УДК 341.3:004.056
DOI https://doi.org/10.24144/2788-6018.2026.02.3.47

ПРАВОВЕ РЕГУЛЮВАННЯ КІБЕРАТАК ПІД ЧАС ЗБРОЙНИХ КОНФЛІКТІВ

Пасешник О.Р.,
аспірант кафедри міжнародного,
цивільного та комерційного права,
Державний торговельно-економічний університет
ORCID: 0009-0005-6692-9925

Пасешник О.Р. Правове регулювання кібератак під час збройних конфліктів.

Статтю присвячено комплексному дослідженню правового регулювання кібератак під час збройних конфліктів у контексті застосування норм і принципів міжнародного гуманітарного права. У роботі обґрунтовано, що кібератаки, наслідки яких є співмірними з наслідками традиційного збройного насильства, підлягають правовій оцінці відповідно до права збройних конфліктів, незважаючи на відсутність спеціального універсального міжнародного договору, присвяченого саме діям у кіберпросторі. Визначено, що ключовим критерієм застосовності міжнародного гуманітарного права є не технічна форма втручання, а характер, масштаб і гуманітарні наслідки відповідної дії. Особливу увагу зосереджено на аналізі принципів розрізнення, пропорційності та військової необхідності як базових орієнтирів для встановлення меж правомірного застосування кібератак у період збройного конфлікту. Показано, що у цифровому середовищі реалізація цих принципів ускладнюється через змішаний характер інфраструктури, поєднання цивільних і військових функцій в одних і тих самих системах, а також через можливість настання непрямих і каскадних наслідків для цивільного населення. Окремо проаналізовано правове значення кібератак, спрямованих на об'єкти критичної інфраструктури, об'єкти подвійного призначення та об'єкти, необхідні для виживання цивільного населення, зокрема системи водопостачання, енергетики, медичні установи та засоби зв'язку. Наголошено, що виведення таких об'єктів з ладу шляхом цифрового впливу може спричиняти тяжкі гуманітарні наслідки й тому потребує оцінки за тими самими правовими критеріями, що й традиційні воєнні дії.

У статті також розкрито питання міжнародної відповідальності за неправомірне використання кібератак під час збройних конфліктів. Зазначено, що порушення норм міжнародного гуманітарного права в кіберпросторі може спричиняти як міжнародно-правову відповідальність держави, так і індивідуальну міжнародну кримінальну відповідальність осіб, якщо наслідки таких дій відповідають ознакам міжнародних злочинів. Досліджено основні труднощі практичної реалізації відповідальності, зокрема проблеми атрибуції, збирання доказів, встановлення джерела кібератаки, а також визначення юрисдикції у справах, пов'язаних із цифровими засобами ведення війни. Значну увагу приділено аналізу сучасних підходів окремих держав до тлумачення застосовності міжнародного гуманітарного права у кіберпросторі, що дає змогу виявити тенденцію до поступового формування узгодженої міжнародної практики у цій сфері.

Ключові слова: міжнародне гуманітарне право, кібератаки, збройний конфлікт, принцип розрізнення, принцип пропорційності, військова необхідність, цивільне населення, критична інфраструктура, об'єкти подвійного призначення, кіберпростір.

Paseshnyk O.R. Legal regulation of cyberattacks during armed conflicts.

The article is devoted to a comprehensive study of the legal regulation of cyberattacks during armed conflicts in the context of the application of the norms and principles of international humanitarian law. The paper substantiates that cyberattacks whose consequences are comparable to those of traditional armed violence are subject to legal assessment under the law of armed conflict, despite the absence of a special universal international treaty specifically devoted to actions in cyberspace. It is determined that the key criterion for the applicability of international humanitarian law is not the technical form of interference, but the nature, scale, and humanitarian consequences of the relevant act. Particular attention is focused on the analysis of the principles of distinction, proportionality, and military necessity as the basic benchmarks for establishing the limits of the lawful use of cyberattacks during armed conflict. It is shown that in the digital environment the implementation of these principles is complicated by the mixed character of infrastructure, the combination of civilian and military functions within the same systems, as well as by the possibility of indirect and cascading consequences for the civilian population. Particular attention is also paid to the legal significance of cyberattacks directed against critical infrastructure, dual-use objects, and objects indispensable to the survival of the civilian

population, including water supply systems, energy facilities, medical institutions, and means of communication. It is emphasised that disabling such objects through digital interference may cause grave humanitarian consequences and therefore requires assessment according to the same legal criteria as traditional military actions.

