

АКТУАЛЬНІ ПРОБЛЕМИ ЦИВІЛІСТИКИ

УДК 34:004.056

DOI <https://doi.org/10.32782/2409-4544/2025-1/8>

КІБЕРБЕЗПЕКА: АКТУАЛЬНИЙ СТАН НОРМАТИВНО-ПРАВОВОЇ БАЗИ ТА ПЕРСПЕКТИВИ ЇЇ РОЗВИТКУ

Книш Зоряна Ігорівна,

кандидат юридичних наук, доцент,
доцент кафедри цивільно-правових дисциплін
Волинського національного університету імені Лесі Українки
ORCID ID: 0000-0002-6548-3301

Стаття присвячена аналізу чинної нормативно-правової бази забезпечення кібербезпеки в інформаційному просторі у сучасних умовах. Аналізуються підходи до визначення кібербезпеки й окреслюються сучасні загрози в інформаційному просторі.

Аналізуються положення нормативно-правових актів, що регулюють відносини у кіберпросторі, які детермінують необхідність забезпечення кібербезпеки.

Формується висновок, що Закон України «Про основні засади забезпечення кібербезпеки України» виступає лише першим кроком і базою для більш глобальної законодавчої роботи у напрямку формування спеціального нормативного матеріалу із забезпечення кібербезпеки. Визначаються фактори, що детермінували актуальний стан нормативно-правової бази забезпечення кібербезпеки, якими виступили: 1) стрімкий розвиток інформаційних технологій й їх впровадження у всі сфери суспільного життя; 2) активна еволюція загроз кібербезпеці, тобто форм використання інформаційних систем у протиправних цілях і при цьому на усіх рівнях злочинної діяльності; 3) відсутність сформованої практики правового регулювання відповідних відносин, здатної не лише оперативно реагувати на зміни у системі основних загроз кібербезпеці, проте й також швидко еволюціонувати відповідно до розвитку загроз у кіберпросторі.

Встановлюється, що у зв'язку з інтегративним (інтегральним) характером феномену кібербезпеки, визначеним масштабами інформатизації усіх сфер суспільного життя, нормативно-правові положення, спрямовані на її забезпечення мають як публічно-правову, так і приватно-правову природу і відносяться до галузей цивільного, фінансового, адміністративного та іншого права. Ця обставина, своєю чергою, визначає в якості наступного етапу еволюції законодавства із забезпечення кібербезпеки його галузевий розвиток на рівні спеціальних нормативних положень і у контексті окремих сфер суспільних відносин.

Ключові слова: кібербезпека, кіберпростір, кіберсередовище, кіберзахист, кіберправо, інформаційне право, діджиталізація, інформатизація, безпека даних, кіберзлочинність, комунікативні системи, соціальні мережі, Інтернет, критична інфраструктура, оборона, національні інтереси, публічні інтереси, приватні інтереси, право на інформацію.

Knysh Zoriana. Cyber security: current state of the regulatory framework and prospects for its development

The article deals with the current regulatory and legal framework for ensuring cyber security in the information space within modern conditions. Approaches to defining cyber security are analyzed modern threats in the information space are outlined.

The provisions of regulatory and legal acts regulating relations in cyberspace that determine the need to ensure cyber security are analyzed.

It is stated that the Law of Ukraine "On the Basic Principles of Cyber security in Ukraine" is the first step and the basis for more global legislative work towards forming special regulatory material on ensuring cyber security. The factors that determined the current state of the regulatory and legal framework for ensuring cyber security are identified, which were: 1) the rapid development of information technologies and their implementation in all spheres of public life;

2) the active evolution of the cyber security threat, i.e. the forms of using information systems for illegal purposes and at all levels of criminal activity; 3) reflect the established practices of legal regulation of relevant relations, capable not only of promptly responding to changes in the system of special cyber security threats but also of rapidly evolving following the development of threats in cyberspace.

Determined that due to the integrative (integral) nature of the cyber security phenomenon, determined by the scale of informatization of all spheres of public life, the regulatory and legal provisions aimed at its provision have both public and private law nature and relate exclusively to the branches of civil, financial, administrative and other law. This circumstance, in turn, contributes to the next stage of the evolution of legislation on cyber security, its sectoral development at the level of special regulatory provisions, and in the context of individual spheres of public relations.

