https://doi.org/10.25313/2617-572X-2023-7

Соціальна і гуманітарна політика

УДК 341.1+327.5

Горліченко Сергій Олександрович
науковий співробітник
Науково-дослідного центру
Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського"
Horlichenko Serhii
Researcher of the
Scientific Research Center
Institute of Special Communication and Information Protection
National Technical University of Ukraine
"Ihor Sikorsky Kyiv Polytechnic Institute"
ORCID: 0000-0002-8999-7526

НОРМАТИВНО-ПРАВОВІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КІБЕРПРОСТОРУ В КРАЇНАХ СВІТУ
REGULATORY AND LEGAL MECHANISMS FOR ENSURING CYBERSPACE SECURITY IN COUNTRIES OF THE WORLD

Анотація. *Вступ. Кібербезпека вважається однією з найактуальніших тем сучасного міжнародного права, вкрай важливою для забезпечення національної безпеки держав. Інформаційно-комунікаційні технології можуть бути використані з метою негативного впливу на економічні, соціальні, культурні та політичні відносини, завдати шкоди економічному, військовому, оборонному потенціалу держави та суспільства. У зв'язку з цим міжнародне суспільство виявляє серйозну зацікавленість у розробці багатосторонньої правової основи*

співробітництва в галузі кібербезпеки. Однак єдиний підхід до вирішення цього завдання на міжнародній арені поки так і не вироблений, оскільки складність правового регулювання кіберпростору обумовлена віртуальною характеристикою відносин, що складаються в цій сфері.

Метою дослідження є аналіз особливостей правового регулювання забезпечення кібербезпеки в різних країнах світу в системі міжнародної безпеки.

Матеріали і методи. Матеріалами дослідження є: 1) нормативно-правове забезпечення щодо регулювання безпеки кіберпростору; 2) праці вітчизняних та зарубіжних авторів, що провадять свої науково-практичні дослідження у сфері кібербезпеки.

Результати. У науковій статті розкрито послідовність формування нормативно-правових механізмів забезпечення безпеки кіберпростору. Розглянуто домінуючі ідеї щодо влаштування кіберпростору та проблеми формулювання міжнародного права про кіберпростір, котрі пов'язані з основними принципами та характеристиками міжнародного публічного права. Приділяється увага впливу цифрового суверенітету на розвиток міжнародного законодавства про кіберпростір. Визначено що створення норм, що регулюють діяльність в кіберпросторі, потребує врахування таких аспектів, як забезпечення кібербезпеки, захист особистих даних, боротьба з кіберзлочинами та кібертероризмом.

Перспективи. На підставі аналізу міжнародного законодавства вказано напрями які потребують поліпшення у сфері забезпечення безпеки кіберпростору в сучасних умовах.

Для забезпечення ефективного захисту кіберпростору важливо продовжувати розвивати міжнародне законодавство та створювати нові технологічні та організаційні інструменти для забезпечення кібербезпеки.

***Ключові слова**: кіберпростір, кібербезпека, інформаційна безпека, кіберзагрози, інформаційно-комунікаційні технології, кіберзлочинність, міжнародне право.*

***Summary.** Introduction. Cyber security is considered one of the most relevant topics of modern international law, extremely important for ensuring the national security of states. Information and communication technologies can be used to have a negative impact on economic, social, cultural and political relations, to harm the economic, military and defense potential of the state and society. In this regard, the international society shows a serious interest in the development of a multilateral legal framework for cooperation in the field of cyber security. However, a unified approach to solving this task in the international arena has not yet been developed, since the complexity of the legal regulation of cyberspace is due to the virtual characteristics of relations in this area.*

The purpose of the study is to analyze the peculiarities of the legal regulation of cyber security in different countries of the world in the system of international security.

Materials and methods. The research materials are: 1) regulatory and legal support for the regulation of cyberspace security; 2) works of domestic and foreign authors conducting scientific and practical research in the field of cyber security.

The results. The scientific article reveals the sequence of formation of regulatory and legal mechanisms for ensuring the security of cyberspace. The dominant ideas regarding the arrangement of cyberspace and the problems of formulating international law on cyberspace, which are related to the main principles and characteristics of international public law, are considered. Attention is paid to the influence of digital sovereignty on the development of international legislation on cyberspace. It was determined that the creation of

norms regulating activities in cyberspace needs to take into account such aspects as ensuring cyber security, protecting personal data, fighting cybercrimes and cyberterrorism.

Prospects. On the basis of the analysis of international legislation, directions that require improvement in the field of ensuring cyberspace security in modern conditions are indicated.

To ensure effective protection of cyberspace, it is important to continue to develop international legislation and create new technological and organizational tools to ensure cyber security

Key words: *cyber space, cyber security, information security, cyber threats, information and communication technologies, cyber crime, international law.*

Вступ. У науковій літературі кіберпростір часто помилково асоціюється з Інтернетом. Однією з причин цієї помилки є відсутність єдиного визначення поняття «кіберпростір». У той же час Міністерство оборони США вважає, що кіберпростір – це «…сфера, що характеризується можливістю використання електронних та електромагнітних засобів для запам'ятовування, модифікування та обміну даними через мережеві системи та пов'язану з ними фізичну інфраструктуру» [1]. У Китаї 7 листопада 2016 року було прийнято Закон про кібербезпеку, що регламентує дії постачальників мережевих продуктів та послуг зі збирання, зберігання та обробки даних користувача; порядок та специфіку забезпечення безпеки інформаційної інфраструктури у стратегічно важливих галузях. Головною метою ухвалення Закону проголошується захист національного «кіберсуверенітету» КНР [2].

Аналіз останніх досліджень і публікацій. Проблемні питання щодо міжнародного співробітництва у сфері забезпечення безпеки кіберпростору перебували у фокусі уваги таких науковців як Башак К. [8], Бабакін В.М.

[16], Грайворонський М.В. [19], Поляков О.М. [26], Лук'янчикова В. Ю. [28]. Серед тем, що були розглянуті авторами, велике значення приділено теоретичним аспектам різних питань, що стосуються інституту міжнародної інформаційної безпеки, а також обговоренню питань співпраці в межах регіональних міжнародних організацій.

