суміжних прав, зокрема, в мережі Інтернет. Реорганізація СКУ передбачала приведення національного законодавства з відповідного питання у відповідність до актів ЄС, забезпечення прозорості діяльності ОКУ, запровадження транспарентної електронної системи обліку колективної винагороди, проведення моніторингу діяльності ОКУ тощо [74]. Варто зазначити, що до появи розглянутої Концепції існувала трирівнева структура правової охорони ІВ, де головним органом виступало Мінекономрозвитку, на другому рівні знаходилась ДСІВ, на третьому - державні організації сфери управління ДСІВ (Укрпатент, Інтелзахист та УААСП).

Побудова дворівневої структури та інші питання стали предметом жвавої дискусії різних кіл. І уже в жовтні 2020 року розпорядженням Кабміну № 1267-р «Про Національний орган інтелектуальної власності» було визначено, що ДП «Український інститут інтелектуальної власності» буде виконувати функції НОІВ [77]. У листопаді 2022 р. дане розпорядження втратило чинність на підставі Розпорядження Кабінету Міністрів № 943-р (від 28.10.2022 р.), яким також функції НОІВ було покладено на ДО «Український національний офіс інтелектуальної власності та інновацій» [17].

Наразі, у зв'язку із повномасштабним вторгненням Російської Федерації в Україну, питання правового регулювання у галузі ПІВ дещо відійшло на другий план. Хоча повністю “законсервованим” не є (про що свідчить, зокрема, прийняття нового актуального Закону про авторське право та суміжні права у 2022 році. Тим не менш, питання все ще потребує вирішення.

В контексті концептуальних засад побудови правового забезпечення дотримання ПІВ, окремо, наостанок, варто вказати і на ті, що стосуються конкретно самого цифрового середовища. Так, щодо сучасної концепції адміністративно-правового захисту кіберпростору в Україні, то О. Зубко формулює її в таких бажаних кроках:

- як пріоритетне завдання - розробити та впровадити в дію ефективне інформаційне законодавство та національний стратегічний інструментарій щодо використання кіберпростору;
- вдосконалити практичну діяльність суб'єктів кібербезпеки;
- розробити та впровадити нові програми й заходи в сфері захисту інформації та протидії кібератакам;
- забезпечити надання високоякісних цифрових послуг;
- забезпечити інтенсивне та безпечне входження українського суспільства у світовий кіберпростір [317, с. 54].

Отже, концептуальні засади побудови ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі як основоположне розуміння відповідної побудови ефективного правового забезпечення, сукупність поглядів на неї вчених та практиків і нормотворців, що втілюють відповідні концепції, є підґрунтям для реформування сучасної ситсеми ІВ в країні. Саме тому владним органам важливо співпрацювати з юридичними експертами, представниками академічних кіл та кінцевими споживачами й безпосередніми правовласниками. Адже захист прав інтелектуальної власності у такому

особливому сегменті як цифрове середовище вимагає особливого гнучкого підходу, що б врахував реалії сьогодення.

Підсумовуючи концепції, розроблені вченими й практиками, можна виділити такі засади побудови ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі:

- країнам слід пристосовувати своє законодавство до норм загальнозживаних міжнародно-правових актів та стандартів, зокрема, до Закону про захист авторських прав у цифрову епоху, Директиви ЄС про авторське право, інтернет-договорів ВОІВ тощо;
- подолання проблеми транскордонності Інтрнету та загалом цифрового простору, зокрема, шляхом співпраці світового співтовариства у розробці та прийнятті універсального закону, адже правопорушники нині, користуючись відмінностями у національних законодавствах різних держав, можуть посилатися на відсутність складу правопорушення щодо об'єктів та прав ІВ, якщо відповідне діяння є порушенням в їх державі, але не є - в іншій. Задля виконання такої рекомендації можливо розробити типовий НПА для захисту цифрової ІВ із визначенням у ньому покарання, юрисдикції тощо;
- є доцільним створення загальновизнаної системи юрисдикції у цифровому домені шляхом активної міжнародної співпраці, гармонізації законів та інноваційних підходів; ускладненість відстеження порушень ПІВ у кіберпросторі має бути подолана, адже нині застосовуються застарілі цивільні, кримінальні та адміністративні засоби правового захисту, яких є недостатньо;
- необхідним є більш чітке тлумачення дій, що є порушенням ПІВ, зокрема, у кіберпросторі, бо нині воно є досить розмитим;
- розробка та впровадження технологічних заходів захисту має відбуватися одночасно із реформуванням законодавства, адже, на думку, деяких вчених, DRM та подібні методи не є достатньо

ефективними. Зокрема, пропонується практика блокування веб-сайтів-порушників. Тим не менш, даний метод не всі підтримують, адже, як було зазначено вище, не кожне порушення є порушенням для іншої правової системи, і, відповідно, блокування може виявитися неправомірним. Щодо DRM, то деякі вчені навпаки пропонують усіляко заохочувати правовласників до його використання;

- також вказаним вище технологічним методам охорони треба забезпечити правовий захист, а за їх обхід - передбачити суворішу відповідальність;
- варто також зобов'язати інтернет-провайдерів контролювати та фільтрувати сайти-порушники, щоб не отримати статус співучасниками у порушенні відповідних прав;
- у законодавстві має бути чітке і транспарентне визначення кіберсквотингу, а також передбачено шляхи покарання порушників і методи відшкодування шкоди;
- щодо засобів індивідуалізації учасників цивільного обороту, країнам слід в своєму законодавстві прописати відповідні норми без зайвої "описовості" та надто широкого трактування, адже інакше права на ТМ та подібні об'єкти можуть бути порушені відносно легко тощо.

Є ще багато рекомендацій щодо побудови ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі, зокрема, конкретно щодо України - дійсне функціонування, а не лише існування "на папері" IP-суду. Загалом же для світової спільноти було б найкращим рішенням багатьох проблем у царині дотримання ПІВ саме розробка, прийняття та приєднання всіх (більшості) країн до універсального кіберзакону для захисту відповідних прав в цифровому середовищі, де б було, зокрема, врегульовано питання юрисдикції та інших "наболілих" моментів. Так би ми досягли глобальної правової одноманітності, тим самим зменшивши навантаження на суди під час розгляду відповідних

справ, полегшивши правозастосування тощо - а це, в свою чергу, призведе до активізації творчо-інноваційної діяльності серед населення.

Висновки до Розділу 5

Україна сьогодні переживає ненайкращі часи, що особливо помітно в зв'язку із повномасштабним вторгненням Російської федерації і введенням режиму воєнного стану. Така ситуація негативно впливає на всі аспекти життя країни. тим не менш, навіть зараз є позитивні зрушення у деяких сферах, зокрема, у галузі права інтелектуальної власності. Так, наприкінці 2022 року було прийнято новий Закон про авторське право і суміжні права, розробляються та втілюються в життя нові стратегії, політики та інструменти формування правового забезпечення дотримання права інтелектуальної власності у кібернетичному просторі. Отже, правова база дійсно реформується з урахуванням викликів сьогодення.

Важливим у цьому руслі є не тільки перетворення, що робляться в країні безпосередньо, але й те, як світ та його провідні країни працюють у даному напрямку. Адже саме досвід інших - це те, що може стати в нагоді при розробці означених політик та інструментарію Україною - на чужих помилках легше вчитися, не роблячи при цьому своїх.

У заключному, п'ятому, Розділі дисертаційного дослідження на основі використання теоретичних наукових та загальнонаукових методів пізнання було детально опрацьовано нові підходи до формування правового забезпечення дотримання ПІВ у кіберпросторі в Україні, проаналізовано ефективність такого забезпечення в інших країнах на основі шляхів впровадження їх найкращих практик, а також вивчено концептуальні засади його побудови. Результати, отримані автором у процесі дослідження, дали змогу дійти наступних висновків:

1. Внесення змін до старого Закону про авторське право та суміжні права 1993 року, а, точніше, його заміна на новий Закон 2022 року

були зумовлені євроінтеграційним вектором спрямуванням України, зокрема, у частині імплементації положень документів Європейського союзу у вітчизняне законодавство. Аспектами вказаного є положення про отримання охорони правам особливого роду (*sui generis*), що є результатом імплементації Директиви 96/9/ЄС «Про правову охорону баз даних» 1996 р.; про відповідальність провайдерів послуг обміну контентом за порушення АП та суміжних прав, в основі чого лежать положення Директиви Європейського Парламенту і Ради (ЄС) 2019/790 2019 р. про авторське право і суміжні права на Єдиному цифровому ринку та про внесення змін до директив 96/9/ЄС та 2001/29/ЄС.

2. Новий Закон про авторське право та суміжні права став справжнім проривом у авторсько-правовій царині: ним було оновлено та конкретизовано випадки вільного використання об'єктів АП та суміжних прав (зокрема, тепер можливе тимчасове вільне відтворення твору); введено поняття твору, музичного кліпу, сирітського твору, цифровому контенту ("електронна (цифрова) інформація"), інтерактивного надання доступу публіки до об'єкта АП й суміжних прав та інші; оновлено поняття відеограми, твору образотворчого мистецтва, фотографічного та службового творів, бази даних, комп'ютерної програми, відтворення тощо; збільшено перелік вірогідних творів-отримувачів правової охорони; означено головний критерій охороноздатності твору (оригінальність); додано норми щодо використання технологій штучного інтелекту (зокрема, в контексті *sui generis* на неоригінальні об'єкти, згенеровані комп'ютерними програмами); розширено межі регулювання не тільки на матеріальні об'єкти, в яких втілені твори, але й на електронні (цифрові), в якому твори були зафіксовані; оновлено підходи до визначення дій, що порушують особистих немайнові та майнові

права; удосконалено інститут компенсації замість відшкодування збитків або стягнення доходу; вдосконалено порядок припинення порушень АП та суміжних прав з використанням інтернету тощо.

3. Зміни, введені новим Законом про авторське право та суміжні права, торкнулися також особистих немайнових та майнових прав автора. Тепер перелік особистих немайнових прав включає право надати роботі назву або взагалі залишити її без такої, а також право автора присвятити твір певним особам, датам або подіям. Щодо матеріальних авторських прав, особливого значення набули положення про легальність лінкування та фреймінгу, якщо матеріал був попередньо правомірно доступний і без вказаних дій, і їх неправомірність у разі надання через них доступу до матеріалу, якщо такий доступ обмежено правовласником. Також новим Законом додано вказівку на майнове право на справедливую винагороду. При укладенні договору про передання майнових прав його предметом не можуть вважатися об'єкти чи майнові права, яких не існувало на момент укладання відповідної угоди. В контексті такого договору у сторони є право вимагати від контрагента виплатити йому додаткову пропорційну винагороду за використання твору або його виконання, якщо розмір винагороди за використання за укладеним між сторонами договором став непропорційно низьким.
4. Закон про авторське право 2022 р., хоч і є дійсно позитивним зрушенням для української правозахисної практики, має ряд недоліків, а саме: відсутність визначення поняття «виключне право» (у Законі 1993 року було наведене); використання обох термінів «суб'єкт майнових авторських прав» та «суб'єкт авторського права», без зазначення, що друге поняття включає в себе перше (як було по суті в попередньому Законі); присутність колізії у питанні розподілу майнових прав на твір, створений за замовленням, такі права

автоматично переходять до замовника по факту створення твору (якщо інше не передбачено договором), хоча за ЦК вони належать сторонам договору спільно; вірогідність ризику зловживань при приватному копіюванні матеріалу (спосіб використання) через наявність формулювання "відтворення в особистих цілях особи...чи близьких знайомих такої сім'ї" без відповідного визначення таких "знайомих"; вичерпність переліку способів використання творів, що не відповідає мінливості сьогодення у зв'язку із невинним розвитком технологій, бо передбачити всі можливі способи використання неможливо практично тощо.

5. Ефективність правового забезпечення дотримання права інтелектуальної власності у кіберпросторі в різних країнах стикається з такими перешкодами: беззупинна поява нових типів інтелектуальної власності, що провокує неспроможність нормотворців встигнути за трендами цифрових трансформацій; відсутність уніфікованого правового регулювання, що не дає змогу забезпечити транскордонний захист відповідних прав; легкість відтворення та розповсюдження об'єктів ПІВ через цифрові канали "грає на руку" порушникам; відсутність (недостатність) дієвих заходів кібербезпеки, зокрема, через постійне збільшення кількості та ускладнення кіберзагроз; великі обсяги даних сприяють нерегульованості їх правового забезпечення та порушенням конфіденційності; способи управління правами інтелектуальної власності змінюються через використання технологій блокчейн, що мають децентралізовану архітектуру; недостатня урегульованість сфери смарт-контрактів (також засновані на блокчейн), які є дієвим засобом, зокрема, при здійсненні транзакцій без втручання фінансових установ.
6. З урахуванням позитивних результатів, яких досягли деякі країни світу, Україні бажано перейняти наступні шляхи впровадження їх

практик: максимально застосовувати уніфіковані стандарти захисту при розробці нормативного регулювання задля недопущення різнорідного трактування положень та уникнення неоднозначності у їх практичному застосуванні; усіляко просувати розуміння необхідності реєстрації авторського права на твори, навіть з урахуванням автоматичного надання захисту таким об'єктам по факту створення (як радить Євросоюз, Індія та інші держави) та удосконалити саму процедуру реєстрації (полегшити її - як це зроблено в США); також спростити процедуру реєстрації торговельних марок, зокрема, дозволяючи проходити її через спеціалізовані мобільні застосунки (за в'єтнамським прикладом); врегулювати на законодавчому рівні питання захисту об'єктів "цифрового мистецтва" та криптомистецтва (як це зроблено в Європейському союзі); розробити та впровадити стратегію ІВ, розраховану на 10 років, для надання підтримки бізнесу і стимулювання творчо-інноваційної діяльності (на прикладі Сінгапуру); для уникнення спорів та зловживань у сфері використання штучного інтелекту імплементувати в законодавство та правозастосування досвід Японії, Сінгапуру та Великобританії; впровадити механізм балансування вигод при розподілі прибутку в технологічній інноваційній діяльності (за досвідом Китаю); залучати до розробки стратегій, НПА та політик у галузі захисту права інтелектуальної власності у кіберпросторі не тільки фахівців з права, але й технічних спеціалістів (щоб відповідні норми дійсно відповідали технічним реаліям в сфері інформаційних технологій) та тісно взаємодіяти з із місцевими правоохоронними органами (за моделлю В'єтнаму); розробити та впровадити "програми прискорення" для здешевлення та прискорення процедури патентування об'єктів ІВ (як це зроблено в Сінгапуру); спростити

судові процедури при розгляді справ щодо захисту прав інтелектуальної власності, реально розпочати роботу Вищого суду з питань інтелектуальної власності; налагоджувати співпрацю між різними відомствами для протидії кіберправопорушенням у сфері ІВ та розвивати співробітництво з іншими державами та міжнародними організаціями з метою обміну практичним досвідом й спільній протидії транснаціональним порушенням.

7. Надано визначення концептуальним засадам побудови ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі як основоположному розумінню відповідної побудови ефективного правового забезпечення, сукупність поглядів на неї вчених та практиків, а також нормотворців, що втілюють відповідні ідеї та концепції у нормативно-правове регулювання щодо права інтелектуальної власності у кіберпросторі.
8. На основі аналізу досліджень різних вчених визначено, що авторсько-правове регулювання є сьогодні основоположним у питанні побудови ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі. Разом з тим вказано на сумнівність ефективності законів про авторське право з точки зору незаконного тиражування творів через швидкий розвиток та прогрес у технологіях копіювання й його малу вартість та легкість оцифрування творів. При цьому цивільні, кримінальні та адміністративні засоби правового захисту не є достатніми через транснаціональність ІТ, що, відповідно, сприяє ускладненню відстеження порушень авторських прав у цифровому середовищі. Негативний вплив спричиняє також відсутність єдиного нормотворчого органу, який би контролював Всесвітню мережу Інтернет, політичних зобов'язань, всеосяжних нормативних механізмів. Погіршує ситуацію й погане виконання наявного

законодавства у розглянутій сфері. Особливе занепокоєння викликає проблема транскордонності цифрового середовища.

9. На основі аналізу наявних концепцій побудови ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі запропоновано наступні засади побудови відповідного забезпечення в Україні: активна співпраця світової спільноти у пошуку регуляторних формул для вирішення наявних проблем щодо забезпечення дотримання права інтелектуальної власності в кіберпросторі, адже відповідні об'єкти не захищені загальноприйнятими стандартами як нецифрові традиційні твори; створення загальновизнаної системи юрисдикції в кіберсередовищі шляхом активної міжнародної співпраці, гармонізації законів та інноваційних підходів; подолання проблеми екстериторіального охоплення та втамування потреби в гармонізації між юрисдикціями, оснований на Каліфорнійському законі про конфіденційність споживачів та Загальному регламенті про захист даних, які наголошують на важливості чіткої правової регламентації, підзвітності та захисту прав особи на конфіденційність у кіберсередовищі; детальна вказівка в законодавстві на підсудність справ з цифрового порушення прав інтелектуальної власності, вчиненого представниками іншої країни, судам своєї держави; подолання технологічної необізнаності, зокрема, серед правоохоронних органів, які не є достатньо обізнаними щодо цифрових порушень; надання правового захисту технологічним методам охорони прав авторів та правовласників, введення в дію жорстких положень щодо відповідальності за обхід технологічних заходів із основою на Інтернет-договорах ВОІВ; забезпечення виконання правових заходів для зберігання даних і записів про використання Інтернет-мережі шляхом введення журналів і реєстрів

для її використання, що мають робити постачальники інтернет-послуг протягом розумного строку задля надання допомоги у відстеженні IP-адрес порушників; розробка і законодавче закріплення положень щодо нового розширеного режиму обміну файлами і посилення відповідальності онлайн-посередників; впровадження програм громадської освіти серед інтернет-користувачів із їх інформуванням про можливі правопорушні дії та засоби самостійного захисту від відповідних порушень ПІВ в кіберпросторі.