Key words: cyber security, cyberspace, cyber environment, cyber defense, cyber law, information law, digitalization, informatization, data security, cybercrime, communication systems, social networks, Internet, critical infrastructure, defense, national interests, public interests, private interests, right to information.

В умовах активного інформаційного розвитку суспільства й впровадження новітніх технологій у всіх сферах суспільного життя, починаючи від оборони і завершуючи побутом, забезпечення кібербезпеки стає однією з найбільш важливих проблем сучасності.

Водночас впровадження ефективної системи кібербезпеки значною мірою залежить від нормативно-правової бази, яка створює умови для активного використання засобів протидії загрозам у кіберпросторі. Адже саме від неї багато у чому залежить те, наскільки оперативно та ефективно держава, а також інші учасники інформаційних відносин зможуть убезпечуватись від відповідних небезпек, а також протидіяти їм та реагувати на спричинювані відповідними протиправними діями негативні наслідки.

Питання правового забезпечення кібербезпеки в умовах сучасних викликів, а також особливості актуального стану нормативно-правової бази регулювання відповідної сфери суспільних відносин ставали предметом розгляду таких вчених-правників як О. Бакалинський, О. Бакалінська, П. Біленчук, В. Богом'я, В. Веремчук, В. Галунько, С. Деніжна, І. Доронін, С. Єсімов, С. Кавин, Х. Кайдрович, І. Каріх, Ю. Кемська, С. Князь, М. Ковалів, І. Коропатнік, І. Красницький, В. Луцюк, Ю. Назар, В. Новицький, Т. Обіход, А. Омельченко, В. Пахомов, М. Плєскач, В. Пядишев, Д. Рєпін, В. Роллер, Р. Скриньковський, М. Сова, Т. Созанський, А. Тарасюк, Н. Туз, Д. Хом'яков, Г. Яремко та ін.

Метою статті є визначення особливостей сучасного стану нормативно-правової бази забезпечення кібербезпеки в актуальних умовах й встановлення можливих векторів її розвитку.

1. Загальні правові положення про кібербезпеку та основні загрози у кіберпросторі

У сучасній юридичній доктрині, а також у положеннях нормативно-правових актів отримало закріплення декілька підходів до розуміння кібербезпеки, які умовно можна диференціювати на інструментальні та результативні (станові). Перші характеризують кібербезпеку як діяльність або ж процес, спрямований на досягнення певного безпекового результату, у той час як другі – як власне результат відповідної діяльності або процесу. У сутності йдеться про один і той самий феномен, який розглядається у різних аспектах.

У межах інструментального підходу кібербезпека визначається, зокрема як сукупність інструментів, політик, концепцій та гарантій безпеки, а також рекомендацій, методів управління ризиками, актів поведінки, провідного досвіду, страхування і технологій, що можуть бути використані для захисту активів організацій та користувачів у кіберсередовищі [1, с. 13].

У той же час «результативний» або ж «становий» підхід отримав закріплення у положеннях Закону України «Про основні засади забезпечення кібербезпеки України» згідно з якими кібербезпекою є захищеність життєво важливих інтересів людини і громадянина, суспільства та дер-

жави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі (пункт 5 частини першої статті 1) [2, ст. 1].

Зв'язок кібербезпеки з комунікативними системами, пов'язаними з мережею Інтернет, тобто, у сутності, з інформаційними у тому числі у широкому розумінні системами сприяє вживанню терміну «кібербезпека», зокрема у синонімічному ключі з термінами «безпека інформації» та «інформаційна система» [3, с. 101]. Водночас, урахувавши те, що важливою і невідворотною тенденцією сьогодення виступає діджиталізація усіх сфер суспільного життя і у першу чергу державних сервісів, й при цьому процес «інформатизації», як стверджується, є більш широким за змістом, ніж процес діджиталізації [4, с. 158], кіберпростір у сучасних умовах охоплює практично усі сфери суспільного життя, яких торкнулася інформатизація і які при цьому пов'язуються з комунікативними системами. Саме тому, як справедливо стверджує А. В. Омельченко, активно еволюціонуючий цифровий світ потребує, зокрема ефективної національної системи кібербезпеки, що здатна у тому числі забезпечити можливості цифровізації усіх сфер суспільного життя [5, с. 144]. Її побудова та ефективне функціонування, вочевидь, повинні здійснюватися на належній нормативній основі.