Процес формування стратегії кібербезпеки Європейського Союзу знаходиться під увагою науковців Забара І.М [27], Грубінко А. [29], Орлов О.В. [21], Оніщенко Ю.М.. Серед основних аспектів, на які вони акцентують увагу, включають загальну юридичну стратегію ЄС щодо протидії кіберзлочинності, міжнародну співпрацю в галузі кібернетичної та інформаційної безпеки, боротьбу з кіберзлочинами, а також конкретні ізольовані випадки кіберзлочинів.

У науковій літературі зустрічається справедливе твердження про те, що проблематика кіберпростору в цілому, і кібербезпеки зокрема, актуалізувалася в результаті війни в Перській затоці 1990 – 1991 рр., у ході якої використання новітніх військових технічних досягнень супроводжувалося потужною інформаційною кампанією та висвітленням у пресі [3].

Після зазначених подій вчені та політики стали переосмислювати поняття «інформаційна війна», «кібервійна». Кіберпростір стали розглядати як «п'ятий простір», що використовується для досягнення політичних цілей за допомогою інформаційно-комунікаційних технологій [4].

Мета дослідження є аналіз особливостей правового регулювання забезпечення кібербезпеки в різних країнах світу в системі міжнародної безпеки.

Постановка проблеми. Глобальні медіа найчастіше вказують на кібератаки з інших держав і стан економіки світу як основні загрози. Найбільше тривоги щодо кібератак виявляють в Японії, а також значуще

хвилювання викликають у країнах, таких як США, Німеччина та Велика Британія [4].

Розвиток інформаційно-комунікаційних технологій та Інтернету призвів до появи зовсім нових концепцій у сфері міжнародної безпеки, таких як "кіберзлочинність" і "кібертероризм". В той же час, все більшу важливість у формуванні єдиної стратегії забезпечення кібербезпеки як неот'ємної частини національної безпеки країн світу і на міжнародному рівні набуває політика кібербезпеки.

Необхідність вирішення на міждержавному рівні питання щодо застосування існуючих міжнародно-правових норм та принципів до інформаційної сфери, а також розробки спеціальних правил поведінки у кіберпросторі з метою правової протидії використанню інформаційно-комунікаційних технологій у незаконних цілях.

Виклад основного матеріалу. Ідея влаштування кіберпростору з використанням норм міжнародного права не нова. З 1996 року спроби формулювання міжнародного права про кіберпростір постійно пропонувалися (і спростовувалися) експертами в галузі права, представниками бізнесу та державами. Відповідно до принципів міжнародного права існує три домінуючі ідеї про влаштування кіберпростору: ліберальні інституціоналісти, кіберлібертаріанці та державники.

Ліберальні інституціоналісти закликають до важливості міжнародних інституцій в управлінні кіберпростором [6]. У той час як кіберлібертаріанці є прихильниками ідеї, що кіберпростір повинен залишатися вільним від тиранії та будь-яких деспотичних правил, які можуть перешкодити інтернет-свободі [7]. Державники вважають, що формулювання національного та міжнародного права, що регулює кіберпростір, є обов'язком держави [8, с. 56], домінуючі ідеї влаштування кіберпростору зображено на рис. 1.

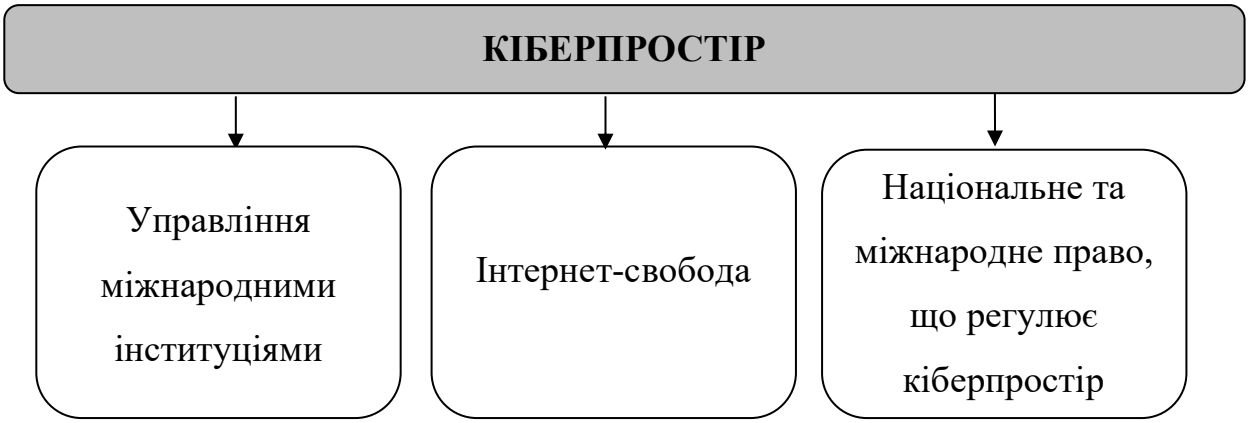

Рис. 1. Домінуючі ідеї про влаштування кіберпростору

Джерело: узагальнено автором на основі [6-8]

Ці три основні ідеї відображають принципи влаштування кіберпростору у міжнародно-правовому аспекті.

Якщо відобразити модель кіберпростіру окремої держави, то можемо зрозуміти, що це структурно-сегментований комплекс інформаційно-комунікаційного виміру життєдіяльності країни, який складається з різних за масштабом і характером елементів та їх взаємодії (рис. 2).

1. Кіберпростір великих міст – є місцеві засобів масової інформації, ряд соціальних мереж та локальні мережі які з'єднані між собою, і мають доступ до глобальної мережі типу інтернет. Тобто це весь сегмент, який присутній на даній території і взаємодіє один з одним.

2. Інформаційно-комунікаційне середовище об'єднань та громад. Це досить нове явище, яке ще до кінця не сформувалося. Громади поступово стають центром життя. Це лише питання часу.

3. Географічна локація окремих інформаційних об'єктів. Коли значуща подія в певному місці або населеному пункті набуває великої популярності. Такі точки будуть завжди. Наприклад можна згадати місто Бахмут у 2023 році.