10. Для досягнення глобальної правової одноманітності у питанні побудови ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі вбачається за необхідне розробити та прийняти універсальний акт, присвячений подоланню проблеми транскордонності Інтернету та загалом цифрового простору, зокрема, шляхом співпраці світового співтовариства. Адже сьогодні порушники прав інтелектуальної власності у кіберпросторі, користуючись відмінностями у національних законодавствах різних держав, можуть з легкістю посилатися на відсутність складу правопорушення, якщо відповідне діяння є порушенням в їх державі, але не є - в іншій. У такому нормативно-правовому акті передбачити норми щодо покарання, юрисдикції тощо. Також важливо, щоб держави розробляли своє законодавство у відповідності до норм загальновизнаних міжнародно-правових актів та стандартів, зокрема, Закону про захист авторських прав у цифрову епоху, Директиви ЄС про авторське право, інтернет-договорів ВОІВ та подібних. Також позитивний вплив матиме розробка типового закону для захисту цифрової інтелектуальної власності для сприяння окремим країнам у співпраці з міжнародними організаціями на кшталт ICANN.

Результати дослідження, викладені у Розділі 5, відображено у таких публікаціях автора: [325]; [146]; [342]; [153]; [161]; [166]; [1686]; [4228].

ВИСНОВКИ

У дисертаційному дослідженні здійснено теоретичне узагальнення й наведено нове вирішення наукової проблеми, що полягає у розкритті сутності і змісту забезпечення дотримання права інтелектуальної власності у кіберпросторі з урахуванням світового досвіду та виробленні дієвих пропозиції для України. Отримані результати дослідження надали можливість сформулювати наступні узагальнені висновки та рекомендації:

1. Глобалізація на сьогодні повністю змінила світ, і, в першу чергу, це проявилось у переорієнтації економіки на інноваційну модель розвитку, бо майже кожен аспект розвитку сучасного життя в будь-якій державі нерозривно пов'язаний саме із розвитком та впровадженням інновацій, що і є рушійною силою та основою для вироблення конкурентних переваг серед суб'єктів міжнародного права. Суспільство розробляє та використовує інноваційні активи, міжнародні та приватні суб'єкти обмінюються ними між собою задля спонукання ще більш активної інноваційної діяльності, і це в більшій мірі стосується саме інтелектуальної власності, що і є найбільш яскравим прикладом відповідних здобутків. І нині найбільше питань в даній сфері викликає саме забезпечення дотримання права відповідної інтелектуальної власності у кібернетичному просторі, який нині по праву вважається четвертим виміром людського існування (на рівні із повітряним, земним та водним). З урахуванням зазначеного, іноді інтелектуальну власність, що існує в кіберсередовищі навіть називають "кібернетичною власністю".
2. Обґрунтовано, що проблема забезпечення дотримання права інтелектуальної власності у кібернетичному просторі значно ускладнюється майже щоденною появою нових інтелектуальних напрацювань, в той час як наявне нормативно-правове забезпечення

"не встигає" за викликами і новими ризиками і, відповідно, потребує значного удосконалення, що, зокрема, передбачає і запозичення дієвих практик та інкорпорації нормативних положень актів провідних країн світу. Також відсутність єдиної стратегії досягнення балансу між бажаннями споживачів цифрових інтелектуальних активів та правовласниками відповідних об'єктів сприяє поглибленню зазначеної проблеми, а тому потребує застосування комплексного підходу для свого вирішення, що передбачає, окрім перегляду нормативно-правового регулювання, виокремлення та опрацювання доктринальних ідей та розробок теоретиків-представників академічних кіл, а також врахування думки інформаційної кіберспільноти. Наріжним каменем є і транскордонність кіберпростору, адже він буквально не є обмеженим державними кордонами і, відповідно, рамками державного суверенітету, що викликає суперечки при віднесенні кіберпорушень до відання того чи іншого правопорядку та негативно сказується на визначенні суб'єктів відповідного правопорушення, зокрема, коли такі об'єкти знаходяться в різних країнах.

3. Встановлено, що "віртуальність" інтелектуальної власності не применшує (й не рідко підвищує) її комерційну цінність як актива, а тому захист даного актива має забезпечуватися також на основі основоположних засад - принципів, зокрема, принципів права власності на інтелектуальну власність, примусового ліцензування, справедливої поведінки, балансу прав правовласника та громадськості, а також гармонізації як взаємної узгодженості та підпорядкування єдиній взаємно-відповідній системі нормативних інструментів та стандартів. Завдяки останньому принципу можна буде досягти правової одноманітності в усьому світі, що, відповідно,

позитивно впливатиме на бажання творців активізувати свою творчо-інноваційну діяльність.

4. Визначено концепт реалізації права, що являє собою реальне, закріплене на практиці втілення в життя формально-визначених правових розпоряджень шляхом правомірних дій (діяльності або бездіяльності) суб'єктів суспільно-правових відносин, метою чого є задоволення основних потреб громадян, суспільства та всієї держави в цілому на підставі засобів та методів, встановлених державою в особі своїх органів. І вирішальне значення для фактичної правореалізації має практичне здійснення заходів, що і є нормою права. Реалізація таких норм, що має три форми прояву (виконання, дотримання, використання), є ключовим етапом процесу правового регулювання та має особливу практичну значимість безпосередньо для сфери права інтелектуальної власності. Основою її є саме правомірна поведінка суб'єктів суспільних відносин, а також створення і впровадження належного правового забезпечення інноваційно-творчої діяльності. Права і обов'язки учасників правовідносин здійснюються саме через правореалізацію; і спори між ними мають вирішуватися, зокрема, шляхом залучення до правозастосовчого процесу спеціальних державних органів - це сприятиме скорішому врегулюванню наявного конфлікту.
5. Надано визначення місцю кіберпростору (як інтерактивного домену, що складається із цифрових мереж, які використовуються для зберігання, зміни, передачі та подібних дій із інформацією) в інформаційному середовищі. Відповідно, кібернетичний простір є елементом (точніше - центральним сегментом) системи інформаційного середовища (сфери) на рівні із традиційним інформаційним простором, у ньому сконцентровані глобальні потоки економічно-політичної природи та соціальних взаємин. Дане

твердження свідчить про необхідність формування ефективного та стабільного українського інформаційного простору, що сприятиме встановленню та розвитку стійкого кіберпростору в країні. Виконання такого завдання базується на необхідності посилення нормативно-правового забезпечення функціонування українського кібернетичного простору програмними та регулюючими документами та системою принципів, що включають, зокрема, принципи поваги прав і свободи людини, відповідальності, розумності, усвідомленості та потрібного втручання тощо.

б. Надано визначення наступним концептам:

- а. "оцифрування" як процесу створення цифрової об'єктивної форми фізичних об'єктів;
- б. "цифровізації (діджиталізації)" як забезпеченню або поліпшенню ділових та інших процесів шляхом використання цифрових технологій та діджитизованої інформації;
- с. "цифровій трансформації" як безпосередній трансформації бізнесу, що забезпечується діджиталізацією.

Окремо акцентовано увагу на тому, що цифровізація може мати негативні результати у вигляді проблем з безпекою порушення конфіденційності, погіршення культурного рівня громадян, поглиблення їх соціальної відчуженості. Тим не менш, вона, як один з ключових елементів кіберпростору, має наступні позитивні характеристики: мінімізація витрат та оптимізація основних робочих процесів у зв'язку із відмовою від матеріальних форм зберігання даних, і, відповідно, перехід на більш "екологічний" рівень; підвищення культури та цифрової грамотності населення; забезпечення швидкого реагування на виникаючі кіберпроблеми та виклики; надання сприятливих умов для спрощеної та легкої комунікації із кінцевим споживачем товарів та послуг тощо.

Задля подолання викликів у галузі цифровізації й посилення сильних сторін даного феномену на різних рівнях, надано наступні рекомендації для можновладців: сприяти формуванню цифрової сумісності між країнами світу із обов'язковою розробкою та впровадженням набору глобальних правил з урахуванням їх економічних, політичних та культурних відмінностей; забезпечити цифровий розвиток нації з метою нівелювати цифровий розрив між різними соціальними групами; розробити та впровадити надійні технології для всіх громадян з одночасним зниженням рівня неефективності та витрат; створити та інтегрувати міжнародну платформу, яка використовуватиметься для вирішення проблем, спричинених негативним впливом цифрових технологій; створити фонд підтримки, кошти якого мають спрямовуватися на розвиток цифрової інфраструктури та цифровізацію в державі.

7. Запропоновано розуміти структуру відносин щодо дотримання права інтелектуальної власності у кіберпросторі як симбіоз суб'єктів, що вступають у правовідносини з приводу інтелектуальної власності, і доцільного способу зв'язку між ними з основою на суб'єктивних юридичних правах та обов'язках по відношенню до певних соціальних благ чи інтересів у кіберпросторі. Елементами такої структури визначено об'єкт правовідносин, їх суб'єкти та зміст таких правовідносин. Перелік традиційних об'єктів інтелектуальної власності (їх умовно поділено на 4 групи - об'єкти авторського права, об'єкти суміжних прав, об'єкти промислової власності та нетрадиційні об'єкти) для цілей виокремлення елементів структури відносин щодо дотримання права інтелектуальної власності саме в кіберпросторі було доповнено інформацію, інформаційними системами та інформаційно-телекомунікаційними технологіями, інформаційними ресурсами і продуктами, доменними іменами тощо.

Суб'єктами означених відносин визначено творців об'єктів права інтелектуальної власності, власників відповідних прав, правонаступників та інших осіб, чия діяльність пов'язана із використанням, захистом результатів творчо-інноваційної діяльності, а також тих, хто вступає у такі відносини в процесі діяльності у кіберсередовищі та безпосередньо Всесвітній Мережі (це провайдери, оператори зв'язку, реєстратори, інтернет-реєстри тощо). Суб'єктивні права та юридичні обов'язки названих суб'єктів, в яких ключовими складовими суб'єктивного права є правовикористання, правовиконання та правозахист, становлять зміст означених відносин. Увага зацентрована на розкритті суб'єктивних права учасників правовідносини у кібердомені саме через власні дії користувачів, адже вони провокують виникнення, зміну, припинення прав і обов'язків інших учасників взаємодії у кібернетичному середовищі, а не лише через обов'язки третіх осіб. Обґрунтовано, що таке визначення і правова кваліфікація зазначених елементів сприятиме якісному аналізу наявних нормативно-правових актів та розпізнаванню їх уразливих сторін, на основі чого в подальшому можна буде розробляти політики удосконалення відповідного законодавства, розроблення нового, а також намітити шляхи розвитку у відповідній сфері.

8. Досліджено генезу становлення правового регулювання функціонування окремих інститутів інтелектуальної власності загалом, та, зокрема, у кіберпросторі, що характеризується як загальними закономірностями, так і специфічними ознаками. Зазначено, що свої витoki правове регулювання інтелектуальної власності бере мало у 17 столітті, а щодо кіберсередовища - наприкінці 20 століття. Встановлено, що останньому сприяло реформування міжнародних договорів з права інтелектуальної

власності, введення в дію Договорів Всесвітньої організації інтелектуальної власності про авторське право та про виконання і фонограми (відомих як "інтернет-договори ВОІВ") з розробкою на їх основі сучасного національного правового інструментарію різних держав, впровадження Директив та Регламентів Євросоюзу тощо. Ключовою особливістю даних документів встановлено відсутність в них визначення Інтернету як середовища використання об'єктів інтелектуальної власності, натомість використовується термін "цифрове середовище". Обґрунтовано необхідність знати особливості генези правового регулювання функціонування інститутів права інтелектуальної власності у кібердомені тим, що на основі таких відомостей можна визначити помилки та недоліки попередніх інструментів забезпечення дотримання відповідних прав і, на такому підґрунті, розробити та впровадити нове, більш досконале, правове регулювання. Встановлено, що для України вирішальними етапом генезису став період з отримання незалежності, який ознаменував початок активної розробки власного законодавства. Доведено, що українське законодавство справді переглядається і покращується з урахуванням сучасних тенденцій у кіберсвіті, зокрема, було розширено перелік об'єктів інтелектуальної власності тими, що мають безпосереднє відношення до цифрового середовища.

9. Визначено коло проблемних питань правового регулювання відносин щодо дотримання права інтелектуальної власності у глобальних інформаційних та комп'ютерних мережах. Такими вбачаються: в галузі авторського права - онлайн-піратство, особливо щодо програмного забезпечення, активний продаж піратських продуктів, фреймінг, лінкінг - глибокі посилання, метатегування; в сфері права промислової власності - питання захисту патентів та боротьби із незаконним використанням товарних знаків (торговельних марок) та

інших засобів індивідуалізації учасників у цивільному обороті; в галузі специфічних об'єктів - кіберсквоттинг та тайпсквоттинг щодо доменних імен (нині вони не є об'єктом права інтелектуальної власності в більшості правових моделей, але теж слугують засобами індивідуалізації, а тому, на думку автора дослідження, мають отримати відповідну охорону), сприяння вчиненню правопорушень у зв'язку із використанням технології штучного інтелекту тощо. В цьому контексті наголошується на розумінні інтелектуальної власності як складової нематеріальних активів підприємства, вказані порушення щодо яких можуть призвести як до матеріальних втрат, так і до нанесення шкоди діловій репутації суб'єктів господарювання.

10. Рекомендовано у якості неюридичних засобів та методів дотримання права інтелектуальної власності у глобальних інформаційних та комп'ютерних мережах: суб'єктам господарювання та іншим організаціям - розвивати й контролювати свої інтелектуальні активи, вживати всіх наявних засобів для її захисту, зокрема, таких як управління цифровими правами; кінцевим користувачам кіберпростору (фізичним особам) - опанувати основи інформаційної та кібергігієни, розвивати в собі повагу до чужих здобутків у сфері творчості та інновацій, також використовувати всі наявні інструменти для захисту своїх творінь; державі - спонукати суспільство до розвитку обізнаності щодо можливих порушень інтелектуальних прав у кіберпросторі та активної їм протидії. Відповідне включає як юридичні засоби, так і соціальні й технологічні.

11. Визначено, що за світовою практикою авторське право поділено на дві окремі системи - загальну (країни англо-американської правової сім'ї) та систему цивільного права (країни романо-германської правової сім'ї). Відповідно, англосаксонська (загальна) система

охороняє саме майнові права, в ній авторське право прирівняно до форми власності; континентальна система (цивільного права) охороняє також і немайнові права, адже креативна діяльність творця є невід'ємною від його особистості, є її відображенням, і, таким чином, потребує охорони на основі природної справедливості, зокрема, і в аспекті кіберсередовища. Україна слідує в даному питанні системі цивільного права.

12. За допомогою використання методу компаративістики було співставлено правові засади регулювання відносин дотримання права інтелектуальної власності у кібернетичному просторі в країнах Європи, Співдружності Незалежних Держав та в США. Встановлено, що американське право виокремлює чотири основні типи об'єктів інтелектуальної власності (патенти, авторські права, комерційні таємниці та торговельні марки), взаємодія з якими підпадає під дію нормативно-правових актів окремих штатів, федерального законодавства та загальновизнаних міжнародних конвенцій. Захист об'єктів можливий у рамках кримінальної, цивільної та прикордонної охорони, і місцевий правовласник сам відповідає за цивільне правозастосування своїх прав інтелектуальної власності, у випадку крадіжки якої може звернутися до Національного координаційного центру з прав інтелектуальної власності методами інтернет-зв'язку. Вказане вважається за доцільне для взяття за основу при розробці українського законодавства, зокрема, шляхом інкорпорації відповідних положень.

Щодо європейського правового регулювання, то рекомендовано гармонізувати українське законодавство до більшості Директив ЄС з питань захисту інтелектуальної власності, зокрема, в кіберпросторі. Вважається за доцільне запозичити європейську методику превентивного захисту прав власників інтелектуально-творчих

об'єктів, що передбачає відправку вимоги про видалення нелегального контенту з веб-ресурсу його власнику, а оператору зв'язку - про необхідність здійснити технічні заходи щодо закриття доступу до таких матеріалів. Вирішення питання правомірності зазначених дій покласти на українські суди.

Щодо СНД, Україна не є її членом, але залишається учасником ряду угод в рамках даної організації. Тому рекомендовано, для досягнення правової одноманітності та подолання прогалів у законодавстві прийняти одноманітний закон щодо відносини інтелектуальної власності в кіберсередовищі й впровадити особливу підвідомчість спорів про захист виняткових прав при використанні контенту у такому просторі арбітражним судам (досягненню зазначених цілей сприятиме створення Суду з інтелектуальних прав).

13.З'ясовано, що на міжнародному та регіональному рівнях функціонують організації, які займаються питаннями інтелектуальної власності, зокрема, і в аспекті кіберпростору, а саме: Всесвітня організація інтелектуальної власності, Корпорація з управління доменними іменами та IP-адресами, Товариство (Суспільство) Інтернету, Консорціум Всесвітньої павутини, Організація номерних ресурсів, Регіональні Інтернет-реєстри та інші. В рамках своєї діяльності, дані суб'єкти сприяють розвитку кіберпростору та захисту інтелектуальної власності у ньому, прагнуть до формування єдиних регулятивних підходів та протидії правопорушенням у відповідній сфері. Регламентація таких відносин на міжнародному рівні здійснюється з урахуванням положень "Інтернет-договорів" та інших угод, що адмініструються ВОІВ, на основі яких також проводиться розробка законодавства Євросоюзу та окремих країн, зокрема, України. Обґрунтовано застосування Політики вирішення доменних суперечок ICANN при вирішення відповідних, адже

відповідна процедура є недорогою та процедурно легкою. Також наголошено на важливості обговорення політик та технологій щодо сфери інтелектуальної власності та її взаємодії з Інтернетом на урядовому та міжнародному рівнях з метою уникнення випадків спекулювання «цифровим суверенітетом» і обмеження кібердомену географічними кордонами. Рекомендовано розробити стратегії створення збалансованого зв'язку між інтернет-платформами та режимами інтелектуальної власності, що потребує введення на глобальному рівні мінімальних уніфікованих стандартів у відповідній галузі.