Що ж стосується власне форм загроз на протидію яким повинна орієнтуватися нормативна база кібербезпеки, то ними виступають, зокрема шкідливе програмне забезпечення (віруси), ботнет, програмивимагачі, фізичне пошкодження системи [1, с. 13], викрадення особистої інформації [6, с. 16] а ін.

Стосовно конкретних кейсів, які демонструють характер та масштаби сучасних кіберзагроз, то з цього приводу можна навести декілька прикладів. Одним із них виступає кібератака на навігаційні системи, що обслуговують порти Республіки Корея внаслідок чого відбулося переривання GPS-сигналу й передача невірної інформації щодо місцезнаходження мор-

ських суден внаслідок чого 280 торговельних кораблів були вимушені повернутися до портів [1, с. 13].

Також у кінці 2016 року вітчизняна енергетична система стала об'єктом кібератаки відомої як «BlackEnergy 3». Серед потужностей «Прикарпаттяобленерго» безпосереднім предметом атаки виступила, ймовірно автоматизована система керування технологічним процесом, що є різновидом інформаційних систем. Кібератака призвела до вимкнення близько 30 підстанцій внаслідок чого без електропостачання опинилося 230 тис. споживачів [6, с. 16].

2. Основні нормативно-правові акти

Основним законодавчим актом, що наразі регламентує відносини у сфері забезпечення кібербезпеки в Україні, виступає Закон України «Про основні засади забезпечення кібербезпеки України» [2].

На момент підготовки цього матеріалу Закон складається з п'ятнадцяти статей, а також прикінцевих та перехідних положень і при цьому не поділяється на розділи. Перші три статті Закону мають певною мірою «вступний» характер, оскільки значною мірою характеризують сам нормативно-правовий матеріал. Йдеться про терміни, принципам застосування Закону та «правові основи забезпечення кібербезпеки України» (у яких окреслюється характер джерел, що регулюють відповідні відносини, а також їх ієрархічна система у ході застосування) [2, статті 1–3].

Своєю чергою стаття 4 «Об'єкти кібербезпеки та кіберзахисту», стаття 5 «Суб'єкти забезпечення кіберзахисту», стаття 6 «Об'єкти критичної інфраструктури» та стаття 7 «Принципи забезпечення кібербезпеки» [2, статті 4–7] у сутності характеризують структуру правовідношення із забезпечення кібербезпеки, а також засади їх побудови та динаміки. Дві статті Закону (стаття 8 «Національна система кібербезпеки» та стаття 9 «Урядова команда реагування на комп'ютері надзвичайні події України CERT-UA» [2, статті 8–9]) присвячені інституційним аспектам вітчизняної системи кібербезпеки. Також у фокус положень Закону включено питання державно-приватної взаємодії у сфері кібер-

безпеки (стаття 10) та необхідності сприяння суб'єктам забезпечення кібербезпеки (стаття 11). Охоронних аспектів аналізованих відносин торкнулися бланкетне положення статті 12 Закону, якою визначаються види юридичної відповідальності за порушення законодавства у сфері забезпечення кібербезпеки, а також стаття 15 «Контроль за законністю заходів із забезпечення кібербезпеки України» [2, статті 10, 11, 12, 15]. Питання фінансового забезпечення заходів кібербезпеки отримало відображення у статті 13 Закону у той час як стаття 14 врегульовує відносини, пов'язані з міжнародною співпрацею у сфері кібербезпеки [2, статті 13, 14].

Закон України «Про основні засади забезпечення кібербезпеки України», як зазначають О. Бакалінська та О. Бакалинський, формує загальну архітектуру національної системи кібербезпеки, а також розподіляє завдання й розмежовує повноваження між основними суб'єктами забезпечення кібербезпеки до яких відносяться, зокрема Національний координаційний центр кібербезпеки, Міністерство оборони України, Служба безпеки України та інші суб'єкти [3, с. 104]. При цьому в якості позитивних сторін Закону, як зазначає А. В. Тарасюк, виступає офіційне введення у юридичний понятійно-категоріальний апарат таких понять як «кібербезпека», «кібератаки» та «кіберзахист» [7, с. 203].

Водночас у світлі окреслених положень важливе значення мають декілька обставин.

Першою виступає те, що норми Закону України «Про основні засади забезпечення кібербезпеки України» за колом відносин, яких вони так чи інакше торкаються, необхідно осмислювати у дещо ширшому контексті, зокрема в аспекті Закону України «Про національну програму інформатизації».

