

## СПИСОК ЛІТЕРАТУРИ

1. Цивільний кодекс України від 16 серпня 2020 р. № 40–44. *Відомості Верховної Ради України*. 2003. Ст. 356 (Із змінами).
2. Про авторське право і суміжні права: Закон України від 2 листопада 2018 р. № 13. *Відомості Верховної Ради України*. 1994. Ст. 64 (Із змінами).
3. П'єр Брассо. URL: [https://uk.wikipedia.org/wiki/%D0%9F%27%D1%4%D1%80\\_%D0%91%D1%80%D0%B0%D1%81%D1%81%D0%BE](https://uk.wikipedia.org/wiki/%D0%9F%27%D1%4%D1%80_%D0%91%D1%80%D0%B0%D1%81%D1%81%D0%BE) (Дата звернення: 13.09.2020 р.).
4. У Лондоні відкрилася галерея з картинами легендарного шимпанзе-художника Конго. URL: <https://world.segodnya.ua/ua/world/europe/v-londone-otkrylas-galereya-s-kartinami-legendarnogo-shimpanze-hudozhnika-kongo-1344548.html> (Дата звернення: 14.09.2020 р.).
5. Як тварини малюють картини, або неупереджена краса. URL: <https://ua.waykun.com/articles/jak-tvarini-maljujut-kartini-abo-neuperedzhena-krasa.php> (Дата звернення: 16.09.2020 р.).
6. Слон малює картини, які продаються за шалені гроші. URL: <https://galka.if.ua/slonmalyuye-kartini-yaki-prodayutsya-za-shaleni-grosi/> (Дата звернення: 16.09.2020 р.).
7. Африканський Пікассо: Талановита свиня малює в стилі абстрактного експресіонізму. URL: [https://zik.ua/news/2019/03/19/afrykanskyu\\_pikasso\\_talanovyta\\_svynya\\_malyuie\\_v\\_styli\\_abstraktnogo\\_1532501](https://zik.ua/news/2019/03/19/afrykanskyu_pikasso_talanovyta_svynya_malyuie_v_styli_abstraktnogo_1532501) (Дата звернення: 09.09.2020 р.).
8. Уткіна М. С. Можливість віднесення творів, створених штучним інтелектом, до об'єктів інтелектуальної власності. *Правові горизонти*. 2019. № 17 (30). С. 42–46.
9. David Crary. Intellectual property: case of the monkey's selfie and animals' copyright. URL: <https://www.insurancejournal.com/news/national/2015/09/25/382768.htm> (Дата звернення: 18.09.2020 р.).
10. Самілік Л. О., Корбут Л. П. Співвідношення понять «суб'єкт права», «особа», «суб'єкт правовідносин», «учасник правовідносин». *Право і суспільство*. № 1. 2016. С. 89–93.

УДК 340.1

## РЕГУЛЮВАННЯ ВІДНОСИН У ЦИФРОВОМУ ПРОСТОРІ: ПОРІВНЯЛЬНО-ПРАВОВИЙ АНАЛІЗ МІЖНАРОДНОГО ТА НАЦІОНАЛЬНОГО ДОСВІДУ

*Б. В. Довгань, Т. В. Михайліна*

*Анотація.* У статті висвітлено проблеми, що виникають в інформаційно-правовому просторі та шляхи їх подолання. За допомогою діалектичного, кібернетичного, статистичного, формально-юридичного, порівняльно-правового методів наукового дослідження охарактеризовано досвід правового закріплення права на Інтернет та суміжних до нього прав на міжнародному рівні; здійснено порівняльно-правовий аналіз вітчизняного та зарубіжного регулювання відносин, що виникають у цифровому просторі. Запропоновано можливі шляхи удосконалення законодавчої бази України у питанні інформаційно-технічних прав з акцентом на права, що виникають в мережі.

*Ключові слова:* інформаційні права, право на доступ до Інтернет, цифровий простір, інформаційно-технологічні відносини.