The article also addresses the issue of international responsibility for the unlawful use of cyberattacks during armed conflicts. It is noted that violations of international humanitarian law in cyberspace may give rise both to the international legal responsibility of a state and to the individual international criminal responsibility of persons where the consequences of such acts correspond to the elements of international crimes. The main difficulties of the practical implementation of responsibility are examined, in particular problems of attribution, evidence collection, identification of the source of a cyberattack, as well as the determination of jurisdiction in cases involving digital means of warfare. Considerable attention is paid to the analysis of contemporary approaches adopted by individual states to the interpretation of the applicability of international humanitarian law in cyberspace, which makes it possible to identify a tendency towards the gradual formation of a more coherent international practice in this field.

Key words: international humanitarian law, cyberattacks, armed conflict, principle of distinction, principle of proportionality, military necessity, civilian population, critical infrastructure, dual-use objects, cyberspace.

Постановка проблеми. Сучасні збройні конфлікти супроводжуються активним використанням кіберзасобів, що актуалізує питання правового регулювання кібератак у межах міжнародного гуманітарного права. Особливого значення набуває визначення критеріїв, за якими такі дії можуть визнаватися правомірними або неправомірними.

Метою статті є з'ясування особливостей правового регулювання кібератак під час збройних конфліктів та визначення меж їх правомірності крізь призму принципів міжнародного гуманітарного права.

Стан опрацювання проблематики. Питання застосування міжнародного гуманітарного права до кібератак висвітлюються у документах Міжнародного Комітету Червоного Хреста, Талліннському посібнику 2.0, актах міжнародних організацій та офіційних позиціях окремих держав. Водночас, низка аспектів правової оцінки кібератак, зокрема щодо об'єктів критичної інфраструктури, подвійного призначення та меж міжнародної відповідальності, потребує подальшого уточнення.

Виклад основного матеріалу. Розвиток цифрових технологій призвів до формування нового виміру збройного протистояння - кіберпростору. Кібератаки дедалі частіше використовуються як доповнення до традиційних воєнних засобів або навіть як окрема форма досягнення стратегічних цілей під час збройних конфліктів. Їхнє значення зростає як у міждержавних, так і у внутрішніх збройних конфліктах, завдяки високій ефективності, глобальному охопленню, а також потенціалу завдавати значної шкоди без безпосереднього застосування фізичної сили. Таке явище ставить перед міжнародним гуманітарним правом низку складних викликів, пов'язаних із розширенням сфери його застосування у кіберпросторі.

Найбільше занепокоєння викликають кібератаки, спрямовані на об'єкти критичної інфраструктури, медичні установи, системи водопостачання, об'єкти енергетики та зв'язку в умовах активних бойових дій. У багатьох випадках такі дії спричиняють страждання цивільного населення, порушують принцип розрізнення між військовими й цивільними цілями, а також перевищують допустимі межі пропорційності в нанесенні побічної шкоди. Це підсилює потребу у формулюванні чітких правових меж допустимого застосування кібератак відповідно до міжнародного гуманітарного права.

Незважаючи на загальне визнання важливості правового регулювання кібератак, наразі не існує жодного універсального міжнародного договору, який би встановлював межі їх використання у збройних конфліктах. Наявна договірна база, а саме, Женевські конвенції 1949 року та Додаткові протоколи до них, формально не містять окремих норм про дії в кіберпросторі. При цьому, Міжнародний Комітет Червоного Хреста зазначає, що міжнародне гуманітарне право повною мірою застосовується і до кібератак, якщо вони здійснюються у контексті збройного конфлікту. Згідно з його позицією, кібератаки, як і будь-які інші засоби або методи ведення війни, підлягають тим самим обмеженням, які передбачені для традиційних форм збройного насильства [1].

Тлумачення поняття кібератаки в цьому контексті є надзвичайно важливим аспектом. На рівні доктрини вважається, що кібератакою є цілеспрямована дія в кіберпросторі, яка має на меті порушити, пошкодити або знищити ціль, що становить військовий інтерес супротивника, за допомогою інформаційних технологій. Йдеться не лише про спричинення фізичної шкоди, а й про функціональні наслідки, такі як блокування систем, унеможливлення управління об'єктами, втрату зв'язку, порушення роботи інфраструктури тощо. Таке розуміння підтримується, зокрема, у Талліннському посібнику 2.0, підготовленому групою незалежних експертів [2].