14. Визначено, що євроінтеграційний вектор розвитку України зумовив зміни в національне законодавство, зокрема, у частині регулювання відносин права інтелектуальної власності як загалом, так і в кіберпросторі. Відповідно, було імплементовано положення директив та регламентів ЄС у вітчизняне законодавство, що відображено у нормах нового закону про авторське право і суміжні права 2022 року, а саме: Директиви 96/9/ЄС «Про правову охорону баз даних» 1996 р. - щодо отримання охорони правам особливого роду (*sui generis*); Директиви 2019/790 про авторське право і суміжні права на Єдиному цифровому ринку 2019 р. та про внесення змін до директив 96/9/ЄС та 2001/29/ЄС - щодо відповідальності провайдерів послуг обміну контентом за порушення авторських та суміжних прав тощо.

15. Визначено такі головні переваги нового Закону України про авторське право і суміжні права 2022 р.: введено поняття твору, музичного кліпу, сирітського твору, цифрового контенту ("електронна (цифрова) інформація"), інтерактивного надання доступу публіки до об'єкта авторського права та суміжних прав тощо; удосконалено концепти відеограми, фотографічного, службового та твору образотворчого мистецтва, бази даних, комп'ютерної

програми, відтворення та деяких інших; оновлено й конкретизовано випадки вільного використання об'єктів авторського права та суміжних прав, зокрема, щодо тимчасового вільного відтворення таких об'єктів; визначено оригінальність ключовим критерієм охороноздатності творіння; розширено перелік вірогідних творів-отримувачів правової охорони; введено положення щодо використання технологій штучного інтелекту, зокрема, щодо *sui generis* на неоригінальні об'єкти, згенеровані комп'ютерними програмами; розширено межі регулювання на електронну (цифрову) форму вираження твору; удосконалено інститут компенсації замість відшкодування збитків або стягнення доходу та порядок припинення відповідних порушень з використанням цифрових мереж (інтернету) тощо. Щодо особистих немайнових та майнових прав: оновлено підходи до визначення правопорушних дій щодо них; перелік немайнових авторських прав доповнено правом надавати результату творчості назву або взагалі залишити його без неї та правом творця присвятити твір певним особам, датам або подіям. Щодо матеріальних прав: додано норми про легальність лінкування та фреймінгу (за попередньої легальної доступності твору) та їх нелегальність (при наданні через них доступу до контенту, з обмежень правовласником); чітко встановлено право автора на справедливую винагороду (може перейти тільки до нащадків, не може бути передано іншим особам); заборонено зазначати предметом договору про передання майнових прав об'єкти і відповідні права, що в момент його укладення не існували; встановлено право вимагати додаткову пропорційну винагороду за використання (виконання) твору при її непропорційно низькому обсязі.

16. Визначено такі ключові недоліки нового Закону України про авторське право і суміжні права 2022 р.: у порівнянні із Законом про

авторське право 1993 р. - не було надано визначення поняттю «виключне право» та не зазначено, що концепт «суб'єкт авторського права» включає в себе «суб'єкт майнових авторських прав»; у порівнянні із Цивільним кодексом - створено колізію щодо розподілу майнових прав на створене за замовленням творіння, де права автоматично переходять до замовника по факту створення твору (за ЦКУ - вони належать сторонам договору спільно); інші недоліки - вичерпність переліку способів використання творів, що не відповідає сьогоденним інформаційно-технологічним реаліям через об'єктивну неможливість передбачити всі способи використання; зростання ризику зловживань при приватному копіюванні матеріалу (спосіб використання) через наявність формулювання "відтворення в особистих цілях особи...чи близьких знайомих такої сім'ї" без відповідного визначення таких "знайомих" тощо.

17. Окреслено коло перешкод та викликів на шляху ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі в різних країнах світу, а саме: неспроможність нормотворців вчасно відповідати на тренди цифрових трансформацій, які щоденно породжують нові типи інтелектуальної власності, зокрема, у кіберсередовищі; недостатність ефективності заходів кібернетичної безпеки, зокрема, викликане безперестанним збільшенням кількості й ускладненням якості кіберзагроз; неможливість забезпечити надійний транскордонний захист прав інтелектуальної власності через відсутність уніфікованого правового інструментарію; вигідне становище порушників відповідних прав у зв'язку із легкістю відтворення та розповсюдження контенту; нерегульованість правового забезпечення великих обсягів даних й часте порушенням їх конфіденційності; невстигання за змінами в управлінні правами інтелектуальної власності, викликані

використанням технологій блокчейну із їх децентралізованою архітектурою; недостатня урегульованість сфери смарт-контрактів тощо.

18. Обґрунтовано, на основі аналізу передових практик країн світу у галузі забезпечення дотримання права інтелектуальної власності у кіберпросторі, застосування багатогранного підходу, що передбачає правові, технологічні й соціальні рішення і взаємодію. Відповідно, при розробці засобів такого правового забезпечення та покращенні наявних політик в Україні, рекомендовано впровадити наступні позитивні практики провідних країн світу: за досвідом Сінгапуру - розробити та ввести в дію стратегію інтелектуальної власності строком на найближчі 10 років (це стимулюватиме активність творців та іноваторів й забезпечить підтримки бізнесу) й "програми прискорення" (це здешевить та полегшить патентну процедуру) та легалізувати й активно пропагувати реєстраційні й подібні дії щодо об'єктів інтелектуальної власності віддалено, через спеціалізовані мобільні та інші онлайн-інструменти; за досвідом Китаю - впровадити механізм балансування вигод при розподілі прибутку в технологічній інноваційній діяльності й налагодити співпрацю між різними відомствами задля недопущення інцидентів у сфері цифрових інтелектуально-правових порушення із посиленням контролю за правоохоронними органами; за досвідом європейських країн, США та інших суб'єктів міжнародного права - використовувати при розробці правових інструментів та механізмів загальноприйнятї юридичні практики (це сприятиме правовій одноманітності, і, відповідно, скорішому вирішенню спорів), підвищувати розуміння суспільства щодо необхідності реєструвати свої авторські права із одночасним спрощенням такої процедури, нормативно врегулювати питання захисту об'єктів цифрового мистецтва та криптомистецтва,

передбачити у законодавстві вимоги про хоча б мінімальну участь людини у створенні об'єктів інтелектуальної власності із залученням технологій штучного інтелекту, застосовувати уніфіковані стандарти захисту з метою недопущення різнорідного трактування положень та уникнення неоднозначності у їх практичному застосуванні, спростити судові процедури при розгляді відповідних спорів та де-факто почати роботу Вищого суду з питань інтелектуальної власності (так званого IP-суду). Окремо слід наголосити на важливості активної співпраці при розробці правових норм із експертами не лише в галузі юриспруденції, а й технологій, без чого неможливе всебічне врегулювання окремих аспектів цифрової інтелектуальної власності, а також на необхідності плідного міжнародного співробітництва, зокрема, у частині обміну практичним досвідом й спільної протидії транснаціональним порушенням.

19. Правовласникам, на основі аналізу дієвих світових практик, рекомендовано, з метою превентивного та об'ємного захисту своїх активів і відповідних прав, наступне: за досвідом В'єтнаму - впровадити в бізнес-стратегію захист інтелектуальної власності частиною бізнес-стратегії компанії; за досвідом Європи та Індії - завжди реєструвати свої авторські права (незалежно від надання їм автоматичної охорони по факту створення), використовувати цифрові платформи для реєстрації своїх прав, розробити й впровадити окремі стратегії захисту відповідних прав в контексті кібердомену (зокрема, з укладенням угод про конфіденційність та неконкуренцію), використовувати системи відстеження активів (зокрема, через використання технології блокчейну та штучного інтелекту), використовувати системи керування цифровими правами, укладати із користувачами ліцензійні угоди, застосовувати ватермарки та шифрування для захисту контенту; за досвідом США та деяких інших

країн - для програмного забезпечення використовувати поєднання методів реєстрації авторських прав, патентування та захисту комерційної таємниці, а також використовувати платформи безпечного обміну у випадку роботи із конфіденційними даними.

20. Запропоновано розуміти концептуальні засади побудови ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі як основоположне розуміння відповідної побудови ефективного правового забезпечення, сукупність поглядів на неї вчених та практиків, а також нормотворців, що втілюють відповідні ідеї та концепції у нормативно-правове регулювання щодо права інтелектуальної власності у кіберпросторі.

21. Запропоновано, з урахуванням наявних концепцій побудови ефективного правового забезпечення дотримання права інтелектуальної власності у кіберпросторі, будувати таке забезпечення в Україні шляхом: активної співпраці світової спільноти у пошуку регуляторних формул для вирішення наявних проблем у контексті зазначеного, зважаючи на незахищеність об'єктів інтелектуальної власності загальноприйнятими стандартами, що застосовуються до нецифрових (традиційних) творів; створення загальноновизнаної системи юрисдикції в кіберсередовищі через плідну міжнародну взаємодію, гармонізацію законів та інноваційних підходів; подолання проблеми екстериторіального охоплення та втамування потреби в гармонізації між юрисдикціями (з основою на нормах Каліфорнійського закону про конфіденційність споживачів та Загального регламенту про захист даних); зазначення у відповідних нормативно-правових актах про віднесення справ з цифрового порушення прав інтелектуальної власності, вчиненого представниками іншої країни, судам своєї держави; подолання технологічної необізнаності, зокрема, серед правоохоронних органів

щодо цифрових порушень та особливостей протидії їм; надання правового захисту технологічним методам охорони прав авторів та правовласників та введення в дію жорстких положень щодо відповідальності за обхід технологічних заходів (з основою на приписах Інтернет-договорах ВОІВ); забезпечення виконання правових заходів для зберігання даних і записів про використання Інтернет-мережі шляхом введення журналів і реєстрів для її використання, що мають вчинятися постачальниками інтернет-послуг протягом розумного строку задля надання допомоги у відстеженні IP-адрес порушників; розробки й нормативного закріплення положень щодо нового розширеного режиму обміну файлами і посилення відповідальності онлайн-посередників; впровадження програм громадської освіти серед інтернет-користувачів із їх інформуванням про можливі правопорушні дії та засоби самостійного захисту від відповідних порушень в кіберпросторі.

22. Основні наукові результати, отримані в процесі порівняльного аналізу законодавства у сфері забезпечення дотримання права інтелектуальної власності у кіберпросторі, дають підстави запропонувати такі практичні рекомендації на міжнародному рівні як розробка та впровадження в дію:

- a. універсального міжнародно-правового акту (конвенції), що б урегулював проблему транскордонності Всесвітньої мережі інтернет як сегменту кіберпростору й цифрового простору загалом, зокрема, шляхом співпраці світового співтовариства. Його основна мета - досягнення глобальної правової одноманітності. Таке є надважливим, адже розрізненість законодавств нерідко сприяє порушенням в галузі права інтелектуальної власності у кібернетичному середовищі,

наприклад, коли діяння є караним в одній правовій системі і не містить складу правопорушення - в іншій. Вагомість прийняття вказаного документу проявляється і в тому, що через територіальність прав інтелектуальної власності, у законодавстві різних країн є й різні вимоги та правила щодо захисту майнових та немайнових прав, термінів охорони, особливостей реєстрації тощо. Проблемність вказаної характеристики розповсюджується й на роль та відповідальність онлайн-посередників (провайдери, реєстратори доменних імен, надавачі інтернет-послуг, провайдери тощо). Запропонований нормативний документ має, окрім положень щодо юрисдикції, також вміщувати і положення щодо відповідальності та покарання порушників. Вимогою до його розробки є основа на загальновизнаних міжнародно-правових актах та стандартах (основними з них є Закон про захист авторських прав у цифрову епоху, Директива ЄС про авторське право, інтернет-договори ВОІВ та інші).

- b. типового (модельного) закону про захист цифрової інтелектуальної власності, з урахуванням відмінності відповідних об'єктів від традиційних об'єктів інтелектуальної власності.
- c. уніфікованих правил з протидії кібер-правопорушенням у сфері інтелектуальної власності в Інтернеті та інших глобальних інформаційно-комунікаційних мережах, задля своєчасного попередження викликів та реагуванні на інциденти у відповідній галузі, зокрема зловживання інформаційними технологіями, що віднесені до об'єктів інтелектуальної власності. Нині такі незаконні активності часто залишаються безкарними, адже відповідні порушники постійно підвищують

свій рівень навичок та знань, винаходять нові методики й інструменти для скоєння неправомірних дій, чим створюють загрози безпеці персональних комп'ютерів фізичних та юридичних осіб і навіть держав. Окремо в такому документі слід передбачити процедури реагування на відповідні події та знешкодження порушників.

До розробки зазначених документів слід залучити не лише юристів, але й представників основних міжнародних суб'єктів, чия діяльність пов'язана із функціонуванням кіберпростору та, зокрема, Інтернету, а також висококваліфікованих технічних спеціалістів з даної сфери й органи забезпечення міжнародного правопорядку (зокрема, Інтерпол).

23. Головні результати, отримані в процесі порівняльного аналізу законодавства у сфері забезпечення дотримання права інтелектуальної власності у кіберпросторі, дають підстави запропонувати такі практичні рекомендації щодо імплементації позитивного зарубіжного досвіду у вітчизняне законодавство:

- a. прийняти Інформаційний Кодекс України, що складатиметься із двох традиційних частин - Загальної та Особливої, де:
 - i. в Загальній частині - буде надано визначення правового статусу та становища інформаційних ресурсів з урахуванням права власності на них, а також рівнів захисту та доступу до інформації; буде надано чіткий перелік прав й обов'язків інформаційних суб'єктів; буде врегульовано питання інформаційного забезпечення органів державної влади;
 - ii. в Особливій частині - буде включено Розділ, присвячений правовому регулюванню інтелектуальної власності, зокрема, у інформаційно-комунікаційних мережах.

Зокрема, відповідний Розділ має вміщувати норми щодо юрисдикції у питаннях спорів з цифрової інтелектуальної власності, а також щодо відповідальності порушників та окремо онлайн-посередників;

- b. доповнити (у разі неможливості прийняття Інформаційного кодексу України) існуючі нормативно-правові акти, що регулюють інформаційну сферу і безпосередньо кіберпростір положеннями про права і обов'язків інформаційних суб'єктів, про інформаційне забезпечення органів державної влади, а також визначенням правового статусу інформаційних ресурсів з урахуванням права власності, рівнів захисту, доступу до інформації та визначенням суб'єктів правопорушення щодо інтелектуальної власності у кібердоміні, з метою чіткого розуміння щодо визначення відповідних осіб;
- c. внести такі зміни до Закону України про авторське право і суміжні права 2022 р.:
 - i. з метою забезпечення ефективного захисту прав та законних інтересів правовласників відповідних об'єктів - доповнити Статтю 1 визначенням терміну *"цифрова інтелектуальна власність"* як *інтелектуальна власність у цифровому форматі*;
 - ii. з метою забезпечення ефективного захисту прав та законних інтересів правовласників відповідних об'єктів - повернути в Статтю 1 визначення терміну «виключне право» (як це зроблено в Законі України про авторське право та суміжні права 1993 р.);
 - iii. з метою забезпечення ефективного захисту прав та законних інтересів правовласників відповідних об'єктів - у ч. 2 Статті 5 зазначити, що до кола суб'єктів

авторського права включено й суб'єктів майнових авторських прав;

- iv. з метою забезпечення ефективного захисту прав та законних інтересів правовласників відповідних об'єктів та уникнення зловживань правами - доповнити п. 39 Статті 1 про приватне копіювання роз'ясненням, яких саме осіб віднесено до "...близьких знайомих такої сім'ї...";
- v. з метою забезпечення ефективного захисту прав та законних інтересів правовласників й інтересів третіх осіб - до ч. 1 Статті 12 внести зміни, відповідно до яких перелік способів використання творів **не є вичерпним** (адже у зв'язку із безперестанним розвитком кіберпростору не можливо практично передбачити всі можливі способи відповідного використання).
- vi. з метою забезпечення освітнього процесу - викласти п. 2 ч. 2 Статті 22: у такій редакції: "...відтворення в електронній (цифровій) формі, інтерактивне надання доступу до правомірно оприлюднених статей та інших невеликих за обсягом творів, *художніх творів*, а також уривків з письмових творів як ілюстрацій для дистанційного навчання..." (це дозволить вільно використовувати в навчальній діяльності малюнки, фотографії тощо для більш якісного ілюстрування навчального матеріалу);
- vii. з метою забезпечення освітнього процесу - доповнити п. 2 ч. 2 Статті 22 у частині переліку суб'єктів вільного відтворення, у тому числі в електронній (цифровій) формі, таким суб'єктом як видавництво (адже саме вони

друкують хрестоматії й подібні посібні матеріали, що використовуються з навчальною метою).

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авторське право в Узбекистані. Wikipedia. URL: https://ru.wikipedia.org/wiki/Авторское_право_в_Узбекистане (дата звернення: 11.06.2024).
2. Актуальні проблем теорії держави та права (Лекції). Studies. URL: <http://studies.in.ua/aktualn-problemi-teoryi-derzhavi-ta-prava> (дата звернення: 05.06.2024).
3. Архіпова Є. О. Соціальна складова інформаційної безпеки. Безпека інформації: Наук.-практ. журнал. 2012. Т. 18, № 2. С. 28–32.
4. Базилевич В. Д. Інтелектуальна власність : підручник. 3-тє вид. переробл. і доповн Київ : Знання, 2014. 671 с.
5. Бондаренко С. Авторське право та суміжні права : курс лекцій. Київ : Ін-т інтел. власн. і права, 2008. 288 с. URL: https://uu.edu.ua/upload/Osvita/Navch_metod_d_t/Navch_metod_materiali/Pravoznavstvo/Bondarenko_Avtorske_pravo_i_sumizhni_prava.pdf (дата звернення: 11.06.2024).
6. Бонч-Бруєвич Г., Носенко Т. Організація та обробка електронної інформації : навч. посіб. Київ : Ун-т ім. Б.Грінченка, ін-т сусп-ва, каф. інформатики, 2013. 108 с.
7. Вірченко В. В., Філюк Г. М., В. В. Вірченко. Архітектоніка та функції інтелектуальної власності в постіндустріальній економіці. Ефективна економіка. 2022. № 1. URL: <https://doi.org/10.32702/2307-2105-2022.1.14> (дата звернення: 07.06.2024).
8. Віхров О.П., Віхрова І.О. Теорія держави і права: курс лекцій: навчальний посібник. Чернігів: Десна Поліграф. 2015. 304 с.
9. Воронкова В.Г., Нікітенко В.О. Цифрова стратегія промислового підприємства : Науково-методичний посібник для здобувачів вищої освіти ступеня доктора філософії у галузі знань 07 «Управління та

адміністрування» спеціальності 073 «Менеджмент». Запорізький національний університет, 2023. 160 с.