**Вступ.** Науково-технічна революція кінця ХХ – початку ХХІ століття спричинила значні зміни у свідомості людини, а це призвело до появи нового покоління прав – четвертого, у якому виділяють інформаційні права. Їх визначають як сукупність прав, тісно пов'язаних з розвитком інформаційно-комунікаційних технологій, глобального інформаційного простору та формуванням інформаційного суспільства [1, с. 156]. Попри те, що цифрові технології швидкими темпами впроваджуються в усі сфери суспільного життя, на законодавчому рівні вони майже не закріплені, що породжує низку проблем, пов'язаних з доступом до всесвітньої мережі, визначенням статусу суб'єктів відносин, що виникають у цифровому просторі, можливістю притягнення до відповідальності порушників авторських чи/або суміжних прав в Інтернеті, забезпеченням кібербезпеки тощо. Для того, щоб зрозуміти, в якому напрямку рухатися Україні, аби досягнути

гармонійного формування інформаційно-технічного суспільства, слід простежити розвиток цієї сфери на міжнародному рівні та у провідних зарубіжних країнах.

Варто зазначити, що проблемі визначення специфіки природи інформаційних прав як складових четвертого покоління присвятили свої праці О. О. Барабаш, С. Б. Булеца, І. Діордіца, Ю. А. Дмитрієва, О. Жидкова, О. М. Калітенко, М. В. Коваль, О. Г. Кушніренко та інші. Окремі проблеми, пов'язані з цією сферою, та шляхи їх вирішення висвітлювали К. І. Беляков, А. О. Костенко, В. Л. Ортинський, К. П. Романюк. Аналіз особливості зарубіжних моделей регулювання цифрового простору зустрічається у роботах Г. Грігорянц, О. О. Золотар, О. О. Потерейко, В. А. Ромашенка та інших. Однак комплексного підходу до пошуку шляхів нормативного врегулювання проблем в інформаційно-технічному середовищі в Україні на прикладі аналізу досвіду міжнародної спільноти та зарубіжних держав досі не було. Саме цьому присвячена наукова стаття.

**Основний розділ.** Міжнародна спільнота має позитивний досвід правового регулювання «технічного» боку функціонування Інтернет-мережі. Вперше питання управління всесвітньою павутиною було обговорене Робочою групою з управління Інтернетом (тимчасовий орган при ООН) у 2004–2005 рр. Це призвело до створення кількох провідних міжнародних організацій (ICANN, IANA, ISOC, IETF, IGF та інші), які контролюють основні процеси діяльності в Інтернеті (розробка та запровадження нових користувацьких доменів вищого рівня, управляє системою нумерації і адресації тощо) [2, с. 116]. Першим значним міжнародним документом, який порушив питання, пов'язані з Інтернет-сферою, була *Окінавська хартія глобального інформаційного суспільства* (20 липня 2000 р.), яка проголошувала, що держава повинна гарантувати такі умови розвитку суспільству, які б забезпечували створення глобального інформаційного суспільства. Значний внесок у розвиток цифрового права внесла *Європейська Декларація про свободу комунікацій в Інтернет*, прийнята в місті Страсбурзі 28 травня 2003 р. з метою досягнення балансу між мережевою свободою слова та інформації та іншими правами, що гарантуються Конвенцією про захист прав людини і основних свобод (4 листопада 1950 р.) [3, с. 341]. У 2003 році був проведений Всесвітній саміт з питань інформаційного суспільства, результатом якого стало прийняття *Женевської Декларації принципів* [4], у якій визначено необхідність регулювання відносин у мережі, оскільки «Інтернет перетворився в загальнодоступний глобальний засіб, і управління його використанням повинне стати одним з основних питань порядку денного інформаційного суспільства» [3, с. 341]. І лише 12 березня 2012 року Рада Європи прийняла Стратегії про управління Інтернетом на період 2012–2015 роки. А 5 липня 2012 р. резолюція ООН закріпила право на свободу слова в Інтернеті. Як зазначає агентство Reuters, ця подія є історичною, адже цей документ забезпечує невід'ємне право людини на доступ до всесвітньої мережі, яке не може бути ніким обмежене [3, с. 342].

В Україні на законодавчому рівні право на доступ до Інтернету ще досі не закріплене. У зв'язку з активним розвитком новітніх технологій 15 жовтня 2019 р. депутати профільного комітету Міністерства цифрової трансформації України внесли законопроект «Про електронні комунікації», яким планується закласти фундамент реалізації концепції створення широкосмугового доступу до Інтернету, а також закріпити право на Інтернет шляхом оновлення переліку універсальних електронних комунікаційних послуг, серед яких доступ до таких сервісів: електронна пошта, пошукові системи, інструменти навчання, Інтернет-газети та новини, е-урядування, Інтернет-банкінг, соціальні медіа, відеодзвінки. Пропонується встановити субсидію на Інтернет особам, у яких середньомісячний сукупний дохід сім'ї в розрахунку на одну особу за попередні шість місяців не перевищує величини доходу, який дає право на податкову соціальну пільгу (2 690 гривень на особу) [5, с. 35–36]. Верховна Рада України 16.06.2020 р. у першому читанні проголосувала за даний законопроект (248 нардепів), але коли він буде остаточно прийнятий поки що не відомо [6].