Перший із зазначених законодавчих актів прийнято у 2017 році, а другий – наприкінці 2022 року.

При цьому, як зазначається у статті 3 Закону України «Про національну програму інформатизації» національна програма інформатизації спрямована на забезпечення, зокрема впровадження та застосування інформаційно-комунікативних технологій у державному управлінні, міс-

цевому самоврядуванні та суспільному житті, створення та розвитку системи державних інформаційних ресурсів, рівного доступу до інформаційно-комунікативних технологій та підвищення рівня освіченості громадян з питань інформаційно-комунікативних технологій [8, ст. 3].

3. Проблемні аспекти

Наведені нормативні положення з урахуванням тенденцій розвитку суспільства дозволяють окреслити два основні вектори еволюції інформаційного законодавства, а тому і два напрямки ґенези нормативно-правової бази забезпечення кібербезпеки. Ними виступають відносини, пов'язані із суспільними та державними інтересами, а також відносини, в основі яких лежить приватний інтерес.

Зокрема, у тому числі у світлі назви Закону України «Про основні засади забезпечення кібербезпеки України» необхідно звернути увагу на статтю 4 Закону, якою в якості об'єктів кібербезпеки розглядаються у тому числі конституційні права і свободи людини і громадянина, а також, зокрема сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, держава та її конституційний лад, суверенітет, національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави (частина перша статті 4) [2, ст. 4]. Але важливо, що дія Закону, як зазначається в частині першій статті 2, не поширюється, зокрема на відносини та послуги, пов'язані із змістом інформації, що обробляється в комунікаційних системах та/або в технологічних системах, а також на соціальні мережі й приватні інформаційні ресурси в мережі Інтернет [2, ст. 2].

Відповідне положення отримує розвиток у частині другій статті 4 зазначеного Закону якою до об'єктів кіберзахисту відносяться, зокрема комунікаційні системи усіх форм власності, в яких обробляються національні інформаційні ресурси, що використовуються у тому числі в інтересах органів державної влади та військових формувань, а також комунікаційні системи, які використовуються для задоволення суспільних потреб, й об'єкти критичної інфраструктури [2, ст. 4].

Ці положення мають важливе практичне значення, адже у сутності вони досить

чітко фрагментують приватні та публічні відносини, на які поширюється Закон.

Інакше кажучи, положення Закону України «Про основні засади забезпечення кібербезпеки України» умовно розмежовують відносини, пов'язані з використанням комунікаційних систем, на публічні, тобто ті, що стосуються національних інтересів України, суспільних та державних інтересів, а також ті, що стосуються суто приватних інтересів. Тобто «життєво важливі інтереси людини і громадянина», як вважається, охоплюються Законом в тій частині, у якій вони входять до зазначених публічних інтересів.

Своєю чергою непоширення Закону на соціальні мережі й приватні інформаційні ресурси в мережі Інтернет означає що це питання залишається у сфері правового впливу інших актів.

І з цього приводу неможливо не відмітити, що у сучасних юридичних дослідженнях питання кібербезпеки осмислюється переважно у ключі захисту критичної інфраструктури [3, с. 105], а також в ключі оборонної функції держави [9, с. 108].

Водночас, приймаючи до уваги зазначене, не можна ігнорувати і того, що кібербезпека стосується також і діяльності суб'єктів господарювання у цілому [3, с. 105] і при цьому не лише електронної торгівлі [6, с. 16] тобто фінансових ринків, проте будь-якої активності у кіберпросторі взагалі, а тому фактично інтересів усіх категорій суспільства [10, с. 3]. У зв'язку з цим положення інформаційного права, спрямовані на забезпечення кібернетичної безпеки, за предметом регулювання можуть мати як публічно-правовий так і приватно-правовий характер [11, с. 203].

Звісно, охоплення відповідними положеннями приватних відносин, зокрема пов'язаних з корпоративними комунікаційними системами, соціальними мережами, а також приватним використанням мережі Інтернет має деліктний характер, адже йдеться у тому числі про право особи на інформацію та приватність. Однак, не можна ігнорувати того, що відповідні інформаційні права відносяться до четвертого покоління прав людини [12, с. 41–44], а тому їх забезпечення є нагальною умовою сучасності.