10. Всесвітня організація інтелектуальної власності (1967), Стокгольмська конвенція про заснування Всесвітньої організації інтелектуальної власності. URL: http://www.wipo.int/treaties/ru/text.jsp?file_id=283807 (дата звернення: 13.09.2022).
11. Гарна С., Шнурко А., Дронов І. М. Інтелектуальна власність як складова нематеріальних активів підприємства. Інноваційна економіка. 2018. Т. 5-6. С. 126–130. URL: <http://inneco.org/index.php/inneco.ua/article/view/304/366> (дата звернення: 07.06.2024).
12. Гончаренко Д. Інтелектуальна власність у мережі Інтернет. Хостпро. URL: <https://hostpro.ua/blog/ua/intellectual-property> (дата звернення: 08.05.2023).
13. Горовий В. Національні інформаційні ресурси в контексті посилення глобальних інформаційних впливів. Україна: події, факти, коментарі. 2013. № 12. С. 59–72.
14. Григор'єва В.А. Концептуальні засади управління розвитком професійно-технічної освіти. Управління розвитком професійно-технічної освіти в сучасних умовах: теорія і практика: монографія. 2014. С. 167-202. URL: https://lib.iitta.gov.ua/9230/1/%D0%93%D1%80%D0%B8%D0%B3%D0%BE%D1%80%D1%8C%D1%8D%D0%B2%D0%B0_2.pdf (дата звернення: 06.05.2024).
15. Грузіна І. А. Вплив інформаційного середовища на діяльність сучасного підприємства. Електронний архів Харківського національного економічного університету. URL: <http://repository.hneu.edu.ua/jspui/bitstream/123456789/7834/1/Влияние>

%20информационной%20среды%20на%20деятельность%20современного%20предприятия.pdf (дата звернення: 11.06.2024).

16. Деякі питання електронної взаємодії державних електронних інформаційних ресурсів : Постанова Каб. Міністрів України від 08.09.2016 р. № 606 : станом на 23 груд. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/606-2016-п#Text> (дата звернення: 11.06.2024).
17. Деякі питання Національного органу інтелектуальної власності : Розпорядж. Каб. Міністрів України від 28.10.2022 р. № 943-р. URL: <https://zakon.rada.gov.ua/laws/show/943-2022-р#Text> (дата звернення: 15.05.2024).
18. Дзвонів Г.Р., Махонько Н.І. 1.2. Структура правовідносини. Медичне право: навчальний посібник. 2009. URL: <http://yport.inf.ua/meditsinskoe-pravo-uchebnoe.html>
19. Директива Європейського Парламенту і Ради (ЄС) 2018/1972 від 11 грудня 2018 року про запровадження Європейського кодексу електронних комунікацій : Директива Європ. Союзу від 11.12.2018 р. № 2018/1972. URL: https://zakon.rada.gov.ua/laws/show/984_013-18#Text (дата звернення: 11.06.2024).
20. Дніпров О. Концептуальні засади діяльності органів виконавчої влади в Україні. Вісник АПСВТ. 2020. № 3-4. С. 35–40. URL: https://www.socosvita.kiev.ua/sites/default/files/Visnyk_3-4_2020-35-40.pdf (дата звернення: 06.05.2024).
21. Довгань Г. В. Становлення та розвиток законодавства України про інтелектуальну власність (історико-правовий аспект) : дис. ... канд. юрид. наук : 12.00.01. Львів, 2009. 290 с.
22. Договір Всесвітньої організації інтелектуальної власності про авторське право, прийнятий Дипломатичною конференцією 20 грудня 1996 року : Договір Всесвіт. орг. інтелект. власності від

- 20.12.1996 р. : станом на 20 верес. 2001 р. URL: https://zakon.rada.gov.ua/laws/show/995_770#Text (дата звернення: 11.06.2024).
23. Договір Всесвітньої організації інтелектуальної власності про виконання і фонограми, прийнятий Дипломатичною конференцією 20 грудня 1996 року : Договір Всесвіт. орг. інтелект. власності від 20.12.1996 р. : станом на 20 верес. 2001 р. URL: https://zakon.rada.gov.ua/laws/show/995_769#Text (дата звернення: 11.06.2024).
24. Дубняк К. А. Інформаційний простір: структура та функціональні параметри. Держава та регіони. Серія: Соціальні комунікації. 2015. Т. 4, № 24. С. 21–25. URL: http://umo.edu.ua/images/content/aspirantura/zabezp_discipl/Інформац.%20простір.pdf (дата звернення: 08.06.2022).
25. Дубов Д., Ожеван М. Кібербезпека: світові тенденції та виклики для України : аналіт. доп. Київ: НІСД, 2011. 30 с.
26. Дяченко Н. П. Дотримання прав інтелектуальної власності як чинник формування передумов зростання суспільної довіри. Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру (з нагоди 30-річчя проголошення незалежності України та 25-річчя прийняття Конституції України) : у 2 т. : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 21 трав. 2021 р.) / за загальною редакцією С. В. Ківалова. Одеса : Видавничий дім «Гельветика», 2021. Т. 2. С. 510-512.
27. Еннан Р. Є. Правове регулювання відносин інтелектуальної власності у Європейському Союзі : автореф. дис. ... канд. юрид. наук : 12.00.09. Одеса. 2010. 20 с.

- 28.Еннан Р. Поняття, ознаки, сутність, специфіка та види відносин у мережі Інтернет. Теорія і практика інтелектуальної власності. 2013. №3. С. 10-19.
- 29.Єфремова К. В. Правова природа Інтернет-правовідносин. Правове регулювання відносин у мережі Інтернет : монографія / ред.: С. В. Глібко, К. В. Єфремова. Харків, 2016. С. 8-22. URL: https://ndipzir.org.ua/wp-content/uploads/2017/07/Yefremova/1_1.pdf (дата звернення: 06.10.2022).
- 30.Єфремова К.В. До перспектив правового регулювання інтернет-правовідносин: господарсько-правовий аспект. Право та інноваційне суспільство. 2014. № 1. С. 5-11. URL: http://nbuv.gov.ua/j-pdf/pric_2014_1_3.pdf (дата звернення: 13.09.2022).
- 31.Жидкова О. О. Проблеми взаємодії людини та інформаційного середовища. Вісн. Харк. нац. ун-ту ім. В. Н. Каразіна. 2010. № 888. С. 58-62.
- 32.Жуковський А., Субтельний О. Нарис історії України. Львів : Вид-во Наук. т-ва ім. Т. Шевченка у Львові, 1991. 230 с.
- 33.Загальна декларація прав людини: ООН; Декларація, Міжнародний документ від 10.12.1948. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text
- 34.Закон Республіки Вірменія про авторське право та суміжні права. Armenian legal information system. URL: <https://www.arlis.am/DocumentView.aspx?docid=173423> (дата звернення: 12.06.2024).
- 35.Зеров. К. Авторське право в Україні з 01.01.2023 року: про нові правила розповів адвокат Костянтин Зеров. Advokat Post. 2023. URL: <https://advokatpost.com/avtorske-pravo-v-ukraini-z-01-01-2023-roku-pro-novi-pravylya-rozpoviv-advokat-kostiantyn-zerov/> (дата звернення: 09.01.2024).

36. Інформаційний простір. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Інформаційний_простір (дата звернення: 11.06.2024).
37. Історія розвитку Інтернету. EServer. 2018. URL: <https://e-server.com.ua/sovety/240-istoriya-razvitiya-interneta> (дата звернення: 02.03.2023).
38. Касимбекова В. Інтелектуальна власність у Таджикистані: Хто та як її захищає?. Новини Таджикистану ASIA-Plus. URL: <https://www.asiaplustj.info/ru/news/tajikistan/20200426/intellektualnaya-sobstvennost-v-tadzhikistane-kto-i-kak-ee-zatshitshaet> (дата звернення: 11.06.2024).
39. Керування іменами та адресами в Інтернеті. WIPO - World Intellectual Property Organization. URL: <https://www.wipo.int/amc/ru/processes/process1/report/summary.html> (дата звернення: 11.06.2024).
40. Клевець О. Чим цифровізація відрізняється від автоматизації. Фінансова академія Актив. 2021. URL: <https://finacademy.net/materials/article/cifrovizaciya-i-avtomatizaciya> (дата звернення: 11.06.2024).
41. Комітет з питань цифрової трансформації закликає брати цифрову зброю. Комітет з питань цифрової трансформації. 2022. URL: http://komit.rada.gov.ua/news/main_news/74168.html (дата звернення: 16.03.2022).
42. Конвенція про заснування Всесвітньої Організації Інтелектуальної Власності: Конвенція від 14.07.1967. URL: https://ips.ligazakon.net/document/view/MU67K05U?ed=1967_07_14
43. Коноваленко В. Про умови ілюстрування навчальних видань за новим законом про авторське право - Юридична газета – онлайн версія. URL: <https://yur-gazeta.com/publications/practice/zahist-intelektualnoyi->

- vlasnosti-avtorske-pravo/pro-umovi-ilyustruvannya-navchalnih-vidan-zanovim-zakonom-pro-avtorske-pravo.html (дата звернення: 09.01.2024).
44. Конспект лекцій з курсу “інтелектуальна власність” для спеціалістів 7.091701, 7.091702, 7.091704, 7.091706, 7.091707, 7.091708, 7.091709, 7.091711, 7.070801, 7.050106, 7.050107 магістрів 8.091701, 8.091702, 8.091704, 8.091706, 8.091707, 8.091708, 8.091709, 8.091711, 8.070801, 8.050106, 8.050107 / уклад.: О. Соколов, О. Данилова. Одеса : ОНАХТ, 2006. 34 с.
45. Конституція України: Конституція, Закон від 28.06.1996 № 254к/96-ВР. Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141.
46. Концепція інформаційної безпеки України: проект. Organization for Security and Co-operation in Europe (OSCE). 2015. 14 с. URL: <https://www.osce.org/files/f/documents/0/2/175056.pdf> (дата звернення: 11.06.2024).
47. Корецкий В. М. "Общие принципы права" в международном праве. Киев : АН УССР, 1957. 52 с.
48. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України : дис. ... д-ра юрид. наук : 12.00.07. Харків, 2004. 427 с.
49. Крайнев П.П. Інтелектуальна економіка: управління промисловою власністю : монографія. Київ : Видавничий дім «Ін Юре». 2004. 448 с.
50. Крижна В.М., Яркіна Н.Є. Право інтелектуальної власності України: Конспект лекцій. Харків: Нац. юрид. акад. України, 2008. 112 с. URL: http://web.kpi.kharkov.ua/acem/wp-content/uploads/sites/16/2017/06/IV_nav_case_1.pdf
51. Маркевич К. Цифровізація: переваги та шляхи подолання викликів. Центр Разумкова. 2021. URL: <https://razumkov.org.ua/statti/tsyfrovizatsiia-perevagy-ta-shliakhy-podolannia-vyukykyv> (дата звернення: 11.06.2024).

52. Мисенко О. Компенсація за порушення авторського права у новому законі. Блоги про бізнес, політику, юридичну систему - LIGA.net. URL: <https://blog.liga.net/user/amyisenko/article/50264> (дата звернення: 09.01.2024).
53. Мисенко О. Новий закон про авторське право: основні новели. Блоги про бізнес, політику, юридичну систему - LIGA.net. URL: <https://blog.liga.net/user/amyisenko/article/48757> (дата звернення: 09.01.2024).
54. Міжнародний пакт про громадянські і політичні права: ООН; Пакт, Міжнародний документ від 16.12.1966. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text
55. Молодковець М. Майнові права на код та AI-об'єкти. Головні зміни в новому законі про авторське право. DOU.ua. URL: <https://dou.ua/lenta/articles/new-copyright-law/> (дата звернення: 19.09.2023).
56. Недбайло П. Е. Применение советских правовых норм. Москва : Госюриздат, 1960. 512 с.
57. Окінавська хартія глобального інформаційного суспільства: Хартія, Міжнародний документ від 22.07.2000 № 998_163. URL: https://zakon.rada.gov.ua/laws/show/998_163#Text
58. ООН: 4,1 мільярда людей у світі підключені до інтернету. Радіо Свобода. URL: <https://www.radiosvoboda.org/a/news-oon-internet/30254946.html>
59. Петрів М.В. Кіберсквотинг як вид недобросовісної конкуренції. Матеріали науково-практична конференція «Актуальні проблеми інтелектуального, інформаційного та ІТ права» м. Львів, 17-18 травня 2019 р. С.125-127.
60. Питання Міністерства цифрової трансформації : Постанова Каб. Міністрів України від 18.09.2019 р. № 856 : станом на 1 черв. 2024 р.

URL: <https://zakon.rada.gov.ua/laws/show/856-2019-п#Text> (дата звернення: 11.06.2024).

61. Піжук О. І. Цифровізація як зміна парадигми розвитку економічних систем. Науковий вісник Ужгородського університету. Науковий вісник Ужгородського університету. Серія «Економіка». 2018. № 2(52). С. 84–91. URL: [https://doi.org/10.24144/2409-6857.2018.2\(52\).84-91](https://doi.org/10.24144/2409-6857.2018.2(52).84-91) (дата звернення: 11.06.2024).

62. Повідомлення про контент у Google - Юридична інформація Довідка. Google Help. URL: <https://support.google.com/legal/troubleshooter/1114905?hl=uk> (дата звернення: 15.05.2024).

63. Порівняльна таблиця до проекту Закону України про авторське право і суміжні права (Реєстраційний № 5552-1) / Р. О. Стефанчук та ін. Київ : Апарат Верхов. Ради України, 2022. 563 с. URL: <https://itd.rada.gov.ua/billInfo/Bills/pubFile/1562981> (дата звернення: 01.01.2024).

64. Постанова Вищого господарського суду України від 19.08.2014 р. у справі № 918/5/14. URL: <https://reyestr.court.gov.ua/Review/40203032> (дата звернення: 08.08.2023).

65. Про авторське право – за новим законодавством: що треба знати медійникам? Платформа прав людини. URL: <https://ppl.org.ua/pro-avtorske-pravo-za-novim-zakonodavstvom-shho-treba-znati-medijnikam.html> (дата звернення: 29.03.2024).

66. Про авторське право і суміжні права : Закон України від 01.12.2022 р. № 2811-IX : станом на 15 квіт. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/2811-20#Text> (дата звернення: 09.01.2024).

67. Про авторське право і суміжні права : Закон України від 23.12.1993 р. № 3792-XII : станом на 1 січ. 2023 р. URL:

<https://zakon.rada.gov.ua/laws/show/3792-12#Text> (дата звернення: 09.01.2024).

68. Про авторське право та суміжні права : Закон Республіки Казахстан від 10.06.1996 р. № 6. Відомості Парламенту РК. 1996. № 8-9. Ст. 237.

69. Про авторське право та суміжні права : Закон Республіки Молдова від 02.07.2010 р №193. Monitorul Oficial Nr. 191-193. 2010. Ст. № 630.

70. Про авторські та суміжні права : Закон Грузії від 22.06.1999 р. Законодавчий Вісник Грузії-ЗВГ, 28(35), 08/07/1999. URL: <https://matsne.gov.ge/ru/document/view/16198?publication=15> (дата звернення: 11.06.2024).

71. Про внесення змін і доповнень до деяких законодавчих актів Республіки Казахстан з питань інтелектуальної власності : Закон Республіки Казахстан від 12.01.2012 р. № 537-IV. Казахстанська правда, 2012, № 23-24.

72. Про електронні довірчі послуги : Закон України від 05.10.2017 р. № 2155-VIII : станом на 1 січ. 2024 р. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text> (дата звернення: 11.06.2024).

73. Про забезпечення прав інтелектуальної власності та боротьбу з піратством : Закон Азербайдж. Респ. від 22.05.2012 р. URL: <https://www.wipo.int/wipolex/ru/text/317291> (дата звернення: 11.06.2024).

74. Про затвердження плану заходів з реалізації Концепції реформування державної системи правової охорони інтелектуальної власності в Україні : Розпорядж. Каб. Міністрів України від 23.08.2016 р. № 632-р. URL: <https://zakon.rada.gov.ua/laws/show/632-2016-p#Text> (дата звернення: 06.05.2024).

75. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 27 квіт. 2024 р. URL:

<https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 11.06.2024).

76. Про інформацію: Закон України від 02.10.1992 № 2657-ХІІ. Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650.
77. Про Національний орган інтелектуальної власності : Розпорядж. Каб. Міністрів України від 13.10.2020 р. № 1267-р : станом на 8 листоп. 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/1267-2020-p#Text> (дата звернення: 15.05.2024).
78. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. Відомості Верховної Ради (ВВР), 2018, № 31, ст.241.
79. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. Відомості Верховної Ради (ВВР), 2017, № 45, ст.403.
80. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 09.01.2007 № 537-V. Відомості Верховної Ради України (ВВР), 2007, № 12, ст.102.
81. Про охорону прав на винаходи і корисні моделі: Закон України від 15.12.1993 № 3687-ХІІ. Відомості Верховної Ради України (ВВР), 1994, № 7, ст. 32.
82. Про охорону прав на знаки для товарів і послуг: Закон України від 15.12.1993 № 3689-ХІІ. Відомості Верховної Ради України (ВВР), 1994, № 7, ст. 36.
83. Про охорону прав на промислові зразки: Закон України від 15.12.1993 № 3688-ХІІ. Відомості Верховної Ради України (ВВР), 1994, № 7, ст. 34).
84. Про перелік, кількісний склад і предмети відання комітетів Верховної Ради України дев'ятого скликання : Постанова Верхов. Ради України від 29.08.2019 р. № 19-IX : станом на 23 лют. 2023 р. URL:

<https://zakon.rada.gov.ua/laws/show/19-20#Text> (дата звернення: 11.06.2024).

85. Про План реалізації Стратегії кібербезпеки України : Рішення Ради нац. безпеки і оборони України від 30.12.2021 р. : станом на 3 лют. 2022 р. URL: <https://zakon.rada.gov.ua/laws/show/n0087525-21#Text> (дата звернення: 11.06.2024).