Аналізуючи перспективи розвитку інформаційних прав в Україні, не можна не згадати про Японію, яка не просто на законодавчому рівні закріпила право на доступ до мережі, а й активно заохочує розвиток інформаційних прав в усіх сферах суспільного життя. Держава рухається у напрямку розробки цифрових технологій та вдосконалення системи управління і важелів правового регулювання, постійного дослідження проблеми втілення інформаційних догм на фоні їх переваг та недоліків. Віртуалізація країни відбувається за принципом ієрархічної піраміди й складається з трьох елементів: *on* (вдячність), *gigi* (відповідальність), *wa* (гармонія). Японські дослідники давно зрозуміли, що втілення правових стандартів у регулювання інформаційного суспільства необхідно так само, як і втілення цифрових технологій в реальне життя. Тому була прийнята Програма ініціативи щодо створення мережі INTERNET, яка передбачала проведення Інтернету в усі школи, розвиток електронної комерції з урахуванням американської стратегії глобалізації інформаційної інфраструктури, глобалізацію стандартів взаємодії [7, с. 15–16]. Саме таку модель регламентації інформаційних прав може взяти за основу Україна як зразкову. Однак, як відомо, економічний потенціал двох держав суттєво відрізняється, тому для створення такого інформаційного суспільства, як у Японії, нашій країні потрібні належна підготовка, час, ресурси, професійні кадри та готовність населення до змін.

Наразі стоїть питання про вирішення нагальних проблем. Тут слід згадати законопроект «Про внесення доповнень до Цивільного кодексу України (щодо гарантування права фізичної особи на доступ до Інтернету)» від 14.05.2015 р., де було запропоновано доповнити ст. 302 ЦК таким положенням: «Фізична особа має право на доступ до Інтернету. Право фізичної особи на доступ до Інтернету не може бути обмежене. Обмеження доступу до певних даних, що містяться у Інтернеті, можливо лише на підставі рішення суду про незаконність таких даних» [8, с. 41–42]. Фактично ця стаття мала на меті закріпити право кожного на доступ до Інтернету, натомість породила низку питань: яким чином це право має бути реалізоване, які можуть бути обмеження, як це право буде захищене тощо. З цього випливає, що для гармонійного розвитку інформаційних прав у суспільстві замало лише закріплення самого права на доступ. Потрібно також нормативно врегулювати відносини, що виникають у цифровому просторі. У чому ж полягає їх специфіка?

Систему правовідносин, що виникають в інформаційно-технічній сфері складають такі елементи: **суб'єкти**, до яких входять *пред'явники контенту* (величезні корпорації (Google, Microsoft) або особа, що створила сайт), *постачальники* (провайдери) та *клієнти* (фізичні або юридичні особи, які користуються мережею) [9, с. 135]. При цьому встановити їх дієздатність, місцезнаходження, та з'ясувати, чи це взагалі жива істота, а не програма-робот, досить проблемно [10, с. 53]; **об'єкти** – блага (що мають цінність тільки в мережі; що мають цінність тільки за її межами; що мають цінність повсюди); **зміст** є найпроблемнішим елементом визначення, так як права та обов'язки сторін визначаються за їх згодою без контролю держави [10, с. 54–57].

Таким чином, саморегуляція відносин у цифровому просторі є причиною того, що збільшується злочинність у цій сфері, адже досить важко встановити особу злочинця, щоб притягнути її до юридичної відповідальності та відновити порушені права. Це говорить про необхідність створення державних механізмів протидії такому явищу. Однак, щоб зрозуміти, яким чином це має відбуватися, доцільно дослідити практику зарубіжних країн.

Першою важливою проблемою, пов'язаною із інформаційно-технічними правовідносинами, є визначення правового статусу їх учасників – провайдерів та користувачів [11, с. 82].