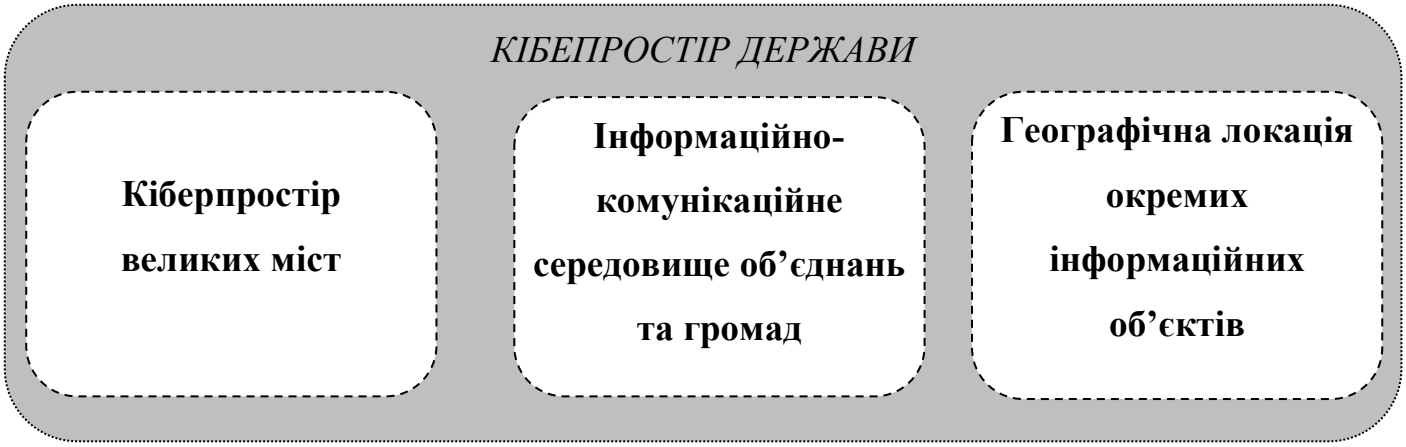

Рис. 2. Модель кібепростору окремої держави

Джерело: розроблено автором

Судячи з цього ми можемо підкреслити необхідність врегулювання відносин в кіберпросторі, як на національному рівні так і в глобальному значенні, що потребує розробки та впровадження нових рішень в сфері безпеки кіберпростору.

Юрисдикції у міжнародному праві значною мірою пов'язані з суб'єктом міжнародного права (або учасниками міжнародних відносин) та територіальністю, до якої право може формально застосовуватися [9, с. 82]. Суб'єкти в кіберпросторі різноманітні та поширені: від державних суб'єктів, великих інтернет-компаній, малих і середніх підприємств до окремих фізичних осіб. Кожен із цих суб'єктів має своє бачення на те, як слід регулювати кіберпростір.

Надзвичайно складним є визначення того, які суб'єкти права законні та підпадають під дію міжнародного права про кіберпростір. Міжнародні суб'єкти все ще не можуть дійти згоди про статус кіберпростору – чи він є глобальним надбанням, чи належить державам, на території яких відбуваються операції з ним. Дані аспекти створюють серйозні проблеми для визначення юрисдикції міжнародного кіберправа на сьогоднішній день.

Визначення особливостей устрою кіберпростору ще більше ускладнює арбітраж. Міжнародне публічне право потребує чітких

механізмів врегулювання спорів та арбітражу для забезпечення відповідальності суб'єктів [9, с. 108]. У міжнародному законодавстві про кіберпростір через різноманітність його учасників досі немає універсально узгодженої правової норми про те, хто має отримати повноваження щодо механізмів вирішення спорів та арбітражу. Арбітраж щодо поведінки у кіберпросторі вже існує, але в основному він пов'язаний з торгівлею та злочинністю і має місце в національних правових системах, а не в міжнародному суді [10]. Таким чином, це потенційно підриває неупередженість закону, оскільки деякі держави, ймовірно, мають більший вплив у даній ситуації. Проте у кіберпросторі можливий міжнародний арбітраж. Постійна палата третейського суду в Гаазі може мати потенціал для розгляду спорів щодо кіберпростору, оскільки вона вже має повноваження щодо розгляду справ, пов'язаних з космосом, енергетикою та навколишнім середовищем.

Що стосується арбітражу, то необхідно брати до уваги проблеми кіберпростору, пов'язані з правовими інструментами та судовою практикою. Обидві спостерігаються на двох рівнях: національному та міжнародному. Правова база, що регулює кіберпростір, відносно добре розвинена у високотехнологічних країнах. На федеральному рівні в США діють три основні постанови: HIPAA (1996), Закон Грема-Ліча-Біллі (1999) і Закон про внутрішню безпеку (2002). У Франції правова база щодо кіберпростору прийнята та розвивається з 1998 року [11].

Також до кіберпростору можливе таке застосування принципів та норм міжнародного права, як невикористання сили та загрози силою; невтручання у справи, що входять до внутрішньої компетенції держав; обов'язок держав співпрацювати одна з одною; суверенну рівність держав; повага до прав людини та основних свобод та ін.

Однак кіберпростір має певну специфіку, обумовлену віртуальною характеристикою глобального інформаційного простору, як об'єкта права,

в якому відстань не має значення. У зв'язку з цим загальновизнані принципи і норми міжнародного права в ряді випадків не можуть застосовуватися до кіберпростору методом простої екстраполяції понять. Так, наприклад, такі поняття, як «акт агресії», «застосування сили», «збройний напад» не можна застосовувати до будь-якої комп'ютерної атаки, а використовуване політологами та в засобах масової інформації поняття «інформаційна війна» не можна застосовувати до поняття «війна» в його міжнародно-правовому розумінні. Деякі існуючі зобов'язання держав можуть виконуватися в кіберпросторі відповідно до принципу mutatis mutandis зі змінами, заснованими на особливій природі кіберпростору. При цьому слід визнати, що концептуальні засади існуючого міжнародного правопорядку часом досить складно адаптуються до загроз, що виникають у кіберпросторі.

Дослідження використання кіберпростору як полігону гібридної агресії є недостатніми, оскільки це стає все більш типовим для стратегії ведення воєнної агресії в сучасних умовах.. Дубов Д., зазначає, що дискусія щодо сприйняття природи кібератак та відповідей на них почалася в 2010-2011 роках. У 2011 році був прийнятий документ «Талліннське керівництво із застосування міжнародного законодавства у кіберсфері», а в 2012 році НАТО визнало кіберпростір новим театром воєнних дій. Однак у практичній площині реагування є досить проблематичним, оскільки важко довести причетність конкретних країни чи груп до здійснення атак [12].