86. Про Регламент Верховної Ради України: Закон України; Регламент від 10.02.2010 № 1861-VI. URL: <https://zakon.rada.gov.ua/laws/show/1861-17/conv#n766> (дата звернення: 09.01.2024).

87. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" : Указ Президента України від 26.08.2021 р. № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text> (дата звернення: 11.06.2024).

88. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки" : Указ Президента України від 28.12.2021 р. № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text> (дата звернення: 11.06.2024).

89. Про схвалення Концепції реформування державної системи правової охорони інтелектуальної власності в Україні : Розпорядж. Каб. Міністрів України від 01.06.2016 р. № 402-р. URL: <https://zakon.rada.gov.ua/laws/show/402-2016-p#Text> (дата звернення: 06.05.2024).

90. Проблемні питання визначення правової природи і структури правовідносин інтелектуальної власності, що виникають у мережі Інтернет / О. І. Харитонова та ін. Наукові праці Національного університету «Одеська юридична академія» / ред. М. В. Афанасьєва.

- Одеса, 2015. С. 159–200. URL: <https://dspace.onua.edu.ua/server/api/core/bitstreams/52103c22-613c-495e-816e-698b9a9f5f76/content> (дата звернення: 14.06.2023).
91. Проект Закону про Національну програму інформатизації № 6241 від 01.11.2021. Верховна Рада України. 2021. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?id=&pf3511=73095 (дата звернення: 16.03.2022).
92. Проскуріна О. Інформаційна стратегія України в сучасному геополітичному просторі. Політичний менеджмент. 2009. № 3. С. 137–144. URL: https://ipiend.gov.ua/wp-content/uploads/2018/07/proskurina_informatsina.pdf (дата звернення: 11.06.2024).
93. Рабінович П.М. Основи загальної теорії права та держави. Київ: Атіка, 2001. 176 с.
94. Регулювання прав інтелектуальної власності в Інтернеті у Киргизькій Республіці. Право та ЗМІ Центральної Азії. 2012. URL: <https://medialaw.asia/posts/20-03-2012/55287.html> (дата звернення: 11.06.2024).
95. Світличний О. П. Право інтелектуальної власності : підручник. 2-ге вид. Київ : НУБіП України, 2016. 355 с.
96. Скакун О. Ф. Теорія держави і права : Підруч. Харків : Консум, 2001. 664 с.
97. Скакун О.Ф. Теорія держави і права. Харків: Консум. 2001. – 656 с.
98. Словник української мови: в 11 томах / ред. І. Білодід ; уклад. Інститут мовознавства АН УРСР. Т. 2, Київ : Наук. думка, 1971. URL: <http://sum.in.ua/s/dijaljnistj> (дата звернення: 09.01.2024)
99. Словник української мови: в 11 томах / ред. І. Білодід ; уклад. Інститут мовознавства АН УРСР. Т. 7, Київ : Наук. думка, 1976. URL: <http://sum.in.ua/s/prascja> (дата звернення: 09.01.2024).

100. Словник української мови: в 11 томах. Київ : Наукова думка. Т. 2. 1971. — С. 49.
101. Сопілко І. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. Scientific works of National Aviation University. Series: Law Journal "Air and Space Law". 2021. Т. 2, № 59. С. 110–115. URL: <https://doi.org/10.18372/2307-9061.59.15603> (дата звернення: 11.06.2024).
102. Сопілко І.М., Пономаренко О. В. Особливості охорони об'єктів авторського права за законодавством України. Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право». 2013. Т. 1, № 26. С. 109–113. URL: <https://doi.org/10.18372/2307-9061.26.4812>.
103. Стратегія дій за п'ятьма пріоритетними напрямками розвитку Республіки Узбекистан у 2017 – 2021 роках : Стратегія від 07.02.2017 р. URL: <https://lex.uz/ru/docs/3107042#3109624> (дата звернення: 11.06.2024).
104. Структура (склад) правових відносин. Донецький національний університет. StudFiles. URL: <https://studfile.net/preview/3009022/page:16/> (дата звернення: 07.06.2024).
105. Тема 9. Правові відносини. Мультимедійний посібник «Теорія держави та права». Національна академія внутрішніх справ. 2016. URL: https://arm.naiaiu.kiev.ua/books/tdp-new/info/lection/lec9/tema9_4.html (дата звернення: 07.06.2024).
106. Теорія держави і права : посіб. для підготовки до держ. іспитів / ТЗЗ за заг. ред. О. В. Петришина. - Харків: Право, 2012. 192 с.
107. Троцюк Н.В., Кудзіновський А.С. Відповідальність інтернет-посередників за порушення авторських прав. Наукові праці

Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право». 2017. № 3 (44). С. 103–107.

108. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони : Угода Україна від 27.06.2014 р. : станом на 30 листоп. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text (дата звернення: 09.01.2024).
109. Українська людина в європейському світі : навч. посіб. / ред.: Т. С. Смовженко, З. Е. Скринник. Київ : УБС НБУ, 2015. 609 с.
110. Україну внесли до списку країн-порушників інтелектуальної власності. Укрінформ. URL: <https://www.ukrinform.ua/rubric-economy/2852491-ukrainu-vnesli-do-spisku-krainporusnikiv-intelektualnoi-vlasnosti.html> (дата звернення: 07.06.2024).
111. Філінович В. В. Веб-сайт як особливий об'єкт права інтелектуальної власності : дис. ... канд. юрид. наук : 12.00.03. Київ, 2015. 225 с.
112. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. Інформація і право. 2012. № 2. С. 162–169. URL: http://nbuv.gov.ua/UJRN/Infpr_2012_2_24 (дата звернення: 05.06.2024).
113. Харитонова О. І. Відносини та правовідносини інтелектуальної власності: проблеми співвідношення. Від римського приватного права до ІТ права : матеріали міжнар. наук.-практич. конф. «Рим. право і сучасність», м. Одеса, 19 трав. 2018 р. Одеса: Фенікс, 2018. С. 85–90.
114. Харитонова О. І. Суб'єкти та об'єкти правовідносин інтелектуальної власності. Актуальні проблеми держави і права. 2011.

- Т. 59. С. 329–335. URL: <http://www.apdp.in.ua/v59/44.pdf> (дата звернення: 12.02.2023).
115. Центральний державний архів вищих органів влади та управління України, ф. 9, оп. 1, спр. 217.
116. Цивільний кодекс України: Кодекс України; Закон, Кодекс від 16.01.2003 № 435-IV. Відомості Верховної Ради України (ВВР), 2003, №№ 40-44, ст.356.
117. Цифрова держава. Дія. 2022. URL: <https://plan2.diia.gov.ua> (дата звернення: 16.03.2022).
118. Цифрова трансформація. Вікіпедія. URL: https://ru.wikipedia.org/wiki/Цифровая_трансформация (дата звернення: 11.06.2024).
119. Цифровізація. Вікісловник. URL: <https://ru.wiktionary.org/wiki/цифровизация> (дата звернення: 11.06.2024).
120. Чередніченко Н. Цифровізація державного управління. Конференції Державного університету «Житомирська політехніка». URL: <https://conf.ztu.edu.ua/wp-content/uploads/2021/01/354.pdf> (дата звернення: 11.06.2024).
121. Шпак Н.О., Найчук-Хрущ М.Б., Гавецька В.М. Проблематика дотримання прав інтелектуальної власності у медіа-просторі. Менеджмент та підприємництво в Україні: етапи становлення та проблеми розвитку. 2021; Вип. 3, № 2: С. 256-271.
122. Штефан О. Цивільно-правові способи захисту авторського права і суміжних прав: новації законодавства. Теорія і практика інтелектуальної власності. 2023. № 1-2. С. 64–74.
123. Шуба В. В. Адміністративно-правові відносини в діяльності органів прокуратури України: загальнотеоретичні аспекти : дис. ... канд. юрид. наук : 12.00.07. Харків, 2007. 200 с. URL:

<http://mego.info/матеріал/21-субєкти-адміністративно-правових-відносин?page=2> (дата звернення: 07.06.2024).

124. Що таке інформаційний простір і чому це важливо в журналістиці. Professional journalism. URL: <http://projournalism.in.ua/shcho-take-informatsijniy-prostir-i-chomu-tse-vagливо-v-journalistitsi/> (дата звернення: 26.04.2022).
125. Яременко О. Кіберпростір як складова інформаційної сфери: проблема правової інституалізації. Кібербезпека в Україні: правові та організаційні питання: : матеріали міжн. наук. практ. конф, м. Одеса, 26 листоп. 2020 р. Одеса, 2021. С. 194–195. URL: <https://dspace.oduvs.edu.ua/server/api/core/bitstreams/2fee92c0-8800-45e1-9c5e-08ac995cf723/content?authentication-token=eyJhbGciOiJIUzI1NiJ9.eyJlaWQiOiJjZmMwZGYxYi04NDlhLTQxNmUtODQ3YS00Y2RmOGNhZDAwYTYiLCJzZyI6W10sImF1dGhlbnRpY2F0aW9uTWV0aG9kIjoicGFzc3dvcmQiLCJleHAiOjE3MTgxMDU5Mzl9.7c-Snpzq3QB-ilweYA1aOt3R8yOn9tKyxCcX6yPyfJA> (дата звернення: 11.06.2024).
126. About CCIPS. Department of Justice | Homepage | United States Department of Justice. URL: <https://www.justice.gov/criminal-ccips/about-ccips> (дата звернення: 11.06.2024).
127. About CISA | CISA. Cybersecurity and Infrastructure Security Agency CISA. URL: <https://www.cisa.gov/about-cisa> (дата звернення: 11.06.2024).
128. About PIR. The New. URL: <https://thenew.org/org-people/about-pir/> (дата звернення: 11.06.2024).
129. About the Internet Society. Internet Society. URL: <https://www.internetsociety.org/about-internet-society/> (дата звернення: 11.06.2024).

130. About us - IANA. Internet Assigned Numbers Authority. URL: <https://www.iana.org/about> (дата звернення: 11.06.2024).
131. An Act for the general revision of the Copyright Law, title 17 of the United States Code, and for other purposes. LII / Legal Information Institute. URL: <https://www.law.cornell.edu/uscode/text/17> (дата звернення: 11.06.2024).
132. An act to modernize copyright law, and for other purposes - H.R.155. Congress.gov. URL: <https://www.congress.gov/bill/115th-congress/house-bill/1551> (дата звернення: 11.06.2024).
133. Anand A. Digital Piracy - An Overview. Analytics Steps. URL: <https://www.analyticssteps.com/blogs/digital-piracy-overview> (дата звернення: 13.03.2023).
134. Anzilotti D. Corso di diritto internazionale: (ad uso degli studenti dell'Università di Roma). 3rd ed. Roma : Athenaeum, 1928.
135. Atkinson, W. H. A Review of the Trump Administration's National Cyber Strategy: Need for Renewal and Rethinking of the Public-Private Partnership in U.S. National Security Policy. Active Measures - IWP's student journal. 2020. URL: <https://www.iwp.edu/active-measures/2020/10/22/a-review-of-the-trump-administrations-national-cyber-strategy-need-for-renewal-and-rethinking-of-the-public-private-partnership-in-u-s-national-security-policy/> (дата звернення: 11.06.2024).
136. Bakharieva N. How technology companies can protect intellectual property. Yalantis. URL: <https://yalantis.com/blog/protecting-intellectual-property-for-technology-companies/> (дата звернення: 08.04.2024).
137. Bell C. Typosquatting: identity theft built on spelling errors. Bankrate. URL: <https://www.bankrate.com/finance/credit/typosquatting-identity-theft.aspx> (дата звернення: 08.05.2023).

138. Bogush P. Digitalization vs Digitization - Knowing the Difference. *Businessstechweekly.com*. 2021. URL: <https://www.businessstechweekly.com/operational-efficiency/digital-transformation/digitalization-vs-digitization/> (дата звернення: 11.06.2024).
139. Brikše I. The information environment: Theoretical approaches and explanations. *Informācijas vide Latvijā: 21. Gadsimta sākums*. Rīga, 2006. P. 368–415. URL: https://www.lu.lv/fileadmin/user_upload/szf_faili/Petnieciba/sppi/mediji/inta-brikse_anglu.pdf (дата звернення: 11.06.2024).
140. Buletsa S. B., Tegza A. V. Cybersquatting as a violation of intellectual property rights. *Uzhhorod National University Herald. Series: Law*. 2022. No. 67. P. 59. URL: <https://doi.org/10.24144/2307-3322.2021.67.11> (дата звернення: 08.05.2023).
141. Case No. 3,662: Davoll et al. v. Brown. *Massachusetts: Circuit Court, D. Massachusetts*, 1845. 6 p. URL: <https://law.resource.org/pub/us/case/reporter/F.Cas/0007.f.cas/0007.f.cas.0197.pdf> (дата звернення: 11.06.2024).
142. Chakraborty P. Emerging trends of trademark in cyberspace. *International Journal of Creative Research Thoughts (IJCRT)*. 2023. Т. 11, № 5. С. 398–406. URL: <https://ijcrt.org/papers/IJCRT23A5139.pdf> (дата звернення: 21.05.2024).
143. Circular 9: Work-Made-For-Hire Under the 1976 Copyright Act. *US Copyright Office*. 2021. URL: <https://www.copyright.gov/circs/circ30.pdf> (дата звернення: 09.01.2024).
144. CNSS Glossary No. 4009. *Committee on National Security Systems*. 165 p. 2015. URL: <https://nsarchive.gwu.edu/document/22385-document-08-committee-national-security> (дата звернення: 11.06.2024).

145. Commerce Clause. LII / Legal Information Institute. URL: https://www.law.cornell.edu/wex/commerce_clause (дата звернення: 11.06.2024).
146. Consolidated text: Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive). EUR-Lex. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02010L0013-20181218> (дата звернення: 11.06.2024).
147. Constitution of the United States. U.S. Senate. URL: https://www.senate.gov/civics/constitution_item/constitution.htm#a1 (дата звернення: 11.06.2024).
148. Copyright Act : Law of Japan of 06.05.1970 р. № 48. URL: <https://www.japaneselawtranslation.go.jp/en/laws/view/4207> (дата звернення: 15.03.2024).
149. Copyright in a Global Information Economy / М. А. O'Rourke et al. New York : Aspen Publishers, 2006. 831 p.
150. Copyright Law of the United States (Title 17) and Related Laws Contained in Title 17 of the United States Code. U.S. Copyright Office. URL: <https://www.copyright.gov/title17/92chap1.html#117> (дата звернення: 11.06.2024).
151. Copyright, Designs and Patents Act 1988: Act of Parliament від 15.11.1988 р. № 1988 с. 48. URL: <https://www.legislation.gov.uk/ukpga/1988/48/contents> (дата звернення: 02.04.2024).
152. Counterfeit or knockoff designer goods - is it illegal to purchase them?. HG.org Leading Lawyers. URL: <https://www.hg.org/legal->

- articles/counterfeit-or-knockoff-designer-goods-is-it-illegal-to-purchase-them-31573 (дата звернення: 11.06.2024).
153. Cyberspace / Internet. TheFreeDictionary.com. URL: <https://legal-dictionary.thefreedictionary.com/cyberspace> (дата звернення: 01.01.2024).
154. Cyberspace. Duhaime Legal Dictionary. URL: <https://www.duhaime.org/Legal-Dictionary/Term/Cyberspace> (дата звернення: 05.06.2024).
155. Czajkowski S. Ochrona własności przemysłowej i handlowej. Polityka gospodarcza – zagadnienia administracji. 1928. № 1. S. 59–69.
156. Digital Millennium Copyright Act - H.R.2281. United States Congress. URL: <https://www.congress.gov/bill/105th-congress/house-bill/2281> (дата звернення: 02.03.2023).
157. Digital piracy. INTERPOL - The International Criminal Police Organization. URL: <https://www.interpol.int/Crimes/Illicit-goods/Shop-safely/Digital-piracy> (дата звернення: 13.03.2023).
158. Digital Theft Deterrence and Copyright Damages Improvement Act of 1999 - H.R.3456. Congress.gov. URL: <https://www.congress.gov/bill/106th-congress/house-bill/3456/text> (дата звернення: 11.06.2024).
159. Digitalization and information society. selected issues : monograph / ed. by A. Ostenda, T. Nestorenko. Katowice : Publishing House of University of Technology, 2022. 567 p. URL: <http://www.wydawnictwo.wst.pl/uploads/files/8b03138919e2513e3eb7df528f532ecc.pdf> (дата звернення: 12.06.2024).
160. Digitization, digitalization, digital and transformation: the differences. i-SCOOP. URL: <https://www.i-scoop.eu/digital-transformation/digitization-digitalization-digital-transformation-disruption/> (дата звернення: 11.06.2024).

161. Directive (EU) 2015/2436 of the European Parliament and of the Council of 16 December 2015 to approximate the laws of the Member States relating to trade marks (recast). EUR-Lex. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2436&qid=1650351845410> (дата звернення: 11.06.2024).
162. Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information (recast). EUR-Lex. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019L1024&qid=1650262305373> (дата звернення: 11.06.2024).
163. Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services. EUR-Lex. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019L0770&qid=1650262305373> (дата звернення: 11.06.2024).
164. Directive (EU) 2019/789 of the European Parliament and of the Council of 17 April 2019 laying down rules on the exercise of copyright and related rights applicable to certain online transmissions of broadcasting organisations and retransmissions of television and radio programmes, and amending Council Directive 93/83/EEC. EUR-Lex. URL: <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32019L0789> (дата звернення: 11.06.2024).
165. Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC. EUR-Lex. URL: <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32019L0790>

content/EN/TXT/?uri=CELEX:32019L0790&qid=1650262305373
(дата звернення: 11.06.2024).

166. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society. EUR-Lex. URL: [https://eur-lex.europa.eu/legal-](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32001L0029&qid=1650262305373)

content/EN/TXT/?uri=CELEX:32001L0029&qid=1650262305373
(дата звернення: 11.06.2024).

167. Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, European Union (EU), WIPO lex. WIPO - World Intellectual Property Organization. URL: <https://www.wipo.int/wipolex/en/legislation/details/1457> (дата звернення: 05.06.2024).

168. Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights. EUR-Lex. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32004L0048&qid=1650262305373>
(дата звернення: 11.06.2024).

169. Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights. EUR-Lex. URL: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32006L0116> (дата звернення: 11.06.2024).

170. Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs. EUR-Lex. URL: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32009L0024> (дата звернення: 11.06.2024).

171. Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA. *EUR-Lex*. URL: <https://eur-lex.europa.eu/eli/dir/2011/93/oj> (дата звернення: 12.06.2024).
172. Directive 2014/26/EU of the European Parliament and of the Council of 26 February 2014 on collective management of copyright and related rights and multi-territorial licensing of rights in musical works for online use in the internal market Text with EEA relevance. *EUR-Lex*. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014L0026&qid=1650262305373> (дата звернення: 11.06.2024).
173. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases: Consolidated text. *EUR-Lex*. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:01996L0009-20190606> (дата звернення: 11.06.2024).
174. Dixit A. Role of Intellectual Property in Cyber Law. *Enhelion Blogs*. 2022. URL: <https://enhelion.com/blogs/2022/09/01/role-of-intellectual-property-in-cyber-law/> (дата звернення: 09.03.2023).
175. ELDRED V. ASHCROFT. LII / Legal Information Institute. URL: <https://www.law.cornell.edu/supct/search/display.html?terms=copyright&url=/supct/html/01-618.ZS.html> (дата звернення: 11.06.2024).
176. Elkin-Koren N. Copyrights in Cyberspace - Rights without Laws. *Chicago-Kent Law Review*. 1998. Vol. 73, no. 4. P. 1155–1201. URL: <https://scholarship.kentlaw.iit.edu/cgi/viewcontent.cgi?article=3146&context=cklawreview> (дата звернення: 06.01.2024).
177. European Innovation Council and SMEs Executive Agency. Intellectual Property in the digital age. IP Helpdesk. URL:

- https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/intellectual-property-digital-age-2023-11-10_en (дата звернення: 08.04.2024).
178. European Innovation Council, SMEs Executive Agency. Intellectual Property and Digital Art. IP Helpdesk. URL: https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/intellectual-property-and-digital-art-2024-02-29_en (дата звернення: 08.04.2024).
179. Fatima R. An analysis of protection of intellectual property rights in cyberspace. *International journal of legal science and innovation*. 2021. Т. 3, № 3. С. 1155-1171. URL: <https://doi.org/10.10000/IJLSI.11852> (дата звернення: 10.05.2024).
180. Faulkner Y. A Brief Overview of Japanese Patent Law. YMF Law Tokyo Japan. URL: <https://www.ymf-law.com/post/a-brief-overview-of-japanese-patent-law> (дата звернення: 11.04.2024).
181. Federal Trademark Dilution Act of 1995 - H.R.1295. Congress.gov. URL: <https://www.congress.gov/bill/104th-congress/house-bill/1295/text/pl?overview=closed> (дата звернення: 11.06.2024).
182. Feist Publications, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340 (1991). Justia Law. URL: <https://supreme.justia.com/cases/federal/us/499/340/case.html> (дата звернення: 11.06.2024).
183. Filinovich V. Domain name as a means of individualization of participants in civil turnover of Ukraine. *Journal of law and political sciences*. 2020. Vol. 23, no. 2/B. P. 122–160. URL: <https://drive.google.com/file/d/14Gqe-knVVnz3fkEVIrACZxb1mK19EWnC/view> (дата звернення: 08.05.2023).
184. Final Report of the WIPO Internet Domain Name Process. The World Intellectual Property Organization. 1999. URL:

<https://www.wipo.int/amc/en/processes/process1/report/finalreport.html>
(дата звернення: 08.05.2023).

185. Folsom T.C. Defining Cyberspace (Finding Real Virtue in the Place of Virtual Reality). *Tulane Journal of Technology & Intellectual Property*, Vol. 9, 2007, p. 75. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1350999 (дата звернення: 01.01.2024).
186. Freedom and Innovation Revitalizing U.S. Entrepreneurship Act of 2007 - H.R.1201 (Introduced in House - IH). *Congress.gov*. URL: <https://www.congress.gov/bill/110th-congress/house-bill/1201> (дата звернення: 11.06.2024).
187. Fruhlinger J. What is information security? Definition, principles, and jobs. *CSO United States*. 2020. URL: <https://www.csoonline.com/article/3513899/what-is-information-security-definitionprinciples-and-jobs.html>.
188. Gao L. Intellectual Property Rights in the Internet Era: the New Frontier. *The John Marshall Review of Intellectual Property Law*. 2006. P. 589–595. URL: <https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1105&context=ripl> (дата звернення: 02.03.2023).
189. Georgia - Sub-regional Innovation Policy Outlook 2020: Eastern Europe and the South Caucasus. *Georgia : United Nations Economic Commission for Europe*, 2020. 54 p. URL: https://unece.org/sites/default/files/2021-09/RU-Sub-regional_Innovation_Policy_Outlook_2020_GEORGIA_CHAPTERS.pdf (дата звернення: 11.06.2024).
190. Goldman E. The New 'Defend Trade Secrets Act' Is The Biggest IP Development In Years. *Forbes*. 2016. URL: <https://www.forbes.com/sites/ericgoldman/2016/04/28/the-new-defend->

- trade-secrets-act-is-the-biggest-ip-development-in-years/ (дата звернення: 11.06.2024).
191. Gordon P. A basic guide to intellectual property principles. Willans. URL: <https://www.willans.co.uk/knowledge/a-basic-guide-to-intellectual-property-principles/> (дата звернення: 05.06.2024).
192. Gorski A. Zarys prawa handlowego austriackiego. Krakow : Drukarnia Uniwersytetu Jagiellońskiego. 1900. 402 s.
193. Gubaidullina M. Foreign activities and diplomacy in the modern conditions of transparency information space. KazNU Bulletin. International relations and international law series. 2017. Vol 79, no. 3. P. 14–22. URL: <https://doi.org/10.26577/irily-2017-3-731> (дата звернення: 11.06.2024).
194. Guide to the Copyright and related rights treaties administered by WIPO. Geneva : WIPO, 2003. 319 с. URL: https://www.wipo.int/edocs/pubdocs/en/copyright/891/wipo_pub_891.pdf (дата звернення: 02.03.2023).
195. Gupta M. S. What is Digitization, Digitalization, and Digital Transformation?. ARC Advisory Group. 2020. URL: <https://www.arcweb.com/blog/what-digitization-digitalization-digital-transformation> (дата звернення: 11.06.2024).
196. Hardy I. T. Criminal Copyright Infringement. William and Mary Bill of Rights Journal. 2002. Vol. 11. P. 209–342.
197. Hildebrandt M. 7. Copyright in Cyberspace. Law for Computer Scientists. 2019. URL: <https://lawforcomputerscientists.pubpub.org/pub/yjwfiwk5/release/8> (дата звернення: 10.05.2024).
198. Hitchens B., Heard C., Vertes J. Sustainability and Intellectual Property in United Kingdom. Sustainability Objectives in Competition and

- Intellectual Property Law. Cham, 2024. С. 387–415. doi: 10.1007/978-3-031-44869-0_21.
199. Hollis D. A Brief Primer on International Law and Cyberspace. Carnegie Endowment for International Peace. URL: <https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763>.
 200. ICANN. ICANNWiki. URL: <https://icannwiki.org/ICANN> (дата звернення: 11.06.2024).
 201. Information security - NIST special publication 800-30 : Guide for Conducting Risk Assessments. Gaithersburg : National Institute of Standards and Technology, 2012. 95 p. URL: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf> (дата звернення: 05.06.2024).
 202. Information security - NIST special publication 800-39 : Organization, Mission, and Information System View. Gaithersburg : National Institute of Standards and Technology, 2011. 88 p. URL: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf> (дата звернення: 05.06.2024).
 203. Information wars as a threat to the information security of Ukraine / I. Sopilko et al. Conflict Resolution Quarterly. 2021. Vol. 39, no. 3. P. 333–347. URL: <https://doi.org/10.1002/crq.21331> (дата звернення: 11.06.2024).
 204. Inside WIPO. WIPO - World Intellectual Property Organization. URL: <https://www.wipo.int/about-wipo/en/index.html> (дата звернення: 11.06.2024).
 205. Intellectual Property Basics: A Q&A for Students. Beijing City: China National Intellectual Property Administration, 2019. 72 p. URL: <https://doi.org/10.34667/tind.29090>.

206. Intellectual Property Enforcement Act. The Library of Congress. URL: <http://www.thomas.gov/cgi-bin/bdquery/D?d110:10:./temp/~bdr8CY:@@@L&summ2=m&%7C/home/LegislativeData.php?n=BSS;c=110> (дата звернення: 11.06.2024).
207. Intellectual property in cyberspace. Berkman Klein Center. URL: <https://cyber.harvard.edu/property00/patents/> (дата звернення: 05.06.2024).
208. Intellectual property principles for Commonwealth entities. Canberra : Department of Communications and the Arts (Department of Australian government), 2018. 9 p. URL: <https://www.infrastructure.gov.au/sites/default/files/intellectual-property-principles-for-commonwealth-entities.pdf> (дата звернення: 05.06.2024).
209. Intellectual property rights in cyber space. JANAMAITHRI – Journal of Democratic Policing. 2022. Т. 9, № 8. С. 7–32. URL: <https://fire.kerala.gov.in/wp-content/uploads/2022/08/journal-vol9.pdf> (дата звернення: 15.05.2024).
210. Intellectual Property Statistics. WIPO - World Intellectual Property Organization. URL: <https://www.wipo.int/ipstats/en/index.html> (дата звернення: 12.06.2024).
211. Intellectual property. Oxford Learner's Dictionaries. URL: https://www.oxfordlearnersdictionaries.com/definition/american_english/intellectual-property (дата звернення: 01.01.2024).
212. Intellectual property. Wikipedia. URL: https://simple.wikipedia.org/wiki/Intellectual_property#cite_ref-4 (дата звернення: 11.06.2024).
213. Intellectual rights. W3C. URL: <https://www.w3.org/Consortium/Legal/IPR-FAQ-20000620#teacher> (дата звернення: 11.06.2024).

214. Internet Corporation for Assigned Names and Numbers (ICANN).
Internet Corporation for Assigned Names and Numbers. URL:
<https://www.icann.org/> (дата звернення: 11.06.2024).
215. Internet piracy is a type of intellectual property rights violation -
Ministry of Justice of the Republic of Kazakhstan. Information system
PARAGRAPH. URL:
https://online.zakon.kz/Document/?doc_id=30622861&pos=4;-90#pos=4;-90 (дата звернення: 11.06.2024).
216. Internet Society Expresses Concern over Impact of Intellectual
Property Rights Provisions in Trans-Pacific Partnership Agreement (TPP)
Draft - Internet Society. Internet Society. URL:
<https://www.internetsociety.org/news/press-releases/2013/internet-society-expresses-concern-over-impact-of-intellectual-property-rights-provisions-in-trans-pacific-partnership-agreement-tpp-draft/> (дата звернення: 11.06.2024).
217. Internet Society Issues Paper on Intellectual Property on the Internet.
Reston : Internet Society, 2017. 14 p. URL:
https://www.internetsociety.org/wp-content/uploads/2017/08/Internet20Society20Issues20Paper20on20Intellectual20Property20on20the20Internet20Final_EN.pdf (дата звернення: 11.06.2024).
218. Internet Society Submission to European Commission Stakeholders
Consultation - Internet Society. Internet Society. URL:
<https://www.internetsociety.org/news/statements/2011/internet-society-submission-to-european-commission-stakeholders-consultation/> (дата звернення: 11.06.2024).
219. Internet. TheFreeDictionary.com. URL: <https://legal-dictionary.thefreedictionary.com/Internet> (дата звернення: 05.06.2024).

220. IP Issues on the Internet. Lawyer Monthly - Legal News Magazine. URL: <https://www.lawyer-monthly.com/2019/04/ip-issues-on-the-internet/> (дата звернення: 17.05.2023).
221. IPR Related Ramifications in the Cyberspace. IPLF. URL: https://www.ipandlegalfilings.com/ipr-related-ramifications-in-the-cyberspace/?utm_source=rss&utm_medium=rss&utm_campaign=ipr-related-ramifications-in-the-cyberspace (дата звернення: 01.01.2024).
222. Irwin L. What's the difference between information security and cyber security? IT Governance. 2020. URL: <https://www.itgovernance.eu/blog/en/whats-the-difference-between-informationsecurity-and-cyber-security> (дата звернення: 11.06.2024).
223. Israelyan I. Georgia is moving away from pirated software. Digital.Report. 2017. URL: <https://digital.report/v-gruzii-otkazyivayutsya-ot-piratskogo-po/> (дата звернення: 11.06.2024).
224. Jha R. Role of copyright in cyberspace. Legal Service India - Law, Lawyers and Legal Resources. URL: <https://www.legalserviceindia.com/legal/article-5718-role-of-copyright-in-cyberspace.html> (дата звернення: 05.06.2024).
225. Joe Newman, Score one for the good guys: Court rejects Wal-Mart's trademark claim. PublicCitizen (March 21, 2008). <https://citizenvox.wordpress.com/2008/03/21/score-one-for-the-good-guys-court-rejects-wal-marts-trademark-claim/>.
226. Judgment of the Court (Third Chamber) of Handelsgericht Wien of 01.12.2011 in no. C-145/10. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62010CJ0145> (дата звернення: 07.08.2023).
227. Kamen J. Tech group execs rake in cash - Tablet war opens a new front: D.C. - Markey to unveil carrier replies on law enforcement requests

- Smith, others unveil IP bill - It's 'malware Monday'. Politico. 2012. URL: <https://www.politico.com/tipsheets/morning-tech/2012/07/tech-group-execs-rake-in-cash-tablet-war-opens-a-new-front-dc-markey-to-unveil-carrier-replies-on-law-enforcement-requests-smith-others-unveil-ip-bill-its-malware-monday-008852> (дата звернення: 11.06.2024).
228. Kellerman A. Cyberspace Classification and Cognition: Information and Communications Cyberspaces. *Journal of Urban Technology*. 2007. Vol. 14, no. 3. P. 5–32. URL: <https://doi.org/10.1080/10630730801923110> (дата звернення: 11.06.2024).
229. Kohen M., Schramm B. *General Principles of Law*. Oxford Bibliographies. URL: <http://www.oxfordbibliographies.com/view/document/obo-9780199796953/obo-9780199796953-0063.xml> (дата звернення: 05.06.2024).
230. Komaitis K. *Introducing Internet Society's Intellectual Property Issues Paper - Internet Society*. Internet Society. 2013. URL: <https://www.internetsociety.org/blog/2013/06/introducing-internet-societys-intellectual-property-issues-paper/> (дата звернення: 11.06.2024).
231. Kono T. *Cross-border Enforcement of Intellectual Property – Japanese Law and Practice*. *Research Hand-book on Cross-border Enforcement of Intellectual Property* / ред. P. Torreman. Cheltenham, 2014. С. 56–80. URL: <https://www.e-elgar.com/shop/gbp/research-handbook-on-cross-border-enforcement-of-intellectual-property-9781781955796.html> (дата звернення: 04.04.2024).
232. Kozek-Kapuścińska A. *Jak wykazać autorstwo utworu? – Prawo Chroni Sztuke*. *Prawo Chroni Sztuke*. 2019. URL: <https://prawochronisztuke.pl/jak-wykazac-autorstwo-utworu/> (дата звернення: 30.04.2024).

233. Kumari V. Cyber Law - I. Lucknow : University of Lucknow, 2018. 10 p. URL: https://udrc.lkouniv.ac.in/Content/DepartmentContent/SM_aec24985-8fe2-4500-8414-85de787ab1e6_30.pdf.
234. Limitations on liability relating to material online - 17 U.S. Code § 512. Cornell Law School. URL: <https://www.law.cornell.edu/uscode/text/17/512> (дата звернення: 11.06.2024).
235. Lukan M. Copyright protection in Poland. Experience using digital platforms. Law and innovative society. 2022. № 1 (18). С. 66–73. URL: [https://doi.org/10.37772/2309-9275-2022-1\(18\)-6](https://doi.org/10.37772/2309-9275-2022-1(18)-6) (дата звернення: 30.04.2024).
236. Mantri K. Copyright issues in Cyberspace. LinkedIn. 2020. URL: <https://www.linkedin.com/pulse/copyright-issues-cyberspace-keshav-mantri/> (дата звернення: 05.06.2024).
237. Mital R. Linking, Inlining and Framing. Intellectual Property Protection in Cyberspace. The Indira Gandhi National Open University (IGNOU). New Delhi, 2017. P. 16–26. URL: <https://egyankosh.ac.in/bitstream/123456789/7670/1/Unit-9.pdf> (дата звернення: 01.01.2024).
238. Mitra N. Intellectual property rights law in cyberspace. iPleaders. 2021. URL: <https://blog.iplayers.in/intellectual-property-rights-law-in-cyberspace/> (дата звернення: 01.01.2024).
239. Monah G. The various issues in cyberspace that are not addressed by the copyright laws, from the Indian perspective: Dissertation for the award of LL.M. Degree in International Trade Law. Kochi, 2021. 110 с. URL: http://14.139.185.167:8080/jspui/bitstream/123456789/448/1/LLM_0220_023_CAL.pdf (дата звернення: 11.05.2024).