У Канаді у разі порушення авторських та/або суміжних прав провайдер зобов'язаний направляти абоненту повідомлення та контролювати його діяльність певний час, поки право не буде відновлене, однак усувати контент можна лише на підставі рішення суду. У Франції такі суб'єкти під час складання та підписання договору про послуги зі своїми

клієнтами зобов'язані включити пункти про законні способи споживання цифрового продукту, про відповідальність за нелегальні дії в мережі, про методи захисту Інтернет-з'єднання. У разі порушення прав він направляє правопорушнику попереджувальний лист і направляє позов до суду. У ФРН суб'єкт порушеного авторського й суміжного права може звернутися до суду з проханням надання провайдером назви та адреси відповідної особи – можливого порушника. У США та Ірландії передбачений механізм припинення доступу до підозрілого матеріалу, а також схема відповідальності самого провайдера за порушення авторського права в мережі [11, с. 82–84].

Ще однією проблемою є забезпечення кібербезпеки. Наша держава ратифікувала Конвенцію Ради Європи про кіберзлочинність, Загальну декларацію прав людини, Міжнародний пакт про громадянські та політичні права, Міжнародний пакт про економічні, соціальні та культурні права, Конвенцію проти катувань та інших жорстоких, нелюдських або таких, що принижують гідність, видів поводження і покарання та інші міжнародні правозахисні акти [12, с. 196; 13, с. 148–149]. Тому загалом законодавство нашої держави відповідає міжнародним стандартам у цьому питанні.

Щодо вітчизняних нормативно-правових актів, то в Україні це питання врегульоване Законами України «Про національну безпеку України» від 21 червня 2018 р., «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. [14]. Стратегія кібербезпеки України від 15 березня 2016 р. закріплює принципи, на яких має ґрунтуватися інформаційне суспільство: верховенство права і повага до прав та свобод людини і громадянина; забезпечення національних інтересів України; відкритість, доступність, стабільність та захищеність кіберпростору; пріоритетність запобіжних заходів та ін. [15]. Однак самих лише принципів недостатньо для протистояння кіберзагрозам.

Загалом національну систему кібербезпеки творить низка державних органів: Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України (у 2015 р. запрацювала кіберполіція) тощо [13, с. 161–162]. У 2016 р. було утворено Національний координаційний центр кібербезпеки [13, с. 172]. Однак, незважаючи на розгалужену систему правоохоронних органів, рівень кіберзлочинності в Україні лише зростає. Так, масштабні хакерські атаки розпочалися у 2017 році запуском вірусу Petya, який заблокував діяльність аеропорту «Бориспіль», ЧАЕС, Укртелекому, Укрпошти, Ощадбанку, Укрзалізниці та низки інших великих підприємств [16, с. 149]. Загалом, у 2017 було зафіксовано 1795 справ, у 2018 – 1023, у 2019 – 4263 [17, с. 9]. Тобто, з того часу злочинність у цій сфері зросла у 2,4 рази.

Проте ця тенденція притаманна не лише для України, а й для багатьох провідних країн світу. Так, США, які у сфері розповсюдження персональних комп'ютерів, цифрової телефонії випереджають навіть Японію – «Мекку використання найсучасніших ІТ-технологій» [18, с. 287], регулярно стає жертвою злочинної кібердіяльності терористів. Саме тому було розроблено Стратегію кібербезпеки, яка спрямована на унормування обов'язків правоохоронних органів щодо затримання, переслідування злочинців, знищення кримінальної інфраструктури, обмеження розповсюдження та використання шкідливих кіберможливостей, попередження діяльності кіберзлочинців і їхніх спонсорів; на залучення до процесу віртуалізації уряду нового суб'єкта – постачальника інформаційно-комунікативних технологій, який на рівні з керівниками підрозділів органів державної влади повинен нести відповідальність за безпеку користування інформаційно-комунікативними технологіями [13, с. 127–129].

Особливістю Стратегії Польщі є те, що в ній закріплено необхідність розглянути можливість правового регулювання так званих програм «bug bounty», завдяки яким люди можуть вносити корективи до роботи певної програми, виправляючи помилки та отримуючи винагороду [13, с. 132].