Автори-розробники «Талліннського керівництва із застосування міжнародного права в кібервійнах» виходять з того, що кіберпростір нічим не відрізняється від інших сфер відносин і не вимагає особливих підходів до його правового регулювання, а основні принципи міжнародного права, норми міжнародного гуманітарного права застосовні до дій у кіберпросторі. Так, згідно з Талліннським керівництвом, термін «зброя»

застосовується до кібертехнологій, а великомасштабні кібератаки можуть вважатися «збройним нападом» за змістом ст. 51 Статуту ООН [13].

У Талліннському керівництві, по суті, розглядаються два основні аспекти: «jus ad bellum», що визначає умови застосування державою сили в міжнародних відносинах, і «jus in bello», що визначає аспекти конфлікту, що становлять гуманітарний інтерес. Як відомо, основним джерелом права jus ad bellum є Статут ООН, а основними джерелами jus in bello є Гаазькі конвенції, Женевські конвенції та інші міжнародні договори, підписані у розвиток норм та ідеї цих конвенції.

Проблемі адаптації міжнародного права збройних конфліктів до кіберпростору присвячено низку наукових статей у зарубіжних доктринах міжнародного права. Так, ст. 41 та ст. 42 Статуту ООН виділяють два основні види «сили» – сила, пов'язана з використанням збройних сил (зброї) і сила, не пов'язана з використанням зброї. Міжнародні відносини у сфері зловмисного використання інформаційно-комунікаційних технологій (ІКТ) в основному врегульовані нормами ст. 2 (4) Статуту ООН, які пред'являють до держав вимогу утримуватися від загрози силою або її застосування у міжнародних відносинах, у тому числі й у кіберпросторі». Водночас варто зазначити, що незважаючи на «очевидність» можливості використання ІКТ у військових цілях, практично всі фахівці вважають, що ІКТ не є зброєю.

Однак слід враховувати, що відповідно до консультативного висновку Міжнародного Суду ООН «Про законність застосування ядерної зброї» здійснення права на самооборону не залежить від типу зброї, яка застосовується для нападу, достатньо самого факту застосування сили [14].

Аналіз існуючої практики демонструє, що нині розширюється трактування поняття «зброя». Так, терористична атака 11 вересня 2001 р. у Нью-Йорку з використанням захоплених терористами літаків була де-факто прирівняна до «збройного нападу» у сенсі ст. 51 Статуту ООН. У

цьому випадку цивільні літаки, які не є за своєю природою зброєю, в результаті їх нецільового використання були перетворені на напад. Таким чином США за підтримки міжнародного співтовариства оголосили про своє право на індивідуальну і колективну самооборону.

У звичайному міжнародному праві є розуміння того, що не будь-яке застосування сили може вважатися збройним нападом. У рішенні Міжнародного Суду у справі про військову та воєнізовану діяльність у Нікарагуа та проти Нікарагуа від 27 червня 1986 р. було позначено «критерій масштабу» збройного нападу будь-якої з держав на іншу державу. У подальшому критерій масштабу було підтверджено у низці інших рішень Міжнародного Суду [15].

У контексті використання інформаційно-комунікаційних технологій критерій масштабу теоретично може вважатися виконаним, якщо кібератака виходить за межі окремих незначних інцидентів. Як приклад експерти наводять безпосередній вивід з ладу інфраструктури (яку неможливо досить швидко виправити) з наслідками, що блокують здатність держави діяти або забезпечувати елементарні життєві умови населення. Таким чином, якщо наслідки від комп'ютерної атаки за своїм ефектом відповідають ефекту від нападу регулярних збройних сил, критерій масштабу теоретично може вважатися виконаним.

Задля справедливості слід зазначити, що критерій масштабу визнається не всіма державами. Наприклад, Держдепартамент США заперечував проти застосування Міжнародним Судом критерію масштабу у рішеннях щодо Нікарагуа та нафтових платформ [16].

Традиційними вимогами до дій держави у відповідь на збройний напад, що здійснюються в рамках права на самооборону, згідно зі ст. 51 Статуту ООН є необхідність і пропорційність. Зазначені вимоги не закріплені безпосередньо у Статуті ООН, проте вони відображають зміст міжнародного звичаю у цій галузі.

Згідно з чинним міжнародним правом, для відповіді на «збройний напад» силою слід визначити, що відповідальність за напад несе інша держава. Стосовно кіберпростору досить важко встановити виконавця нападу та визначити, чи діє він під контролем держави. У той час як місце розташування мети атаки очевидне, розташування її джерела часто не піддається визначенню [17].

Вищезазначені обставини демонструють певні складнощі щодо застосування існуючих норм сучасного міжнародного права до кіберпростору. Вирішенню багатьох питань у цій сфері могло б сприяти обговоренню проблеми з технічними фахівцями щодо використання інформаційно-комунікаційних технологій, зокрема у військових цілях.

У практичному плані у контексті права на самооборону за ст. 51 Статуту ООН міжнародному співтовариству слід виробити чіткі категорії, що дозволяють кваліфікувати кібератаку як «застосування сили» або «акт агресії», а також відповідні критерії для кваліфікації інформаційно-комунікаційних технологій як зброї.

Якщо ж звернутися до питання створення нових норм для регулювання кіберпростору, то в даний час зусилля держав, на жаль, сконцентровані на вузькій сфері питань прав людини, конфіденційності даних тощо. Більш того, не всі держави зацікавлені у створенні сучасного та ефективного механізму співробітництва, відкрито виступаючи проти розробки нових міжнародно-правових інструментів. З цієї причини нині відсутня всеосяжна міжнародно-правова база у сфері кіберпростору.

Поняття «кіберзлочин» з'явилося досить недавно завдяки сполученню двох слів: «кібер» і «злочин» [17]. Кібертермінологія включає в себе поняття кіберпростору, що використовується як термін для віртуального світу та інформаційного простору, що можна моделювати за допомогою комп'ютера. Вже у 1960-х роках у зарубіжній пресі з'явилося поняття "кіберзлочинність", що стосувалось злочинів, що були скоєні з

використанням ЕОМ. Але зв'язувати поняття кіберзлочинності тільки з комп'ютерами значно збіднює дану дефініцію, не дозволяючи оцінювати кіберзлочини, учинені з використанням інших засобів зв'язку, таких як мобільні телефони. Наприклад, дії, шахрайства з оплатою послуг зв'язку.