Окремо слід розглянути застосування міжнародного гуманітарного права до кібератак, спрямованих на об'єкти, необхідні для виживання цивільного населення. Стаття 54 Додаткового протоколу I забороняє руйнування, виведення з ладу або знищення таких об'єктів, як запаси продуктів, джерела води, енергетичні системи, медичні заклади тощо. У кіберпросторі ця норма набуває нового змісту: атака може здійснюватися без фізичного втручання, однак спричиняти серйозні гуманітарні наслідки. Наприклад, уразливість електронної документації медичних установ або централізованих систем водопостачання відкриває можливість для завдання шкоди шляхом логічного впливу на системи, що забезпечують базові життєві функції населення. У цьому контексті слід наголосити, що застосовність міжнародного гуманітарного права до кібератак визначається не засобом впливу, а характером дії. Якщо наслідки кібератаки відповідають поняттю "нападу", тобто акту насильства проти супротивника згідно зі статтею 49 додаткового протоколу до Женевських конвенцій, то до неї підлягають усі норми права збройних конфліктів. Таким чином, кібератака, яка блокує доступ до електроенергії чи води або виводить з ладу систему охорони здоров'я, може вважатися нападом у розумінні міжнародного гуманітарного права, з усіма відповідними юридичними наслідками [3].

Водночас слід розрізняти кібератаки, що досягають порогу застосування сили, і дії, які мають менш руйнівний характер. Наприклад, збирання розвідувальних даних, дезінформація або короткострокове порушення роботи інформаційних ресурсів. Такі дії не підпадають під регулювання міжнародного гуманітарного права, а мають оцінюватися в межах загального міжнародного права, зокрема крізь призму принципів суверенної рівності держав, незастосування сили або погрози силою, невтручання у внутрішні справи держав, мирного вирішення міжнародних спорів і територіальної цілісності держав.

Окрему увагу слід приділити атакам на об'єкти подвійного призначення, тобто такі, що використовуються як цивільною, так і військовою стороною. Наприклад, телекомунікаційна мережа, що забезпечує одночасно мобільний зв'язок для населення і передавання командування в збройних силах, у разі ураження створює непряму, але значну загрозу для цивільних. Такі ситуації вимагають особливої юридичної оцінки з точки зору принципу розрізнення та пропорційності.

Зважаючи на все вищезазначене, кібератаки, що відбуваються у контексті збройного конфлікту і мають гуманітарні наслідки, прирівнювані до звичайного збройного насильства, підпадають під регулювання міжнародного гуманітарного права. Оцінювати такі дії слід не лише з технічної точки зору, а й базуватись на їх впливі на людей, інфраструктуру, гуманітарну ситуацію та на контекст, у якому вони здійснюються. Саме це дозволяє провести межу між неправомірною атакою і правомірною дією, що здійснюється з дотриманням норм міжнародного гуманітарного права.

Щоб зрозуміти, в яких межах кібератаки можуть вважатися правомірними під час збройних конфліктів, необхідно, насамперед, звернутися до базових принципів міжнародного гуманітарного права. Саме вони встановлюють критерії допустимості засобів і методів ведення бойових дій та забезпечують правову основу для оцінки кожної конкретної дії у складних умовах збройного конфлікту. Першим і найважливішим є принцип розрізнення, який вимагає постійного розмежування між цивільним населенням і комбатантами, а також між цивільними об'єктами й військовими цілями. Він не лише забороняє безпосередні атаки на цивільних осіб, а й обмежує можливість завдання побічної шкоди цивільній сфері. У кіберпросторі реалізація цього принципу ускладнена: інфраструктура часто виконує змішані функції, і визначити, чи є об'єкт виключно військовим, надзвичайно складно. Наприклад, атакуючи систему керування залізничним сполученням, яка водночас використовується і для постачання військових вантажів, і для евакуації цивільного населення, сторона конфлікту ризикує порушити вимоги цього принципу [4].