Висновки. Підводячи підсумки під викладеним вище, необхідно погодитися з вченими, які висловлюють переконаність у тому, що вітчизняна нормативно-правова база кібербезпеки перебуває лише у стані свого зародження [11, с. 203], а Закон України «Про основні засади забезпечення кібербезпеки України» є лише переважно «дорожньою картою» для формування спеціального нормативного матеріалу, а не всеосяжним актом, що регулює відносини у сфері кібербезпеки [7, с. 204]. Тобто це лише перший крок, база і свого роду «трамплін» для більш глобальної законодавчої роботи.

І проблема полягає не стільки в «недовершеності» нормативно-правового матеріалу, скільки у впливі на правотворчий процес декількох факторів, які унеможливили формування одразу комплексної й завершеної на даному історичному етапі розвитку системи нормативно-правових положень, що регламентують відповідні відносини. Такими факторами виступили: 1) стрімкий розвиток інформаційних технологій й їх впровадження у всі сфери суспільного життя; 2) активна еволюція загроз кібербезпеці, тобто форм використання інформаційних систем у протиправних цілях і при цьому на усіх рівнях злочинної діяльності; 3) відсутність сформованої практики правового регулювання відповідних відносин, здатної не лише оперативно реагувати на зміни у системі основних загроз кібербезпеці, проте й також швидко еволюціонувати відповідно до розвитку загроз у кіберпросторі.

Проте, чи не найбільш важливим фактором, який з одного боку визначив актуальний стан розвитку правової бази кібербезпеки, а з іншого – детермінує вектори її подальшої еволюції виступає інтегральний характер піднятої проблеми. Кібербезпека стосується усіх сфер суспільного життя у яких використовуються комунікаційні системи, а це, у сутності, усі сфери життя. І з цього слідує, що питання кібербезпеки охоплюється усіма галузями права внаслідок чого набуває відносно них інтеграційного характеру.

Саме у цьому знаходить підтвердження та обставина, що сучасна нормативно-правова база кібербезпеки пройшла лише перший етап свого становлення. В якості

наступного етапу необхідно розглядати її нормативних положень і у контексті окремих сфер суспільних відносин.

ЛІТЕРАТУРА:

1. Веремчук В. С. Міжнародно-правове регулювання кібербезпеки у морській галузі: сучасний стан та перспективи розвитку. *Вісник Одеського національного університету. Серія: Правознавство*. 2024. Т. 26, вип. 1 (38). С. 12–17.
2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403 (із змінами).
3. Бакалінська О., Бакалинський О. Правове забезпечення кібербезпеки в Україні. *Підприємство, господарство і право*. 2019. № 9. С. 100–107.
4. Духневич А. В., Спесівцев Д. С. «Юридичні інновації» як освітній компонент (навчальна дисципліна). *Юридичний науковий електронний журнал: електрон. наук. фахове вид.* 2023. № 4. С. 156–160. URL: http://lsej.org.ua/4_2023/37.pdf (дата звернення: 22.03.2025).
5. Омельченко А. В. Організаційно-правові засади забезпечення кібербезпеки України. *Київський часопис права*. 2021. № 3. С. 140–145.
6. Біленчук П., Обіход Т., Правове і наукове забезпечення кібербезпеки України. *Юридичний вісник України*. 2022. № 44–46 (1424–1426). С. 16–17.
7. Тарасюк А. В. Стан правового забезпечення кібербезпеки в Україні. *Наукові записки Львівського університету бізнесу та права. Серія Юридична*. 2019. Т. 13. С. 201–206.
8. Про Національну програму інформатизації: Закон України від 01.12.2022 р. № 2807-IX. *Офіційний вісник України*. 2023. № 2. Ст. 86.
9. Доронін І. М. Правове регулювання забезпечення кібербезпеки у реалізації окремих функцій держави. *Інформація і право*. 2017. № 1 (20). С. 104–111.
10. Sozanskyi T., Krasnytskyi I., Lutsyk V., Yaremko G., Tuz N. International practice of legal support of cyber security of the country. *Journal of Legal, Ethical and Regulatory Issues*. 2020. Vol. 23, Issue 2. URL: <https://www.abacademies.org/abstract/international-practice-of-legal-support-of-cyber-security-of-the-country-9137.html> (access date: 28.03.2025).
11. Плєскач М. В. Сутність поняття та основні елементи механізму адміністративно-правового забезпечення кібернетичної безпеки людини. *Часопис Київського університету права*. 2020. № 4. С. 201–209.
12. Маложон О. І. Четверте покоління прав людини в контексті української сучасності. *Юридичний науковий електронний журнал: електрон. наук. фахове вид.* 2021. № 12. С. 41–44. URL: http://lsej.org.ua/12_2021/7.pdf (дата звернення: 22.03.2025).