Цікава думка Бабакіна В.М., який зазначає, що поняття «кіберзлочину» є поки незвичним для правоохоронних органів, проте злочинні дії, в яких використовується глобальна комп'ютерна мережа Internet, містять в собі велику суспільну небезпеку. Автор акцентує увагу, що транснаціональний характер злочинності з використанням комп'ютерної мережі дає підстави вважати, що розробка спільної політики по основних питаннях повинна бути частиною будь-якої стратегії боротьби з кіберзлочинністю. Також певною мірою чинником, що сприяє зростанню цього нового виду злочинів, можна вважати відсутність належної взаємодії національних правоохоронних органів у питаннях попередження та розслідування таких видів злочинів [17].

Єдиним багатостороннім договором стосовно злочинної діяльності у сфері інформаційних технологій є Конвенція про злочинність у сфері комп'ютерної інформації, прийнята 23 листопада 2001 р. у Будапешті. Також проводиться серія дискусій про заохочення того, щоб звичайне міжнародне право стало основою міжнародного права щодо кіберпростору, але для цього потрібне переосмислення практики та правових інструментів, що діють на національному рівні [18]. Це все ще малоймовірне через відмінності в національних правових системах щодо кіберпростору у різних країнах.

Зазначена Конвенція включає заходи щодо різних видів злочинів, включаючи, але не обмежуючись такими: порушення конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, неправомірне перехоплення, маніпулювання даними, вплив на функціонування систем, незаконне використання пристроїв);

правопорушення, пов'язані з використанням комп'ютерних засобів (підроблення з використанням комп'ютерних технологій, шахрайство з використанням комп'ютерних технологій); а також порушення авторських та суміжних прав.

Слід враховувати, що ця конвенція розроблялася у той час, коли рівень розвитку інформаційно-комунікаційних технологій був невисоким і багато видів мережевих загроз ще не були відомі. З цієї причини ст. 1 Конвенції, що містить визначення, та наступні статті Конвенції навіть не згадують про використовувані зловмисниками «ботнети», «фішинг», «спам» та ін.

Звернення уваги до того, що деякі кіберзлочини не були виділені нормами Конвенції про кіберзлочинність в окремі групи, є важливим. У наукових колах досі тривають дискусії про ті кіберзлочини, які викликають суперечки щодо того, чи потрібно гармонізувати законодавство на міжнародному рівні для того, щоб криміналізувати їх. Серед таких кіберзлочинів є "кібертероризм" та використання кіберпростору в терористичних цілях. Держави та міжнародні організації докладають зусиль для боротьби з терористичними організаціями, які використовують кіберпростір. Наприклад, на рівні Європейського Союзу існує проект Clean IT, метою якого є боротьба з кібертероризмом [19]. Однак, через відсутність узгодженого визначення тероризму на міжнародному рівні, боротьба з кібертероризмом ускладнюється, хоча не стає неможливою. Тому криміналізація кібертероризму як явища є нагальною та необхідною для міжнародного співтовариства.

Ми не можемо ігнорувати ще одну групу кіберзлочинів, а саме - викрадення, передачу та незаконне використання особистих даних з метою вчинення злочинів (identity theft), яка, хоча і не включена окремо в Конвенцію про кіберзлочинність, але отримала поширення після прийняття міжнадордного документа. Деякі країни виділяють ці злочини в

окрему категорію, інші вважають, що дані діяння підпадають під кілька статей кримінального законодавства [18, с. 33], це в свою чергу викликає необхідність віднесення цього виду злочину до окремої категорії та узгодження міжнародного законодавства в даній області.

На сьогодні викликає занепокоєння зростання масштабів як традиційного картингу (вид шахрайства, пов'язаний із використанням платіжних карток або їхніх реквізитів.), так і більш складних кіберзлочинів. Крім того, й досі значними за обсягами та збитками залишаються такі злочини, як поширення порнографії, порушення авторських прав [20]. За останні роки в мережі все частіше з'являються сайти, основною функцією яких є негласний доступ особистої інформації їх відвідувачів: номери платіжно-розрахункових карт і PIN-коди до них; логіни і паролі; адресна книга; історія відвідувань і закладки у браузері; нещодавно збережені документи тощо [21]. Фахівці, які досліджують питання кібербезпеки, до кіберзагроз також відносять: таргетовані атаки (Advanced Persistent Threat); кібертероризм (вплив на системи керування); кібервійни; хактивізм; зловживання у соціальних мережах (вплив на суспільство); атаки на банківські системи (викрадення грошей); атаки на електронний уряд; апаратні закладки у мікросхемах і прошивках комп'ютерного і мережного обладнання [22].

Зусилля щодо формулювання міжнародних нормативно-правових актів також докладають у різних установах, таких як International Telecommunication Union (ITU) та Internet Corporation for Assigned Names and Numbers (ICANN). На жаль, даним організаціям не вдається подолати те, що міжнародне право ефективно застосовується лише у боротьбі з кіберзлочинністю та при вирішенні технічних деталей [23]. Ці організації, не включають належних та обов'язкових міжнародно-правових документів і судової практики. Таким чином, міжнародне право, яке стосується

кіберпростору, зараз має обмежену ефективність, і його складно впровадити для державних суб'єктів.

Міжнародне право про кіберпростір починає більш стрімко розвиватися з просуванням цифрового суверенітету. Цифровий суверенітет – це ідея контролю та управління доступом, інформацією, комунікаціями, мережами та інфраструктурою у цифровій сфері з боку міжнародних суб'єктів [24]. В останні роки ця ідея набирає обертів завдяки трьом історичним обставинам у кіберпросторі: кіберальянсу Китаю та Росії з питань цифрового суверенітету; Справи Сноудена та Wikileaks; та зростання Google, Apple, Facebook, Amazon (GAFA).

Кіберальянс Китаю та Росії характеризується тим, що обидві країни вимагають більшого контролю над власним кіберпростором, підтримуючи принцип невтручання у глобальні системи управління Інтернетом, такі як ITU, ICANN, IANA. Це викликає суперечки про те, чи не суперечить ідея цифрового суверенітету інтернет-нейтралітету. Однак їхні зусилля суттєво змінюють парадигму державного контролю над своїм кіберпростором, оскільки цю ідею підтримують також такі країни, як Саудівська Аравія та Єгипет. Їхні зусилля також спонукали Європейський Союз переглянути питання щодо управління Інтернетом в умовах невтручання.