Більш радикальною є програма забезпечення кібербезпеки КНР, яка полягає у суворій регламентації порядку надання населенню доступу до Інтернету. Передусім потрібно отримати платну ліцензію і вказати, які мережеві ресурси планується відвідувати – іноземні чи вітчизняні [7, с. 17]. За даними Грега Уолтона з Міжнародного центру з прав людини та демократичного розвитку, Китай реалізував найскладнішу фільтрацію Інтернет-контенту, що здатна ефективно відслідковувати контент з використанням безлічі методів регулювання і технічного контролю (блокування IP-адрес, скидання з'єднання тощо) (Проект «Великий брандмауер Китаю», 2003 р.) [19, с. 162].

**Висновки.** Отже, для гармонійного розвитку інформаційних прав у суспільстві замало лише закріплення самого права на доступ до Інтернету. Також потрібно нормативно врегулювати відносини, що виникають у цифровому просторі, передусім визначити правовий статус їх учасників – провайдерів і користувачів. За зразком Канади, Франції, ФРН, США, Ірландії, нашої країні необхідно надати провайдерам повноваження та одночасно обов'язок зберігати особисті дані користувачів (наприклад, електронна пошта, ID-адреса пристрою, з якого здійснюється вхід в мережу), щоб у разі порушення авторських чи/або суміжних прав мати можливість ідентифікувати особу. При цьому можливість примусити цього суб'єкта видаляти контент чи нести юридичну відповідальність залишається лише за судом.

Аналіз досвіду провідних зарубіжних держав щодо забезпечення кібербезпеки показав, що Україні потрібно підвищувати ефективність правоохоронних органів, які сьогодні не в змозі протистояти кібератакам. А також залучити до вирішення цього питання IT-фахівців (постачальника інформаційно-комунікативних технологій), у тому числі IT-бізнесу, кіберцентрів та кіберспільнот (як це роблять США), що здатні створювати потужні програми захисту, знешкоджувати загрози, можуть посприяти формуванню в Україні ефективної кіберрозвідки тощо. Державі варто нарешті усвідомити, що в питанні забезпечення кібербезпеки самих лише принципів та пріоритетів замало, потрібний чіткий план дій та готовність протистояти нападам. Із цього випливає, що Україні потрібно збільшувати кількість IT-спеціалістів. Для цього доцільно говорити про:

- переформатування системи вищої освіти в Україні, головним завданням якої має бути підготовка IT-спеціалістів, здатних виготовляти самостійний програмний продукт, а не лише виконувати аутсортингові функції [20, с. 79];

- перешкоджання їх виїзду за кордон (причини – відсутність можливості самореалізації в нашій державі, висока заробітна плата працівників IT-сфери на закордонному ринку зайнятості, кращі умови життя та праці тощо) за рахунок створення відповідних стимулів та гарантій, але не заборон;

- державне заохочення IT-спеціалістів до удосконалення IT-сфери України, що може бути реалізоване шляхом забезпечення їх працевлаштування після закінчення ВНЗ, збільшення заробітних плат, розробки програм сприяння малому та середньому бізнесу (для фахівців та підприємців IT-сфери) тощо.

Таким чином, лише комплексний підхід до регламентації інформаційних прав та врегулювання цифрового простору сприятиме формуванню інформаційно-технічного суспільства в Україні.

*Аннотація.* В статье раскрыты проблемы, возникающие в информационно-правовом пространстве и пути их преодоления. С помощью диалектического, кибернетического, статистического, формально-юридического, сравнительно-правового методов научного исследования охарактеризованы опыт правового закрепления права на доступ к Интернету и смежных ему прав на международном уровне; осуществлён сравнительно-правовой анализ отечественного и зарубежного регулирования отношений, возникающих в цифровом пространстве. Предложены возможные пути усовершенствования законодательной базы Украины в вопросе информационно-технических прав с акцентом на права, возникающие в сети.

*Ключевые слова:* информационные права, право на доступ к Интернет, цифровое пространство, информационно-технологические отношения.

*Abstract.* An article clarifies problems that occur in informational and legal space and ways of their solution. With the help of dialectical, cybernetic, statistical, formal and legal, comparative and legal methods of scientific research the experience of legal law fixing in the Internet and adjacent on international level is characterized. The comparative and legal analysis of national and foreign relationships regulation that that occur in informational space is done. The possible ways of Ukrainian legislative framework development is offered from the view of informational and technical rights with an accent on the particular rights that arise in the network.

*Key words:* informational rights, the right to access to the Internet, digital space, informational and technical relationships.