Другим фундаментальним обмеженням є принцип пропорційності. Згідно з ним, шкода, яка може бути завдана цивільному населенню під час атак на військові об'єкти, не повинна бути надмірною порівняно з передбачуваною військовою перевагою. У випадку кібератак це особливо складно: наслідки таких дій можуть мати каскадний характер і проявлятися з затримкою. Наприклад, якщо атака на електромережу з метою ускладнити управління військами призводить до тривалого знеструмлення лікарень, шкіл і пунктів евакуації, така дія може бути визнана непропорційною [5].

Наступним ключовим елементом є принцип військової необхідності. Він допускає застосування сили лише у тому випадку, якщо це обумовлено потребою досягнення визначеної і конкретної воєнної мети. Дії, що не мають військової доцільності, навіть якщо вони здійснюються в межах конфлікту, є порушенням міжнародного гуманітарного права. Наприклад, кібератака, що дестабілізує системи електронного врядування або викликає паніку серед цивільного населення без досягнення воєнної мети, порушує цей принцип.

Такі правові межі застосовуються незалежно від виду озброєння або способу досягнення ефекту. Відповідно до позиції Міжнародного Комітету Червоного Хреста, будь-який засіб, здатний спричинити ті ж самі наслідки, що й традиційне збройне насильство, має регулюватися тими ж самими

нормами міжнародного гуманітарного права [6]. Таким чином, юридична кваліфікація кібератаки не залежить від того, чи застосовано фізичне знищення, а визначається характером впливу на об'єкт і його гуманітарними наслідками.

Водночас, як свідчить аналіз практики останніх років, багато держав не мають чітко визначених механізмів реалізації цих принципів у кіберсфері. Відсутність прозорих критеріїв розрізнення, методик оцінки пропорційності та процедур визначення військової необхідності в умовах цифрової війни створює серйозні загрози для дотримання гуманітарного права. Це підкреслює потребу у більш деталізованому правовому регулюванні, з урахуванням технічних реалій кіберпростору.

Порушення визначених гуманітарним правом меж застосування кібератак породжує питання міжнародної відповідальності. Як і в разі збройного насильства у фізичному просторі, відповідальність може настати як на рівні держави, так і на рівні індивідуальної міжнародної кримінальної відповідальності окремих осіб.

У разі, коли кібератака призводить до ураження цивільного населення, знищення об'єктів, які не є військовими цілями, або має невибірковий характер, такі дії можуть бути визнані міжнародно-протиправним діянням держави. Ця позиція узгоджується з положеннями проєкту статей Комісії міжнародного права ООН про відповідальність держав за міжнародно-протиправні діяння, зокрема статтями 1 і 2, які встановлюють загальні умови настання міжнародної відповідальності держави за дії, що порушують її міжнародні зобов'язання, включно з нормами міжнародного гуманітарного права [7].

Наявність збройного конфлікту або вчинення дії особами, що діють від імені держави, не виключає міжнародно-правової оцінки такої дії. У цьому випадку держава може бути зобов'язана припинити порушення, надати відшкодування та гарантії того, що такі дії не повторяться. Однак притягнення до відповідальності в цифровому середовищі наштовхується на серйозну перешкоду - питання атрибуції. Встановити з достатньою впевненістю, що конкретна атака була здійснена з ініціативи або за підтримки держави, надзвичайно складно. Це пов'язано з технічними труднощами у зборі доказів, застосуванням проксі-структур і анонімних каналів комунікації.

Окрім відповідальності держави, міжнародне право передбачає також можливість індивідуальної кримінальної відповідальності. Якщо кібератака має ознаки злочину, передбаченого Римським статутом Міжнародного кримінального суду, такі як умисний напад на цивільне населення або гуманітарні об'єкти, особа, яка організувала або виконала таку дію, може бути притягнута до відповідальності за воєнний злочин. Хоча кібератаки прямо не згадані у Римському статуті, це не виключає їх криміналізації. Римський статут застосовується до діянь, що за своїм змістом є злочинами, незалежно від засобу їх вчинення. Якщо кібератака призводить до ефекту, рівнозначного обстрілу або блокування гуманітарного об'єкта, вона може бути підставою для переслідування винних осіб [8].