Справи Сноудена-Wikileaks привернули увагу громадськості до проблем безпеки та захисту даних. Пізніше цей неспокій розширився до економічних міркувань через неконтрольовану поведінку великих інтернет-компаній, особливо GAFA. Астрономічне зростання GAFA змусило ЄС задуматися про свою цифрову екосистему, щоб запобігти монополії бізнесу та підтримати відкритість та можливості Інтернету по всій Європі.

Ці ситуації однозначно встановлюють новий клімат міжнародного права щодо кіберпростору, сприятливий для державних суб'єктів. Просування цифрового суверенітету не тільки потенційно підірве інтернет-

нейтралітет, а й як наслідок, порушить питання прав і свобод у кіберпросторі. Це пов'язано з тим, що цифровий суверенітет потенційно може створити фрагментований кіберпростір, оскільки він ретельно регулюватиметься державами на територіальній основі. У результаті це обмежує можливість міжнародних суб'єктів дійти згоди для формулювання ефективного та обов'язкового міжнародного права щодо кіберпростору. Це також ускладнює можливість винесення судових рішень у справах про кіберпорушення державним суб'єктам, оскільки цифровий суверенітет укорінений у принципах невтручання.

Таким чином, міжнародне співробітництво є ключовим моментом у ліквідації правового вакууму, який існує між динамічним розвитком інформаційних технологій та законодавчим реагуванням на сучасні кіберзагрози. Міжнародне співробітництво здійснюється з метою зміцнення взаємної довіри у сфері кібербезпеки; вироблення спільних підходів до протидії кіберзагрозам; консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в протиправних цілях; виконання Україною зобов'язань у рамках укладених міжнародних договорів у контексті співробітництва у сфері кібербезпеки з іноземними державами, їх збройними силами, правоохоронними органами і спеціальними службами, а також міжнародними організаціями; оптимізації надання міжнародної технічної допомоги.

У сучасних умовах ситуація, що склалася навколо майбутнього глобального кіберпростору, перебуває на перетині двох рівнозначних трендів. З одного боку, офіційні зусилля світової спільноти спрямовані на демілітаризацію кіберпростору та недопущення його перетворення на нове поле збройного конфлікту, а з іншого – де-факто триває процес полярного протистояння. Міжнародні структури, на кшталт ООН, хоча й роблять спроби впливати на цей процес, однак ці наміри є досить фрагментарними. Незважаючи на цілу низку рішень і резолюцій таких як Резолюція

Генеральної Асамблеї ООН A/RES/55/63 від 4 грудня 2000 року «Боротьба із злочинним використанням інформаційних технологій». Її ухваленню сприяло завершення обговорення Конвенції про кіберзлочинність. Після підбиття підсумків кількох міжнародних конгресів і конференцій з проблематики кіберзлочинності суттєвого коригування зазнала резолютивна частина Резолюції [25].

Проте, Організація Об'єднаних Націй до цього часу не впровадила ефективний міжнародно-правовий механізм, що міг би системно вирішувати питання кібербезпеки. Велика кількість документів, виданих ООН у цій сфері, мають суперечливий характер та не сприймаються деякими державами-членами як ключові. Недавно, однак, спостерігається певне пожвавлення діяльності ООН у напрямку нормативного врегулювання глобальної кібербезпеки. Наприклад, у червні 2015 року було оголошено, що за результатами засідання Групи урядових експертів ООН з міжнародної інформаційної безпеки було визначено, що на використання інформаційно-комунікаційних технологій поширюється діюче міжнародне право, але за певних обставин це право може бути доповнене, включаючи прийняття нових норм [26, с. 132].

Навіть при застосуванні принципів та норм сучасного міжнародного права до сфери інформації, необхідно узагальнити існуюче міжнародно-правове регулювання стосовно кіберпростору, враховуючи його специфіку, з метою ефективної правової боротьби проти незаконного використання інформаційно-комунікаційних технологій.

Застосування міжнародного права до суб'єктів в кіберпросторі сьогодні проявляє обмежену результативність через недоліки, які виникають у трьох ключових аспектах міжнародного права: судової компетенції, розгляду спорів та судової практики.

Існуючі тенденції щодо розвитку концепції цифрового суверенітету можуть стати на заваді ефективному застосуванню міжнародного права у

кіберпросторі державними суб'єктами. У такій ситуації необхідні більш широкі заклики до формулювання правил використання кіберпростору, що базуються на ідеї свободи та інклюзивності глобальних норм.

Підбиваючи підсумки, можна відзначити, що ключові документи міжнародного нормативного регулювання в галузі захисту кіберпростору включають Кібербезпекову стратегію ООН, Декларацію про принципи поведінки держав в кіберпросторі та Конвенцію про кіберзлочинність. Ці документи визначають ключові поняття в сфері кібербезпеки, встановлюють принципи захисту критичних інфраструктур та протидії кіберзлочинам. Наприклад, Декларація про принципи поведінки держав в кіберпросторі містить 13 принципів, які регулюють дії держав в цій сфері, включаючи захист прав людини та свободу в Інтернеті. Конвенція про кіберзлочинність встановлює основи міжнародного правового режиму для цієї галузі, визначаючи правила визначення кіберзлочинів, їх кримінальну відповідальність та міжнародну співпрацю. Ці документи є ключовими для розвитку співпраці між державами та встановлення стандартів в сфері кібербезпеки.

Висновки. Загалом, можна зазначити, що розвиток міжнародного законодавства у сфері захисту кіберпростору є складним завданням, яке вимагає спільних зусиль держав на національному та міжнародному рівнях. Створення норм, що регулюють діяльність в кіберпросторі, потребує врахування таких аспектів, як забезпечення кібербезпеки, захист особистих даних, боротьба з кіберзлочинами та кібертероризмом.