REFERENCES:

1. Veremchuk, V. S. (2024). Mizhnarodno-pravove rehuliuвання kiberbezpeky u morskii haluzi: suchasnyi stan ta perspektyvy rozvytku [International Legal Regulation of Cyber Security in the Maritime Industry: the Current State and Prospects for Development]. *Visnyk Odeskoho natsionalnoho universytetu. Serii: Pravoznavstvo*, 26(1), 12–17 [in Ukrainian].
2. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 r. № 2163-VIII [On the Basic Principles of Cybersecurity in Ukraine]. *Vidomosti Verkhovnoi Rady Ukrainy*, 45, 403 [in Ukrainian].
3. Bakalinska, O., & Bakalynskyi, O. (2019). Pravove zabezpechennia kiberbezpeky v Ukraini [Legal protection of cybersecurity in Ukraine]. *Pidpriemnytstvo, hospodarstvo i pravo*. 9, 100–107 [in Ukrainian].
4. Dukhnevych, A. V., & Spiesivtsev, D. S. (2023). «Iurydychni innovatsii» yak osvittii komponent (navchalna dystsyplina) [“Legal innovations” as educational component (academic discipline)]. *Iurydychnyi naukovyi elektronnyi zhurnal*, 4, 156–160. Retrieved from http://lsej.org.ua/4_2023/37.pdf [in Ukrainian].
5. Omelchenko, A. V. (2021). Orhanizatsiino-pravovi zasady zabezpechennia kiberbezpeky Ukrainy [Organizational and legal bases of cybersecurity of Ukraine]. *Kyivskyi chasopys prava*, 3, 140–145 [in Ukrainian].

6. Bilenchuk, P., & Obikhod, T. (2022). Pravove i naukovе zabezpechennia kiberbezpeky Ukrainy [Legal and scientific security of cybersecurity in Ukraine]. *Yurydychnyi visnyk Ukrainy*. 44–46 (1424–1426), 16–17 [in Ukrainian].
7. Tarasiuk, A. V. Stan pravovoho zabezpechennia kiberbezpeky v Ukraini [Cybersecurity Legal Security Center in Ukraine]. *Naukovi zapysky Lvivskoho universytetu biznesu ta prava. Seriia Yurydychna*, 13, 201–206 [in Ukrainian].
8. Pro Natsionalnu prohramu informatyzatsii: Zakon Ukrainy vid 01.12.2022 r. № 2807–IX [On the National Information Program]. *Ofitsiyni visnyk Ukrainy*, 2, 86 [in Ukrainian].
9. Doronin, I. M. (2017). Pravove rehuliuвання zabezpechennia kiberbezpeky u realizatsii okremykh funktsii derzhavy [Legal regulation of ensuring cybersecurity in the implementation of certain state functions]. *Informatsiia i pravo*, 1(20), 104–111 [in Ukrainian].
10. Sozanskyi, T., Krasnytskyi, I., Lutsyk, V., Yaremko, G., & Tuz, N. (2020). International practice of legal support of cyber security of the country. *Journal of Legal, Ethical and Regulatory Issues*. 23(2). Retrieved from <https://www.abacademies.org/abstract/international-practice-of-legal-support-of-cyber-security-of-the-country-9137.html>.
11. Pleskach, M. V. (2020). Sutnist poniattia ta osnovni elementy mekhanizmu administrativno-pravovoho zabezpechennia kibernetychnoi bezpeky liudyny [The mechanism of administrative and legal support of human cybersecurity: concept and basic elements]. *Chasopys Kyivskoho universytetu prava*, 4, 201–209 [in Ukrainian].
12. Malozhon, O. I. (2021). Chetverte pokolinnia prav liudyny v konteksti ukrainskoi suchasnosti [The Fourth generation of human rights in the context of Ukrainian modernity]. *Yurydychnyi naukovyi elektronnyi zhurnal*, 12, 41–44. Retrieved from http://lsej.org.ua/12_2021/7.pdf [in Ukrainian].