Реалізація юрисдикції Міжнародного кримінального суду пов'язана не лише з юридичними, а й з практичними складнощами. Для того, щоб Міжнародний кримінальний суд розглянув справу, мають бути дотримані основні умови визначені Римським статутом, а саме: територіальна та персональна юрисдикція згідно зі статтею 12, а також умови прийнятності справи, передбачені статтею 17, яка включає достатню серйозність злочину й відсутність дійсного національного розслідування. У випадку кібератак, особливо тих, що здійснюються з використанням інфраструктури в третіх державах або через анонімні канали, виникають складнощі з визначенням відповідної території, ідентифікацією винних осіб та підтвердженням серйозності наслідків. Це значно ускладнює відкриття справи в Міжнародному кримінальному суді. Водночас із розвитком цифрової криміналістики та міжнародно-правового співробітництва зростає потенціал встановлення індивідуальної відповідальності за кібератаки, що мають ознаки воєнних злочинів.

Таким чином, міжнародна відповідальність за неправомірне використання кібератак у збройному конфлікті є цілком можливою з правової точки зору, але реалізація такої відповідальності стикається з низкою технічних, доказових і процедурних бар'єрів. Це вимагає подальшого розвитку як міжнародно-правового регулювання, так і технічного співробітництва між державами, щоб зробити притягнення до відповідальності не лише формально можливим, а й практично здійсненним.

Окремого значення набуває практика окремих держав щодо застосування міжнародного гуманітарного права до дій у кіберпросторі. Хоча не існує універсального міжнародного документа, який би комплексно регулював правовий режим кібератак під час збройних конфліктів, низка держав уже сформулювала власні доктринальні позиції. Вивчення цих підходів дає змогу глибше зрозуміти, як саме в національних правових рамках визначаються межі допустимого у кіберпросторі.

Сполучені Штати Америки послідовно визнають застосовність міжнародного гуманітарного права до кібератак. У "Польовому статуті щодо права війни" Міністерства оборони США зазначено, що правила, які регулюють ведення бойових дій у традиційних доменах, застосовуються і до кі-

берпростору. У документі підтверджено, що кібератаки, які спричиняють насильницький вплив на супротивника, можуть кваліфікуватися як напади згідно з гуманітарним правом, за умови, що вони відбуваються в рамках збройного конфлікту [9, с. 1026].

Франція у 2019 році оприлюднила офіційну позицію щодо міжнародного права у кіберпросторі, підготовлену Міністерством збройних сил. У ній прямо зазначається, що міжнародне гуманітарне право застосовується до кібердій під час збройного конфлікту. Франція наголошує на необхідності суворого дотримання принципів розрізнення, пропорційності та гуманного ставлення, включно з забороною нападів на об'єкти цивільної інфраструктури, навіть якщо вони є цифровими за своєю природою [10].

Естонія, у свою чергу, підтримує повну застосовність гуманітарного права до дій у кіберпросторі. У своїй офіційній заяві 2021 року Міністерство закордонних справ Естонії підкреслило, що кіберзасоби не створюють правового вакууму, і що всі акти, які можуть бути розцінені як збройний напад, підпадають під існуючі норми міжнародного гуманітарного права. Особливий акцент зроблено на необхідності дотримання зобов'язань із захисту цивільного населення та об'єктів, що користуються особливим режимом захисту [11].

Велика Британія у своїй офіційній позиції підтверджує застосовність міжнародного гуманітарного права до дій у кіберпросторі в період збройного конфлікту. Наголошуючи, що правові норми збройного конфлікту не залежать від виду технологій, а кібератака може вважатися збройним нападом, якщо її масштаб і наслідки є еквівалентними до традиційного збройного насильства [12].

У цілому, зростання кількості офіційних державних позицій із питань правового режиму кіберпростору свідчить про поступове формування практики, яка з часом може набути характеру звичаєвої норми. Це підтверджує загальну тенденцію до визнання того, що кібератаки в умовах збройного конфлікту не виходять за межі правового поля, а мають регулюватися в межах існуючих міжнародно-правових механізмів.

Висновки. Отже, кібератаки, що здійснюються під час збройних конфліктів, підлягають оцінці крізь призму основоположних принципів міжнародного гуманітарного права. Попри технічну специфіку кіберпростору, принципи розрізнення, пропорційності та військової необхідності залишаються застосовними до тих дій, наслідки яких є співмірними з наслідками традиційного збройного насильства. Саме ці принципи визначають межі допустимого застосування кібератак та слугують основою для відмежування правомірних дій від порушень міжнародного гуманітарного права.