Для забезпечення ефективного захисту кіберпростору важливо продовжувати розвивати міжнародне законодавство та створювати нові технологічні та організаційні інструменти для забезпечення кібербезпеки. Безпека кіберпростору є неодмінною складовою загальної безпеки, і тому держави та міжнародна спільнота повинні продовжувати пріоритетну роботу з розвитку міжнародного законодавства у сфері кібербезпеки

Література

1. National Military Strategy for Cyberspace Operations URL: https://www.hsdl.org/The_National_Military_Strategy_for_Cyberspace_Operations (дата звернення: 12.08.2023)
2. 中华人民共和国网络安全法. URL: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm (дата звернення: 12.08.2023)
3. Почепцов Г. Г., Чукут С. А. Інформаційна політика. 2-ге вид., стер. Київ : Знання, 2008. 663 с. С. 584.
4. Poushter J., Manevich D. Globally, People Point to ISIS and Climate Change as Leading Security Threats. Pew Research Center. August 1, 2017. URL: http://www.pewglobal.org/2017/08/01/globally-people-point-to--isis-and-climate-change-as-leading-security-threats (дата звернення: 12.08.2023)
5. Woolley P. Defining Cyberspace as a United States Air Force Mission. URL: https://apps.dtic.mil/sti/pdfs/ADA453972.pdf (дата звернення: 21.04.2023)
6. Wu T. Cyberspace Sovereignty – The Internet and the International System. Harvard Journal of Law & Technology. 2017. №10. P. 647-666. P. 649.
7. Barlow J. P., A Declaration of the Independence of Cyberspace. Electronic Frontier Foundation. URL: https://www.eff.org/cyberspace-independence (дата звернення: 11.04.2023)
8. Lewis J. Sovereignty and the Role of Government in Cyberspace. Brown Journal of World Affairs. 2018. №16. P. 55-65.
9. Basak C. International Law of International Relations : Palgrave MacMillan, 2015. 188 p.
10. Kriangsak K. Public International Law of Cyberspace. Law, Governance and Technology. Series, 32 : Springer, 2017. 407 p.

11. Подготовка вхождения Франции в информационное общество. Правительственная программа действий. URL: http://old.unesco.kz/ip/countries/france_is_rus.htm (дата звернення: 15.04.2023)
12. Військова відповідь на кібератаки Кремля? І так, і ні. *Укрінформ.* URL: https://www.ukrinform.ua/rubric-technology/2251563-vijskova-vidpovidnakiberataki-kremla-i-tak-i-ni.html (дата звернення: 18.04.2023)
13. Schmitt M. (red. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations USA : Cambridge University Press. 2017. URL: http://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf (дата звернення: 18.04.2023)
14. Міжнародний Суд ООН. Організація Об'єднаних Націй. Нью-Йорк, 1998. URL: https://www.icj-cij.org/sites/default/files/summaries/summaries-1992-1996-ru.pdf (дата звернення: 22.04.2023)
15. Справа про військову і воєнізовану діяльність в Нікарагуа і проти неї (Нікарагуа проти США), рішення від 27 червня 1986 р. (по суті). URL: https://www.icj-cij.org/files/case-related/70/070-19841126-JUD-01-00-EN.pdf (дата звернення: 22.04.2023)
16. Савчук К.О. Міжнародний суд ООН як засіб мирного розв'язання міжнародних спорів у сучасному міжнародному праві. Часопис Київського університету права. 2013. № 4. С. 341–347.
17. Бабакін В.М. Особливості міжнародного співробітництва при розслідуванні кіберзлочинів. Форум права. 2011. № 4. С. 27-35. URL: https://dspace.univd.edu.ua/bitstreams/661ed915-06d3-49da-beb3-06056c249682/download (дата звернення: 12.05.2023)
18. Конвенція Ради Європи про кіберзлочинність : Міжнародний документ від 23 листоп. 2001 р. URL:

https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 12.05.2023)

19. Winterford B. Clean IT project considers terrorist content database. 2012. URL: https://www.itnews.com.au/news/clean-it-project-considers-terrorist-content-database-303729 (дата звернення: 12.05.2023)
20. Грайворонський М.В. Сучасні підходи до забезпечення кібербезпеки. О кибернетике как лженауке. URL: https://ela.kpi.ua/bitstream/123456789/16999/1/Grajvoronsky.pdf (дата звернення: 15.05.2023)
21. Орлов О.В., Оніщенко Ю.М. Попередження кіберзлочинності – складова частина державної політики в Україні. Теорія та практика державного управління. Вип. 1(44). С. 9-15. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64 (дата звернення: 15.05.2023)
22. Черноног О.О. Напрями підвищення ефективності забезпечення кібербезпеки інформаційних технологій в системі публічного управління. Междисциплинарные исследования в науке и образовании. 2015. URL: http://mino.esrae.ru/178-1484 (дата звернення: 15.05.2023)
23. Executive summary of ITU-T SG9 meeting (fully virtual, 6-14 September 2022). URL: https://www.itu.int/en/ITU-T/studygroups/2022-2024/09/Documents/Executive-summary-2022-09_virtual-meeting.pdf (дата звернення: 20.05.2023)
24. Couture S., Toupin S. What Does the Notion of "Sovereignty" Mean When Referring to the Digital. New Media & Society. 2019. № 21. P. 2305-2322.
25. Борьба с преступным использованием информационных технологий : Резолюция ООН от 22 января 2001 г. № 55/63. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/563/19/PDF/N0056319.pdf?OpenElement (дата звернення: 20.05.2023)

26. Поляков О.М. Активізація міжнародної співпраці у сфері забезпечення кібербезпеки: шляхи удосконалення в реаліях сьогодення. Інформація і право. 2021. № 2(37). С. 129-138.
27. Забара І. М. Міжнародна інформаційна безпека: сучасні концепції в міжнародному праві. Теорія і практика правознавства. 2013. Вип. № 2. URL: http://nbuv.gov.ua/j-pdf/tipp_2013_2_77.pdf (дата звернення: 28.05.2023)
28. Лук'янчикова В. Ю. Кіберпростір: загрози для міжнародних відносин та глобальної безпеки. Гілея: наук. вісн. 2013. № 72. С. 793–796. URL: http://nbuv.gov.ua/j-pdf/gileya_2013_72_153.pdf (дата звернення: 28.05.2023)

References

1. National Military Strategy for Cyberspace Operations URL: https://www.hsdl.org/The_National_Military_Strategy_for_Cyberspace_Operations (date of access: 12.08.2023) [in English]
2. 中华人民共和国网络安全法. URL: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm (date of access: 12.08.2023)
3. Pocheptsov H. H., Chukut S. A. Informatsiina polityka. 2-he vyd., ster. Kyiv : Znannia, 2008. 663 s. S. 584. [in Ukrainian]
4. Poushter J., Manevich D. Globally, People Point to ISIS and Climate Change as Leading Security Threats. Pew Research Center. August 1, 2017. URL: http://www.pewglobal.org/2017/08/01/globally-people-point-to--isis-and-climate-change-as-leading-security-threats (date of access: 12.08.2023) [in English]
5. Woolley P. Defining Cyberspace as a United States Air Force Mission. URL: https://apps.dtic.mil/sti/pdfs/ADA453972.pdf (date of access: 21.04.2023) [in English]