240. Morin J.F. Paradigm shift in the global IP regime. The agency of academics, *Review of International Political Economy*, vol 21-2, 2014, P. 275-309. URL: http://www.chaire-epi.ulaval.ca/sites/chaire-epi.ulaval.ca/files/publications/morin_2014_paradigm_shift_agency_of_a_cademics.pdf
241. Mossoff A. Rethinking the Development of Patents: An Intellectual History, 1550–1800. *Hastings Law Journal*, Vol. 52. 2001. p. 1255. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=863925
242. Muchene P. Sharing and Intellectual Property Protection- An Incongruity? - Internet Society. Internet Society. 2012. URL: <https://www.internetsociety.org/blog/2012/11/sharing-and-intellectual-property-protection-an-incongruity/> (дата звернення: 11.06.2024).
243. Murray M. D. Trademarks, NFTs, and the Law of the Metaverse. 2022. URL: https://www.researchgate.net/publication/361938859_Trademarks_NFTs_and_the_Law_of_the_Metaverse (дата звернення: 21.05.2024).
244. New WIPO Service Provides Evidence of Intellectual Assets' Existence. WIPO - World Intellectual Property Organization. URL: <https://www.wipo.int/wipoproof/en/index.html> (дата звернення: 15.05.2024).
245. Ochoa T. T. Chapter 7: Copyright Duration: Theories and Practice. *Intellectual Property and Information Wealth: Copyright and related rights* / ed. by P. K. Yu. Greenwood, 2007. 133 p.
246. Orlando L. Piracy provisions under the Enforcement Directive and patent infringement. *Jnl of Intellectual Property Law & Pract.* 2007. Vol. 2, no. 10. P. 642—643. URL: <https://academic.oup.com/jiplp/article-abstract/2/10/642/801687?redirectedFrom=fulltext&login=false>
247. Peer-to-Peer File Sharing and Copyright Infringement. University of Maryland, Baltimore. URL: <https://www.umaryland.edu/cits/it-security->

- and-compliance/higher-education-security-standards/peer-to-peer-file-sharing-and-copyright-infringement/ (дата звернення: 13.03.2023).
248. Petrosyan D. Armenia: Copyrights are violated en masse. Law and media of Central Asia. URL: <https://medialaw.asia/node/5450> (дата звернення: 11.06.2024).
249. Płaza S. Historia prawa w polsce na tle porownawczym: w 3 cz. Krakow : Ksiegarnia Akademicka, 2001. 762 p.
250. Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011 - S. 968 (112th). GovTrack. URL: <https://www.govtrack.us/congress/bills/112/s968> (дата звернення: 11.06.2024).
251. Prioritizing Resources and Organization for Intellectual Property Act of 2008 - H.R.4279. Congress.gov. URL: <https://www.congress.gov/bill/110th-congress/house-bill/4279?q=H.R.+4279+%28110%29> (дата звернення: 11.06.2024).
252. Protecting Cyberspace as a National Asset Act of 2010 : a Bill of 15.12.2010 no. S. 3480 [Report No. 111-368]. URL: <https://www.congress.gov/bill/111th-congress/senate-bill/3480/text> (дата звернення: 02.01.2024).
253. Quinn Eu. R. Jr. Abusing Intellectual Property Rights in Cyberspace: Patent Misuse Revisited. William Mitchell Law Review. 2002. Vol. 28: Iss. 3, Article 9. P. 955-1000. URL: <https://open.mitchellhamline.edu/wmlr/vol28/iss3/9>
254. Regional Internet registry. Wikipedia. URL: https://en.wikipedia.org/wiki/Regional_Internet_registry (дата звернення: 11.06.2024).
255. Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union trade mark (codification). EUR-Lex. URL: <https://eur-lex.europa.eu/legal->

content/EN/TXT/?uri=CELEX:32017R1001&qid=1650351845410
(дата звернення: 11.06.2024).

256. Regulation (EU) 2017/1128 of the European Parliament and of the Council of 14 June 2017 on cross-border portability of online content services in the internal marketText with EEA relevance. EUR-Lex. URL: [https://eur-lex.europa.eu/legal-](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32017R1128&qid=1650262305373)

content/EN/TXT/?uri=CELEX:32017R1128&qid=1650262305373
(дата звернення: 11.06.2024).

257. Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240. EUR-Lex. URL: [https://eur-](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R0694&qid=1650352002302)

lex.europa.eu/legal-
content/EN/TXT/?uri=CELEX:32021R0694&qid=1650352002302
(дата звернення: 11.06.2024).

258. Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online. EUR-Lex – Access to European Union law – choose your language. URL: [https://eur-lex.europa.eu/legal-](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R0784&qid=1650351760772)

content/EN/TXT/?uri=CELEX:32021R0784&qid=1650351760772
(дата звернення: 11.06.2024).

259. Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. EUR-Lex. URL: [https://eur-](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32021R0887&qid=1650352002302)

lex.europa.eu/legal-
content/EN/TXT/?uri=CELEX:32021R0887&qid=1650352002302
(дата звернення: 11.06.2024).

260. Regulation (EU) No 386/2012 of the European Parliament and of the Council of 19 April 2012 on entrusting the Office for Harmonization in the

Internal Market (Trade Marks and Designs) with tasks related to the enforcement of intellectual property rights, including the assembling of public and private-sector representatives as a European Observatory on Infringements of Intellectual Property Rights T. EUR-Lex. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012R0386&qid=1650262630281> (дата звернення: 11.06.2024).

261. Regulation (EU) No 513/2014 of the European Parliament and of the Council of 16 April 2014 establishing, as part of the Internal Security Fund, the instrument for financial support for police cooperation, preventing and combating crime, and crisis management and repealing Council Decision 2007/125/JHA. EUR-Lex. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0513&qid=1650352002302> (дата звернення: 11.06.2024).

262. Research Works Act - H.R.3699. Congress.gov. URL: <https://www.congress.gov/bill/112th-congress/house-bill/3699> (дата звернення: 11.06.2024).

263. Review of the legislation of Moldova in the field of intellectual property. Digital Report. URL: <https://digital.report/zakonodatelstvo-moldovy-copyright/> (дата звернення: 11.06.2024).

264. Röttger P., Vedres B. The Information Environment and its Effects on Individuals and Groups. Oxford : Oxford Internet Institute, 2020. 60 p. URL: <https://royalsociety.org/-/media/policy/projects/online-information-environment/oie-the-information-environment.PDF> (дата звернення: 11.06.2024).

265. Rouse M. Internet Society. Techopedia. 2010. URL: <https://www.techopedia.com/definition/2432/internet-society-isoc> (дата звернення: 11.06.2024).

266. Rousseau C. Principes généraux du droit international public. Paris : A. Pedone, 1944. Vol. 1. 975 p.
267. Rudra A. What is Typosquatting in Cybersecurity? Definition, Prevention & More. PowerDMARC. URL: <https://powerdmarc.com/what-is-typosquatting/> (дата звернення: 08.05.2023).
268. Rueter T. Newegg and Overstock win a patent-infringement case in federal court. Digital Commerce 360. URL: <https://www.digitalcommerce360.com/2011/10/19/newegg-and-overstock-win-patent-infringement-case/> (дата звернення: 17.05.2023).
269. Sansare N. S. Protecting Digital Intellectual Property in the Digital Era. Medium. URL: <https://medium.com/@sansareneha10/protecting-digital-intellectual-property-in-the-digital-era-3d77fea44349> (дата звернення: 02.04.2024).
270. Sarangi K. Concept of Jurisdiction in Cyberspace. LinkedIn. 2023. URL: <https://www.linkedin.com/pulse/concept-jurisdiction-cyberspace-kirtika-sarangi-tv3dc/> (дата звернення: 10.05.2024).
271. Security and defense. MFA. URL: <https://www.mfa.am/ru/security-and-defense/> (дата звернення: 11.06.2024).
272. Security and privacy controls for federal information systems and organizations. Gaithersburg : National Institute of Standards and Technology, 2013. 463 p. URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf> (дата звернення: 05.06.2024).
273. Sherman B. The making of modern intellectual property law: The British experience, 1760-1911. Cambridge: Cambridge University Press, 1999. 242 p.
274. Shetland times, ltd. v. Jonathan Wills. Casemine. URL: <https://www.casemine.com/judgement/uk/5a8ff8d660d03e7f57ece180> (дата звернення: 07.06.2024).

275. Singh S. Analysis of copyright issue in cyberspace. Legal Service India - Law, Lawyers and Legal Resources. URL: <https://www.legalserviceindia.com/legal/article-3286-analysis-of-copyright-issue-in-cyberspace.html> (дата звернення: 05.06.2024).
276. Stop Online Piracy Act - H.R.3261. The Library of Congress. URL: <http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.3261> (дата звернення: 11.06.2024).
277. Structure Definition & Meaning. Encyclopedia Britannica. URL: <https://www.britannica.com/dictionary/structure> (дата звернення: 17.05.2022).
278. Structure noun. Oxford Learner's Dictionaries. URL: https://www.oxfordlearnersdictionaries.com/definition/english/structure_1 (дата звернення: 07.06.2024).
279. Supplemental information for the interagency report on strategic U.S. government engagement in international standardization to achieve U.S. objectives for cybersecurity : NISTIR 8074. Gaithersburg : National Institute of Standards and Technology, 2015. Vol. 2. 79 p. URL: <https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf> (дата звернення: 05.06.2024).
280. Svitlichnyy O. To the question reform of the state system of legal protection of intellectual property in Ukraine. Visegrad journal on human rights. 2023. № 2. С. 152–155. URL: <https://doi.org/10.61345/1339-7915.2023.2.22> (дата звернення: 22.05.2024).
281. Tarasenko L. L. New Copyright Law (2022): Challenges and Prospects. Juridical scientific and electronic journal. 2022. № 12. С. 171–174. URL: <https://doi.org/10.32782/2524-0374/2022-12/36> (дата звернення: 09.01.2024).

282. Tareen N. Trademark in Cyberspace. Legal Desire Media and Insights. URL: <https://legaldesire.com/trademark-in-cyberspace/> (дата звернення: 05.06.2024).
283. The Anticybersquatting Consumer Protection Act - Senate Report 106-140. GovInfo - U.S. Government Publishing Office. URL: <https://www.govinfo.gov/content/pkg/CRPT-106srpt140/html/CRPT-106srpt140.htm> (дата звернення: 11.06.2024).
284. The Concept of Framing. Legal Services India. URL: <https://www.legalservicesindia.com/article/2413/The-Concept-of-Framing.html> (дата звернення: 09.03.2023).
285. The Copyright Term Extension Act of 1998. Congress.gov. URL: <https://www.congress.gov/bill/105th-congress/senate-bill/505> (дата звернення: 11.06.2024).
286. The Internet Society and IETF Announce New Strategic Agreement to Support Ongoing Work on Open Standards - Internet Society. Internet Society. URL: <https://www.internetsociety.org/news/press-releases/2020/the-internet-society-and-ietf-announce-new-strategic-agreement-to-support-ongoing-work-on-open-standards/> (дата звернення: 11.06.2024).
287. The law regulating the copyright of Armenian media came into force. Telecommunications portal telecom.arka.am. URL: https://telecom.arka.am/ru/news/internet/vstupil_v_silu_zakon_reguliruyushchiy_avtorskie_prava_armyanskikh_smi/ (дата звернення: 11.06.2024).
288. The Problems of Intellectual Property in Digital Protection of Cultural Heritage—Taking Dunhuang Culture as an Example / S. Yu1 та ін. Proceedings of the 2023 9th International Conference on Humanities and Social Science Research (ICHSSR 2023). 2023. С. 790–798. URL:

https://doi.org/10.2991/978-2-38476-092-3_96 (дата звернення: 08.04.2024).

289. The right to share: principles on freedom of expression and copyright in the digital age. London: ARTICLE 19, 2013. 28 p. URL: <https://www.article19.org/data/files/medialibrary/3716/13-04-23-right-to-share-EN.pdf> (дата звернення: 05.06.2024).
290. The situation, challenges, and future research directions in cyber crime analysis. Intellectual property and cyber law / ред.: А. К. Babu, Т. Singh. New Delhi, 2023. С. 1–15. URL: https://www.researchgate.net/publication/378182974_Intellectual_Property_and_Cyber_Law (дата звернення: 07.05.2024).
291. The United States Patent and Trademark Office (USPTO). United States Patent and Trademark Office. URL: <https://www.uspto.gov/about-us> (дата звернення: 11.06.2024).
292. Theories of Intellectual Property Rights. *IP Matters*. URL: <https://www.theipmatters.com/post/theories-of-intellectual-property-rights> (дата звернення: 13.06.2024).
293. Thon А. Z zagadnień ochrony prawa z rejestracji znaku towarowego. Warszawa : Skład Główny: Dom Książki Polskiej. 1934. 21 s.
294. Till E. Nauki ogólne austriackiego prawa prywatnego. Lwow : Nakładem Księgarni H. Altenberga. 1911. 510 s.
295. Title developing cyber resilient systems: a systems security engineering approach : Series/Number NIST Special Publication 800-160. Gaithersburg : National Institute of Standards and Technology, Vol. 2, 2021. 230 p. URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf> (дата звернення: 05.06.2024).

296. Trademark Dilution Revision Act of 2006 - H.R. 683 (109th). GovTrack. URL: <https://www.govtrack.us/congress/bills/109/hr683> (дата звернення: 11.06.2024).
297. UDRP. ICANNWiki. URL: <https://icannwiki.org/UDRP> (дата звернення: 11.06.2024).
298. Uniform Domain-Name Dispute-Resolution Policy. Internet Corporation for Assigned Names and Numbers (ICANN). URL: <https://www.icann.org/resources/pages/help/dndr/udrp-en> (дата звернення: 11.06.2024).
299. Uniform Trade Secrets Act. WIPO - World Intellectual Property Organization. URL: <https://www.wipo.int/edocs/lexdocs/laws/en/us/us034en.pdf> (дата звернення: 11.06.2024).
300. Unlocking Consumer Choice and Wireless Competition Act - S.517. Congress.gov. URL: <https://www.congress.gov/bill/113th-congress/senate-bill/517> (дата звернення: 11.06.2024).
301. Ustawa o prawie autorskiem z dnia 29 marca 1926r. DzURP, 1926.Nr. 48. Poz. 286.
302. Veliyev H. Azerbaijan launches copyright protection system on the Internet. Trend.Az. URL: <https://www.trend.az/business/it/2306291.html> (дата звернення: 11.06.2024).
303. Verma R. Trademark issues in cyberspace. LinkedIn: Log In or Sign Up. 2020. URL: <https://www.linkedin.com/pulse/trademark-issues-cyberspace-radhika-verma/> (дата звернення: 17.05.2024).
304. Vincent J. AI art tools Stable Diffusion and Midjourney targeted with copyright lawsuit. The Verge. 2023. URL: <https://www.theverge.com/2023/1/16/23557098/generative-ai-art-copyright-legal-lawsuit-stable-diffusion-midjourney-deviantart> (дата звернення: 09.01.2024).

305. Watanabe T., Kidokoro I. A World Without Cablevision nor Sony: How Japanese Courts Find Providers of Personal Locker and Content-Sharing Services Liable. SSRN Electronic Journal. 2013. С. 1–34. URL: <https://doi.org/10.2139/ssrn.2238359> (дата звернення: 11.04.2024).
306. Węgrzak M. Intellectual Property Law in Japan. Contemporary trends and challenges. Gdańskie Studia Azji Wschodniej. 2022. № 21. С. 27–40. URL: <https://doi.org/10.4467/23538724gs.22.020.16136> (дата звернення: 11.04.2024).
307. What Does ICANN Do? Internet Corporation for Assigned Names and Numbers (ICANN). URL: <https://www.icann.org/resources/pages/what-2012-02-25-en> (дата звернення: 11.06.2024).
308. What is Smart Everything? – How it Works. Synopsys. URL: <https://www.synopsys.com/glossary/what-is-smart-everything.html> (дата звернення: 12.06.2024).
309. WIPO: Conference drops controversial provisions. SUNS - South North Development Monitor. URL: <https://www.sunsonline.org/trade/areas/intellect/12200096.htm> (дата звернення: 12.06.2024).
310. WIPO/ACE/12/INF/2 PROV. 2 : документ Секретаріату ВОІВ. Женева : ВОІВ, 2017. 18 р. URL: https://www.wipo.int/edocs/mdocs/enforcement/ru/wipo_ace_12/wipo_ace_12_inf_2_prov_2.pdf (дата звернення: 11.06.2024).
311. Xin C. How Does Intellectual Property Protection Empower Technological Innovation in Enterprises - Take China as an Example. Lecture Notes in Education Psychology and Public Media. 2023. Т. 24, № 1. С. 108–114. URL: <https://doi.org/10.54254/2753-7048/24/20230635> (дата звернення: 09.04.2024).

312. Yadav S. N. What is the difference between copyright and piracy?. Quora. URL: <https://www.quora.com/What-is-the-difference-between-copyright-and-piracy> (дата звернення: 13.03.2023).
313. Zaidi K. IPR Issues In Cyberspace. IP Bulletin. URL: <https://ipbulletin.in/ipr-issues-cyberspace/> (дата звернення: 13.03.2023).
314. Zalnieriute M. Beyond the Governance Gap in International Domain Name Law: Bringing the UDRP in Line with Internationally Recognized Human Rights. *Stanford Journal of International Law*. 2019. Т. 56, № 1. С. 5–67. URL: <https://doi.org/10.2139/ssrn.3532799> (дата звернення: 21.05.2024).
315. Zekos G. I. Copyrights and trademarks in cyberspace: a legal and economic analysis. *Chicago-Kent journal of intellectual property*. 2016. Т. 15, № 1. С. 313–363. URL: <https://scholarship.kentlaw.iit.edu/cgi/viewcontent.cgi?article=1166&context=ckjip> (дата звернення: 10.05.2024).
316. Ziter P. Protecting Intellectual Property in the Digital Age: Safeguarding Creations in Vietnam. *Lexology*. URL: <https://www.lexology.com/library/detail.aspx?g=40a6cc4d-722c-46a9-b4f9-398626296d17> (дата звернення: 02.04.2024).
317. Zubko O. Modern concept of administrative and legal protection of cyberspace in Ukraine. *Entrepreneurship, economy and law*. 2022. № 5. С. 51–55. URL: <https://doi.org/10.32849/2663-5313/2022.5.08> (дата звернення: 06.05.2024).