## СПИСОК ЛІТЕРАТУРИ

1. Вакарюк Л. Основні підходи до розуміння поняття «інформаційні права людини». *Підприємництво, господарство і право*. 2018. № 2. С. 155–159.
2. Гуцу С. Ф. Правове регулювання мережі Інтернет: міжнародний і вітчизняний досвід. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право*. 2018. Вип. 2 (38). С. 114–118.
3. Супрун О. В. Право на доступ до Інтернету: поняття та міжнародно-правове регулювання. *Міжнародні читання з міжнародного права пам'яті професора П.Є. Казанського*: матер. третьої міжнар. наук. конф. (м. Одеса, 2–3 листопада 2012 р.). Одеса: Фенікс. 2012. С. 339–342.
4. Підсумкові документи Всесвітнього саміту з питань інформаційного суспільства. *Державний комітет телебачення і радіомовлення України*. URL: [http://comin.kmu.gov.ua/control/uk/publish/printable\\_article?art\\_id=61592](http://comin.kmu.gov.ua/control/uk/publish/printable_article?art_id=61592) (дата звернення 19.09.2020).
5. Васильченко О. П. Право на доступ до мережі: надати не можна позбавити. *Науковий вісник Міжнародного гуманітарного університету*. Сер.: Юриспруденція. 2019. № 41. Том 1. С. 34–37.
6. Офіційний сайт Верховної Ради України. URL: [http://w1.c1.rada.gov.ua/pls/zweb2/webproc4\\_1?pf3511=68059](http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68059).
7. Ромащенко В. А. Азійська модель правового регулювання інформаційного суспільства. *Юридичний науковий електронний журнал*. 2016. №5. С. 15–18.
8. Головкин О. М. Цифрова культура та інформаційна культура: права людини в епоху цифрових трансформацій. *Інформація і право*. 2019. № 4(31). С. 37–44.
9. Коваленко О. Ю. Особливості правовідносин в Інтернеті. *Актуальні проблеми вітчизняної юриспруденції*. 2017. Спецвип. Ч. 1. С. 134–137.
10. Беляков К. І. Понятійні та методологічні основи регулювання нових типів інформаційних відносин: «віртуальні правовідносини». *LEX PORTUS*. 2016. № 2. С. 47–63.
11. Грігорянц Г. Правовий статус провайдера за законодавством зарубіжних країн. *Юридичний вісник*. 2016. №4. С. 82–90.
12. Романюк К. П. Правові проблеми захисту авторського права і суміжних прав від Інтернет-піратства в Україні. *Збірник наукових рефератів магістрів юридичного факультету національної академії управління – 2017*. 2017. С. 194–205.
13. Потерейко О. О. Віртуалізація держави: теоретико-методологічний аналіз: дис. ... канд. юрид. наук: 23.00.01. Львів, 2019. 201 с.
14. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р., № 2163-VIII. Відомості Верховної Ради. 2017. № 45. Ст. 403.
15. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 березня 2016 року, № 96/2016. URL: <https://zakon.rada.gov.ua/laws/show/96/2016#n11> (дата звернення 19.08.2020).
16. Ортинський В. Л. Основні засади забезпечення кібербезпеки України. *ІТ-право: проблеми та перспективи розвитку в Україні*: зб. матер. II-ї Міжнар. наук.-практ. конф. (17 листопада 2017 р.). Львів, 2017. С. 149–151.
17. Звіт Голови Національної поліції України про результати роботи відомства у 2019 році. С. 1–12. URL: [www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit\\_2019/zvit-npu-2019.pdf](http://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit_2019/zvit-npu-2019.pdf).
18. Золотар О. О. Правові основи інформаційної безпеки людини: дис. ... канд. юрид. наук: 12.00.07. Київ, 2018. 499 с.
19. Радейко Р. І. Міжнародна практика блокування доступу до інформаційних ресурсів у мережі Інтернет. *ІТ-право: проблеми та перспективи розвитку в Україні*: зб. матер. II-ї Міжнар. наук.-практ. конф. (17 лист. 2017 р.). Львів, 2017. С. 160–166.
20. Єршов М. О. Роль української ІТ-освіти на світовому ринку інформаційних товарів і послуг. *Науковий вісник*. 2018. № 16. С. 74–81. URL: <https://doi.org/10.32835/2223-5752.2018.16.74-81>.