Особливого значення у цьому контексті набуває правова оцінка кібератак, спрямованих на об'єкти критичної інфраструктури, об'єкти подвійного призначення, а також на об'єкти, необхідні для виживання цивільного населення. У таких випадках застосовність принципів міжнародного гуманітарного права зумовлюється не технічним способом впливу, а характером і масштабом можливих гуманітарних наслідків для цивільного населення та цивільних об'єктів.

Водночас реалізація цих принципів у кіберпросторі супроводжується низкою складнощів, пов'язаних із визначенням правового статусу цифрових цілей, прогнозуванням непрямих і каскадних наслідків кібератак, а також оцінкою їх впливу в умовах збройного конфлікту. Саме тому застосування норм міжнародного гуманітарного права до кібератак потребує не створення окремого правового режиму, а послідовного тлумачення й адаптованого застосування вже чинних гуманітарно-правових принципів до реалій сучасної війни.

Загалом, застосовність принципів міжнародного гуманітарного права до кібератак під час збройних конфліктів є необхідною умовою збереження гуманітарних обмежень у цифровому середовищі. Подальший розвиток державної практики та уточнення підходів до правової оцінки кібератак мають важливе значення для забезпечення ефективного захисту цивільного населення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. International Committee of the Red Cross. International Humanitarian Law and Cyber Operations during Armed Conflicts. Geneva, 2021. DOI: https://doi.org/10.1017/S1816383120000478. URL: https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/ihl-and-cyber-operations-during-armed-conflicts-913.pdf (дата звернення: 24.04.2025).
2. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / ed. by M.N. Schmitt. Cambridge: Cambridge University Press, 2017. DOI: https://doi.org/10.1017/9781316822524. URL: https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf (дата звернення: 24.04.2025).
3. Додатковий протокол I до Женевських конвенцій від 12 серпня 1949 року. 1977. URL: https://zakon.rada.gov.ua/laws/show/995_199#Text (дата звернення: 27.04.2025).
4. Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 / International Committee of the Red Cross. Geneva : Martinus Nijhoff Publishers,

1987. URL: https://tile.loc.gov/storage-services/service/ll/llmlp/Commentary_GC_Protocols/Commentary_GC_Protocols.pdf (дата звернення: 27.04.2025).
5. Rule 14. Customary International Humanitarian Law. ICRC Database. URL: https://ihl-databases.icrc.org/en/customary-ihl/v1/rule14 (дата звернення: 11.05.2025).
6. International Committee of the Red Cross. The Potential Human Cost of Cyber Operations. Geneva, 2019. URL: https://www.icrc.org/en/document/potential-human-cost-cyber-operations (дата звернення: 11.05.2025).
7. Комісія міжнародного права ООН. Проєкт статей про відповідальність держав за міжнародно-протиправні діяння. Нью-Йорк: ООН, 2001. URL: https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf (дата звернення: 25.05.2025).
8. Rome Statute of the International Criminal Court. Rome, 17 July 1998. URL: https://www.icc-cpi.int/sites/default/files/2024-05/Rome-Statute-eng.pdf (дата звернення: 25.05.2025).
9. U.S. Department of Defense. Law of War Manual. Washington : Office of General Counsel, 2015. URL: https://media.defense.gov/2023/Jul/31/2003271432/-1/-1/0/DOD-LAW-OF-WAR-MANUAL-JUNE-2015-UPDATED-JULY%202023.PDF (дата звернення: 17.06.2025).
10. Ministry of the Armed Forces of France. International Law Applied to Operations in Cyberspace. Paris, 2019. URL: https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf (дата звернення: 17.06.2025).
11. Ministry of Foreign Affairs of Estonia. Estonia's Positions on International Law Applicable in Cyberspace. Tallinn, 2021. URL: https://vm.ee/en/activity/digital-and-cyber-diplomacy/international-law-and-cyberspace (дата звернення: 17.06.2025).
12. Government of the United Kingdom. Application of International Law to States' Conduct in Cyberspace: UK Statement. London, 2021. URL: https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement (дата звернення: 17.06.2025).

Дата першого надходження рукопису до видання: 1.03.2026
Дата прийняття до друку рукопису після рецензування: 20.03.2026
Дата публікації: 3.04.2026