6. Wu T. Cyberspace Sovereignty – The Internet and the International System. Harvard Journal of Law & Technology. 2017. №10. P. 647-666. P. 649. [in English]
7. Barlow J. P., A Declaration of the Independence of Cyberspace. Electronic Frontier Foundation. URL: https://www.eff.org/cyberspace-independence (date of access: 11.04.2023) [in English]
8. Lewis J. Sovereignty and the Role of Government in Cyberspace. Brown Journal of World Affairs. 2018. №16. P. 55-65. [in English]
9. Basak C. International Law of International Relations : Palgrave MacMillan, 2015. 188 p. [in English]
10. Kriangsak K. Public International Law of Cyberspace. Law, Governance and Technology. Series, 32 : Springer, 2017. 407 p. [in English]
11. Podgotovka vkhozhdeniya Frantsii v informatsionnoe obshchestvo. Pravitelstvennaya programma deystviy. URL: http://old.unesco.kz/ip/countries/france_is_rus.htm (date of access: 15.04.2023) [in Russian]
12. Viiskova vidpovid na kiberataky Kremlia? I tak, i ni. Ukrinform. URL: https://www.ukrinform.ua/rubric-technology/2251563-vijskova-vidpovidnakiberataki-kremla-i-tak-i-ni.html (date of access: 18.04.2023) [in Ukrainian]
13. Schmitt M. (red. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations USA : Cambridge University Press. 2017. URL: http://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf (date of access: 18.04.2023) [in English]
14. Mizhnarodnyi Sud OON. Orhanizatsiia Obiednanykh Natsii. Niu-York, 1998. URL: https://www.icj-cij.org/sites/default/files/summaries/summaries-1992-1996-ru.pdf (date of access: 22.04.2023) [in Russian]

15. Sprava pro viiskovu i voienizovanu diialnist v Nikarahua i proty nei (Nikarahua proty SShA), rishennia vid 27 chervnia 1986 r. (po suti). URL: https://www.icj-cij.org/files/case-related/70/070-19841126-JUD-01-00-EN.pdf (date of access: 22.04.2023) [in Ukrainian]
16. Savchuk K.O. Mizhnarodnyi sud OON yak zasib myrnoho rozviazannia mizhnarodnykh sporiv u suchasnomu mizhnarodnomu pravi. Chasopys Kyivskoho universytetu prava. 2013. № 4. S. 341–347. [in Ukrainian]
17. Babakin V.M. Osoblyvosti mizhnarodnoho spivrobitnytstva pry rozsliduvanni kiberzlochyniv. Forum prava. 2011. № 4. S. 27-35. URL: https://dspace.univd.edu.ua/bitstreams/661ed915-06d3-49da-beb3-06056c249682/download (date of access: 12.05.2023) [in Ukrainian]
18. Konventsiia Rady Yevropy pro kiberzlochynnist : Mizhnarodnyi dokument vid 23 lystop. 2001 r. URL: https://zakon.rada.gov.ua/laws/show/994_575 (date of access: 12.05.2023) [in Ukrainian]
19. Winterford B. Clean IT project considers terrorist content database. 2012. URL: https://www.itnews.com.au/news/clean-it-project-considers-terrorist-content-database-303729 (date of access: 12.05.2023) [in English]
20. Hraivoronskyi M.V. Suchasni pidkhody do zabezpechennia kiberbezpeky. O kibernetike kak lzhenauke. URL: https://ela.kpi.ua/bitstream/123456789/16999/1/Grajvoronsky.pdf (date of access: 15.05.2023) [in Ukrainian]
21. Orlov O.V., Onishchenko Yu.M. Poperedzhennia kiberzlochynnosti – skladova chastyna derzhavnoi polityky v Ukraini. Teoriia ta praktyka derzhavnoho upravlinnia. Vyp. 1(44). S. 9-15. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64 (date of access: 15.05.2023) [in Ukrainian]
22. Chernonoh O.O. Napriamy pidvyshchennia efektyvnosti zabezpechennia kiberbezpeky informatsiinykh tekhnolohii v systemi publichnoho upravlinnia. Mezhdistsiplinarnye issledovaniya v nauke i obrazovanii.

2015. URL: http://mino.esrae.ru/178-1484 (date of access: 15.05.2023) [in Ukrainian]

23. Executive summary of ITU-T SG9 meeting (fully virtual, 6-14 September 2022). URL: https://www.itu.int/en/ITU-T/studygroups/2022-2024/09/Documents/Executive-summary-2022-09_virtual-meeting.pdf (date of access: 20.05.2023) [in English]
24. Couture S., Toupin S. What Does the Notion of "Sovereignty" Mean When Referring to the Digital. New Media & Society. 2019. № 21. P. 2305-2322. [in English]
25. Borba s prestupnym ispolzovaniem informatsionnykh tekhnologiy : Rezolyutsiya OON ot 22 yanvarya 2001. № 55/63. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/563/19/PDF/N0056319.pdf?OpenElement (date of access: 20.05.2023) [in Russian]
26. Poliakov O.M. Aktyvizatsiia mizhnarodnoi spivpratsi u sferi zabezpechennia kiberbezpeky: shliakhy udoskonalennia v realiiakh sohodennia. Informatsiia i pravo. 2021. № 2(37). S. 129-138. [in Ukrainian]
27. Zabara I. M. Mizhnarodna informatsiina bezpeka: suchasni kontseptsii v mizhnarodnomu pravi. Teoriia i praktyka pravoznavstva. 2013. Vyp. № 2. URL: http://nbuv.gov.ua/j-pdf/tipp_2013_2_77.pdf (date of access: 28.05.2023) [in Ukrainian]
28. Lukianchykova V. Yu. Kiberprostir: zahrozy dlia mizhnarodnykh vidnosyn ta hlobalnoi bezpeky. Hileia: nauk. visn. 2013. № 72. S. 793–796. URL: http://nbuv.gov.ua/j-pdf/gileya_2013_72_153.pdf (date of access: 28.05.2023) [in Ukrainian]