Опубліковані праці здобувачки за темою дисертації:

318. Филинович В. В. Киберсталкинг: проблемы правовой защиты. Наукові праці Національного авіаційного університету. Серія: «Юридичний вісник «Повітряне і космічне право». 2021. №1 (58). – С. 135-141.
319. Филинович В.В. Место киберпространства в информационной среде и правовое обеспечение их функционирования. Матеріали XII Міжнародної науково-практичної конференції "Права людини в епоху цифрових трансформацій", м. Київ, Національний авіаційний університет, 25 лютого 2022 р. Том 2. – Тернопіль: Вектор, 2022. – С. 106-109.
320. Филинович В.В. Фотография и авторское право: роль объекта и его правовая защита. АЕРО-2020. Повітряне і космічне право: зб. тез доп. всеукр. наук.-практ. конф., м. Київ, 20 листопада 2020 р. Київ, 2020. Том 2. С. 26-28.
321. Філінович В. В. Визначення поняття веб-сайт у національному законодавстві та правовій доктрині // Інноваційний розвиток правової науки в умовах модернізації суспільства: матеріали X Міжнародної науково-практичної конференції, м. Київ, Національний авіаційний університет, 28 лютого 2020 р. Тернопіль: Вектор. 2020. С. 174-176.
322. Філінович В. В. Кібербезпека та інтернет речей: правовий аспект. Наукові праці Національного авіаційного університету. Серія: «Юридичний вісник «Повітряне і космічне право». 2020. №4 (57). С. 122-127.
323. Філінович В. В. Передання прав на доменне ім'я та його трансфер до іншого реєстратора. Науковий вісник Міжнародного гуманітарного університету. Серія «Юриспруденція». 2018. № 34. С. 62–64.

324. Філінович В. В. Проблеми правового регулювання відповідальності органів державної влади за порушення прав громадян в сфері кіберзлочинів. Проблеми правового регулювання відповідальності органів державної влади за порушення прав громадян : колект. монографія. НАУ. Київ, 2021. С. 116–126.
325. Філінович В. В. Система DAAR та моніторинг зловживань у галузі доменних імен. Матеріали ІХ Міжнародної науково-практичної конференції молодих учених і студентів «Юриспруденція в сучасному інформаційному просторі», (Київ, 1 березня 2019 р). 2019. Т. 2. С. 157-159.
326. Філінович В. В. Сутність інтернаціоналізованих доменних імен та їх правове регулювання. Електронне наукове фахове видання «Порівняльно-аналітичне право». 2019. №3. С. 99-101.
327. Філінович В. В. Тростове середовище Інтернет як важливий елемент кібербезпеки. Матеріали ХІ Міжнародної науково-практичної конференції «Сучасне право в епоху соціальних змін», (Київ, 26 лютого 2021 р). – С. 157-159.
328. Філінович В. В. GDPR та специфікація реєстраційних даних загальних доменів верхнього рівня. АЕРО-2018. Повітряне і космічне право: матеріали Всеукраїнської конференції молодих учених і студентів, м. Київ, Національний авіаційний університет, 22 листопада 2018 р. Том 2. – Тернопіль: Вектор. 2018. С. 21–23.
329. Філінович В. В., Новгородська І.М. Захист прав власників доменних імен. Електронне наукове фахове видання «Порівняльно-аналітичне право». 2019. №5. С. 136-138.
330. Філінович В.В. Кібербезпека та загрози авіаційній сфері: правовий аспект. Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне

право». 2021. № 3 (60). С. 38–44. <https://doi.org/10.18372/2307-9061.60.15950>

331. Філінович В.В. Права інтелектуальної власності у кібернетичному просторі як неосновоположні, але важливі права людини. Гарантії прав людини і громадянина в контексті європейської інтеграції України: монографія / Юринець Ю.Л., Токарева К.С., Філінович В.В. та ін. - Чернівці: Технодрук. 2023. С. 166-177.
332. Filinovich V. Cybersecurity guarantees as a factor of state information security. Problems of implementation of state policy in the field of information security of Ukraine : Collective monograph. Accent Graphics Communications & Publishing. Ottawa, 2020. С. 144–156.
333. Filinovich V. Conceptual Grounds for Development of Effective Legal Enforcement of Intellectual Property Rights in Cyberspace. Journal of International Legal Communication. 2024. Vol. 13, № 2. P. 74–843. URL: <https://doi.org/10.32612/uw.27201643.2024.13.2.pp.74-84>
334. Filinovich V. Correlation between human rights and intellectual property rights. III Міжнародна науково-практична конференція «Модернізація вітчизняної правової системи в умовах світової інтеграції» (м. Кропивницький, 23-24 червня 2022 року). - Кропивницький, 2022. С. 240-242. URL: https://www.klanau.kr.ua/images/docs/Modernizaciia_vitchiznianoy_pravovoy_systemy_23062022.pdf.
335. Filinovich V. Domain Name as a Means of Individualization of Participants in Civil Turnover of Ukraine. Journal of Law and Political Sciences. 2020. Vol. 24. Issue 3. P. 180–211. / Web of Science.
336. Filinovich V. Effectiveness of legal enforcement of intellectual property rights in cyberspace. Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне

право». 2024. Т. 2, № 71. С. 154–160. URL: <https://doi.org/10.18372/2307-9061.71.18804>.

337. Filinovich V. How to overcome intellectual property infringements in cyberspace: Ukrainian experience. Book of Abstracts. International Conference: XXI century, new challenges and modern development tendencies of law, December 21-22, 2021. Baku State University. Baku, Azerbaijan, 2021. С. 196-197.
338. Filinovich V. Problems of Human Rights Violations Caused by Cybercrimes and Ways to Overcome Them. Наукові праці Національного авіаційного університету. Серія: «Юридичний вісник «Повітряне і космічне право». 2020. №3 (56). С. 143–148.
339. Filinovich V. V. Cybersecurity gaps as a problem of modern aviation: legal aspect. «АВІА-2021» : матеріали XV міжнар. науково-техн. конф., м. Київ, 20–22 квіт. 2021 р. Київ, 2021. С. 31.1–31.4. URL: <http://conference.nau.edu.ua/index.php/AVIA/AVIA2021/paper/view/7995/6631>.
340. Filinovich V. V. Legal status of domain names in the legislation of Ukraine and doctrinal sources. Наукові праці Національного авіаційного університету. Серія: «Юридичний вісник «Повітряне і космічне право». 2020. №2 (55). С. 144–150.
341. Filinovich V. V. Website regulatory laws of the USA. Наукові праці Національного авіаційного університету. Серія: «Юридичний вісник «Повітряне і космічне право». 2019. №3 (52). С. 115–121.
342. Filinovich V. Violation of antitrust laws by UIA and well-known low-cost carriers. Тези доповідей XIV Міжнародної науково-технічної конференції «АВІА-2019», (Київ, 23-25 квітня 2019 року). – С. 33.8–33.11.
343. Filinovich V. Violation of copyright and related rights on the internet: how to protect yourself and your creation. Наукові праці

- Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право». 2021. №4 (61). С. 144–150. <https://doi.org/10.18372/2307-9061.61.16362>
344. Filinovych V., Hu Z. Aviation and the Cybersecurity Threats. Proceedings of the International Conference on Business, Accounting, Management, Banking, Economic Security and Legal Regulation Research (BAMBEL 2021) : Proceedings of the International Conference, Kyiv, 26–27 August 2021. Amsterdam, 2021. P. 120–126. URL: <https://doi.org/10.2991/aebmr.k.210826.021>.
345. Filinovych V., Sukhanov O. Domain name in the system of objects of intellectual property rights. Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право». 2022. №3 (64). С. 146–152. <https://doi.org/10.18372/2307-9061.64.16884>
346. Filinovych V.V. Genesis of the legal regulation of the functioning of intellectual property in cyberspace. Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право». 2023. №1 (66). С. 133-139.
347. Filinovych V.V. The structure of intellectual property rights relations in cyberspace. Матеріали XIII Міжнародної науково-практичної конференції "Свобода, безпека та незалежність: правовий вимір", Національний авіаційний університет (Київ, 24 лютого 2023 р.). – С. 553-556.
348. Sopilko I., Filinovych V. Development of the Internet trust Environment as an Important Element for Cybersecurity. University law science and education in the challenges of our time : Collective monograph. Warszawa, 2021. С. 291–30.
349. Sopilko I., Filinovych V., Pankova L. O., Obshalov S.V., Chaplinskyi K. O. Protection of Intellectual Property Rights from Cyber

Threats in the Global Information Environment. *Novum Jus*. 2023. Vol. 17(1). P. 237–258. <https://doi.org/10.14718/NovumJus.2023.17.1.10>

350. Sopilko I., Filinovich V., Prudnykova O. V., Krupnova A., Smetanina N. Ensuring the functioning of cyberspace in Ukraine: Legal and technical aspects. *Sapienza: International Journal of Interdisciplinary Studies*. 2024. Vol. 5, no. 3. P. e24055. <https://doi.org/10.51798/sijis.v5i3.787>.

351. Voronova O., V. Filinovich. The Role of the Web-based Distance Learning Environment in the Education of Future Lawyers. *Наукові праці Національного авіаційного університету. Серія: «Юридичний вісник «Повітряне і космічне право»*. 2020. №4 (57). – С. 188–193.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковано основні наукові результати дисертації

Статті в наукових фахових виданнях України

1. Філінович В. В. Передання прав на доменне ім'я та його трансфер до іншого реєстратора. *Науковий вісник Міжнародного гуманітарного університету. Серія «Юриспруденція»*. 2018. № 34. С. 62–64.
2. Філінович В. В. Сутність інтернаціоналізованих доменних імен та їх правове регулювання. *Електронне наукове фахове видання «Порівняльно-аналітичне право»*. 2019. №3. С. 99-101.
3. Filinovych V. V. Website regulatory laws of the USA. *Наукові праці Національного авіаційного університету. Серія: «Юридичний вісник «Повітряне і космічне право»*. 2019. №3 (52). С. 115–121.
4. Філінович В. В., Новгородська І.М. Захист прав власників доменних імен. *Електронне наукове фахове видання «Порівняльно-аналітичне право»*. 2019. №5. С. 136-138. *Внесок здобувача: 75%*
5. Filinovych V. V. Legal status of domain names in the legislation of Ukraine and doctrinal sources. *Наукові праці Національного авіаційного університету. Серія: «Юридичний вісник «Повітряне і космічне право»*. 2020. №2 (55). С. 144–150.
6. Filinovych V. Problems of Human Rights Violations Caused by Cybercrimes and Ways to Overcome Them. *Наукові праці Національного авіаційного університету. Серія: «Юридичний вісник «Повітряне і космічне право»*. 2020. №3 (56). С. 143–148.
7. Філінович В. В. Кібербезпека та інтернет речей: правовий аспект. *Наукові праці Національного авіаційного університету. Серія:*

- «Юридичний вісник «Повітряне і космічне право»*. 2020. №4 (57). С. 122-127.
8. Voronova O., V. Filinovych. The Role of the Web-based Distance Learning Environment in the Education of Future Lawyers. *Наукові праці Національного авіаційного університету. Серія: «Юридичний вісник «Повітряне і космічне право»*. 2020. №4 (57). – С. 188–193. *Внесок здобувача: 50%*
 9. Филинович В. В. Киберсталкинг: проблемы правовой защиты. *Наукові праці Національного авіаційного університету. Серія: «Юридичний вісник «Повітряне і космічне право»*. 2021. №1 (58). – С. 135-141.
 10. Філінович В.В. Кібербезпека та загрози авіаційній сфері: правовий аспект. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. 2021. № 3 (60). С. 38–44. <https://doi.org/10.18372/2307-9061.60.15950>
 11. Filinovych V. Violation of copyright and related rights on the internet: how to protect yourself and your creation. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. 2021. №4 (61). С. 144–150. <https://doi.org/10.18372/2307-9061.61.16362>
 12. Filinovych V., Sukhanov O. Domain name in the system of objects of intellectual property rights. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. 2022. №3 (64). С. 146–152. <https://doi.org/10.18372/2307-9061.64.16884> *Внесок здобувача: 75%*
 13. Filinovych V.V. Genesis of the legal regulation of the functioning of intellectual property in cyberspace. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. 2023. №1 (66). С. 133-139.

14.Filinovych V. Effectiveness of legal enforcement of intellectual property rights in cyberspace. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. 2024. Т. 2, № 71. С. 154–160. URL: <https://doi.org/10.18372/2307-9061.71.18804>.

Статті в наукових періодичних виданнях інших держав

15.Filinovych V. Domain Name as a Means of Individualization of Participants in Civil Turnover of Ukraine. *Journal of Law and Political Sciences*. 2020. Vol. 24. Issue 3. P. 180–211. / *Web of Science*.

16.Sopilko I., Filinovych V., Pankova L. O., Obshalov S.V., Chaplynskyi K. O. Protection of Intellectual Property Rights from Cyber Threats in the Global Information Environment. *Novum Jus*. 2023. Vol. 17(1). P. 237–258. <https://doi.org/10.14718/NovumJus.2023.17.1.10> *Внесок здобувача: 20% / Scopus*.

17.Filinovych V. Conceptual Grounds for Development of Effective Legal Enforcement of Intellectual Property Rights in Cyberspace. *Journal of International Legal Communication*. 2024. Vol. 13, № 2. P. 74–843. URL: <https://doi.org/10.32612/uw.27201643.2024.13.2.pp.74-84>

18.Sopilko I., Filinovych V., Prudnykova O. V., Krupnova A., Smetanina N. Ensuring the functioning of cyberspace in Ukraine: Legal and technical aspects. *Sapienza: International Journal of Interdisciplinary Studies*. 2024. Vol. 5, no. 3. P. e24055. <https://doi.org/10.51798/sijis.v5i3.787> *Внесок здобувача: 20% / Scopus*.

Розділи в монографіях

19.Filinovich V. Cybersecurity guarantees as a factor of state information security. *Problems of implementation of state policy in the field of*

information security of Ukraine : Collective monograph. Accent Graphics Communications & Publishing. Ottawa, 2020. С. 144–156.

20. Філінович В. В. Проблеми правового регулювання відповідальності органів державної влади за порушення прав громадян в сфері кіберзлочинів. *Проблеми правового регулювання відповідальності органів державної влади за порушення прав громадян* : колект. монографія. НАУ. Київ, 2021. С. 116–126.
21. Sopilko I., Filinovych V. Development of the Internet trust Environment as an Important Element for Cybersecurity. *University law science and education in the challenges of our time* : Collective monograph. Warszawa, 2021. С. 291–30. *Внесок здобувача: 50%*
22. Філінович В.В. Права інтелектуальної власності у кібернетичному просторі як неосновоположні, але важливі права людини. *Гарантії прав людини і громадянина в контексті європейської інтеграції України: монографія* / Юринець Ю.Л., Токарева К.С., Філінович В.В. та ін. - Чернівці: Технодрук. 2023. С. 166-177.

Наукові праці, які засвідчують апробацію матеріалів дисертації

23. Філінович В. В. GDPR та специфікація реєстраційних даних загальних доменів верхнього рівня. *АЕРО-2018. Повітряне і космічне право*: матеріали Всеукраїнської конференції молодих учених і студентів, м. Київ, Національний авіаційний університет, 22 листопада 2018 р. Том 2. – Тернопіль: Вектор. 2018. С. 21–23.
24. Філінович В. В. Система DAAR та моніторинг зловживань у галузі доменних імен. Матеріали *IX Міжнародної науково-практичної конференції молодих учених і студентів «Юриспруденція в сучасному інформаційному просторі»*, (Київ, 1 березня 2019 р). 2019. Т. 2. С. 157-159.

25. Filinovich V. Violation of antitrust laws by UIA and well-known low-cost carriers. Тези доповідей *XIV Міжнародної науково-технічної конференції «AVIA-2019»*, (Київ, 23-25 квітня 2019 року). – С. 33.8–33.11.
26. Філінович В. В. Визначення поняття веб-сайт у національному законодавстві та правовій доктрині // *Інноваційний розвиток правової науки в умовах модернізації суспільства*: матеріали X Міжнародної науково-практичної конференції, м. Київ, Національний авіаційний університет, 28 лютого 2020 р. Тернопіль: Вектор. 2020. С. 174-176.
27. Филинович В.В. Фотография и авторское право: роль объекта и его правовая защита. *АЕРО-2020. Повітряне і космічне право*: зб. тез доп. всеукр. наук.-практ. конф., м. Київ, 20 листопада 2020 р. Київ, 2020. Том 2. С. 26-28.
28. Філінович В. В. Трестове середовище Інтернет як важливий елемент кібербезпеки. *Матеріали XI Міжнародної науково-практичної конференції «Сучасне право в епоху соціальних змін»*, (Київ, 26 лютого 2021 р). – С. 157-159.
29. Filinovich V. V. Cybersecurity gaps as a problem of modern aviation: legal aspect. «AVIA-2021» : матеріали XV міжнар. науково-техн. конф., м. Київ, 20–22 квіт. 2021 р. Київ, 2021. С. 31.1–31.4. URL: <http://conference.nau.edu.ua/index.php/AVIA/AVIA2021/paper/view/7995/663>.
30. Filinovich V. How to overcome intellectual property infringements in cyberspace: Ukrainian experience. Book of Abstracts. *International Conference: XXI century, new challenges and modern development tendencies of law*, December 21-22, 2021. Baku State University. Baku, Azerbaijan, 2021. С. 196-197.
31. Filinovich V., Hu Z. Aviation and the Cybersecurity Threats. *Proceedings of the International Conference on Business, Accounting, Management*,

Banking, Economic Security and Legal Regulation Research (BAMBEL 2021) : Proceedings of the International Conference, Kyiv, 26–27 August 2021. Amsterdam, 2021. P. 120–126. URL: <https://doi.org/10.2991/aebmr.k.210826.021>. *Внесок здобувача: 75%*

32. Филинович В.В. Место киберпространства в информационной среде и правовое обеспечение их функционирования. Матеріали XII Міжнародної науково-практичної конференції "Права людини в епоху цифрових трансформацій", м. Київ, Національний авіаційний університет, 25 лютого 2022 р. Том 2. – Тернопіль: Вектор, 2022. – С. 106-109.
33. Filinovich V. Correlation between human rights and intellectual property rights. III Міжнародна науково-практична конференція «Модернізація вітчизняної правової системи в умовах світової інтеграції» (м. Кропивницький, 23-24 червня 2022 року). - Кропивницький, 2022. С. 240-242. URL: https://www.klanau.kr.ua/images/docs/Modernizaciia_vitchiznianoy_pravovoy_systemy_23062022.pdf.
34. Filinovich V.V. The structure of intellectual property rights relations in cyberspace. Матеріали XIII Міжнародної науково-практичної конференції "Свобода, безпека та незалежність: правовий вимір", Національний авіаційний університет (Київ, 24 лютого 2023 р.). – С. 553-556.