УДК 327.432(477):351.848.2
DOI https://doi.org/10.32782/2524-0374/2024-10/115

КОНЦЕПТ «ВТРАТИ ФУНКЦІОНАЛЬНОСТІ» В КОНТЕКСТІ ВИЗНАННЯ КІБЕРАТАК ВОЄННИМ ЗЛОЧИНОМ

THE CONCEPT OF "FUNCTIONALITY LOSS" IN THE CONTEXT OF RECOGNIZING CYBERATTACKS AS WAR CRIMES

Бондаренко І.Д., к.ю.н.,
доцент кафедри кібербезпеки
Національна академія Служби безпеки України

Стаття присвячена аналізу можливості застосування міжнародного гуманітарного права до кібератак у контексті міжнародного збройного конфлікту. Автор розглядає проблеми захисту цивільного населення від кібератак, що стає надзвичайно актуальним в умовах активного використання кіберпростору державами для досягнення воєнних цілей. У статті обґрунтовано, що кібероперації, які призводять до припинення надання критично важливих для населення послуг, можуть кваліфікуватися як атаки у розумінні міжнародного гуманітарного права, навіть якщо відсутні фізичні руйнування чи загибель людей. Це стає можливим у випадку застосування концепту «втрати функціональності», яка обгрунтовує еквівалентність кібератак і кінетичних атак за їх наслідками втрати критичних життєзабезпечувальних послуг для цивільного населення. Розглядаються приклади атак на критичну інфраструктуру України з боку російських спецслужб, що призвели до перебоїв у постачанні електроенергії, порушень роботи комунікаційних мереж і супутникових систем.

Здійснено порівняльний аналіз концепту «фізичних наслідків» та «втрати функціональності», який засвідчує переваги останнього у контексті сучасних загроз та технологічних реалій. Наведені також аргументи щодо потенціалу використання концепту «втрати функціональності» Міжнародним кримінальним судом для розслідування воєнних злочинів у кіберпросторі, зокрема російських кібератак на українську критичну інфраструктуру. Стаття підкреслює важливість формування міжнародно-правового підходу до кібервійни і зазначає, що національна правова позиція України щодо застосування норм МГП до кібероперацій може мати далекосяжні наслідки для міжнародного права.

Ключові слова: атака, злочин, кібератака, критична інфраструктура, міжнародний збройний конфлікт, Міжнародний кримінальний суд, розслідування, спецслужба, хакер, шкідливе програмне забезпечення.

The article examines the applicability of international humanitarian law (IHL) to cyberattacks within the context of an international armed conflict. The author examines the issue of protecting civilians from cyberattacks, which has become particularly relevant amid the active use of cyberspace by states to achieve military objectives. The article substantiates that cyber operations leading to the disruption of critical services essential for civilians may be qualified as attacks under IHL, even in the absence of physical destruction or loss of life. This qualification becomes feasible through the application of the concept of «functionality loss», which equates cyberattacks with kinetic attacks based on the resulting loss of critical life-supporting services for the civilian population. Examples are provided of cyberattacks on Ukraine's critical infrastructure by russian intelligence services, which have led to power outages, disruptions in communication networks, and satellite systems.

A comparative analysis of the «physical consequences» and «loss of functionality2 concepts is conducted, highlighting the advantages of the latter in the context of modern threats and technological realities. The article also presents arguments for the potential application of the «functionality loss» concept by the International Criminal Court (ICC) to investigate war crimes in cyberspace, specifically russian cyberattacks on Ukraine's critical infrastructure. The study underscores the importance of developing an international legal approach to cyber warfare and notes that Ukraine's national legal stance on applying IHL to cyber operations could have far-reaching implications for international law.

Key words: attack, crime, cyberattack, critical infrastructure, international armed conflict, International Criminal Court, investigation, intelligence agency, hacker, malware.

Постановка проблеми. Міжнародне гуманітарне право формувалося задовго до появи комп'ютерів, кібервійськ і кібероперацій і наразі виявилося неадаптованим для захисту цивільного населення від новітніх загроз. Ці загрози були масштабно реалізовані в Україні, де російські спецслужби здійснили низку безпрецедентних кібератак на невоєнну критичну інфраструктуру України, спричинивши, зокрема, регіональний блекаут, комунікаційний аутедж провідного мобільного оператора, а деякі із загроз навіть вийшли за межі України, яскраво демонструючи свою невибірковість, наприклад, спричинивши блокування супутникової мережі KA-SAT Viasat в ЄС.

Українці, як ніяка інша нація, на власному досвіді розуміємо, що настав час, коли право має наздогнати практику і справедливість має бути відновлена. Невизначеність агресор сприймає як слабкість і зловживає нею. У кібер-домені ця невизначеність пов'язана із відсутністю на даний момент чіткої міжнародно-правової регламентації меж дозволеності використання державами кіберпростору у міжнародних збройних конфліктах. Здійснюються спроби внормування цього питання, але дієвого результату вони не принесли з огляду конфронтаційні позиції окремих країн в умовах глобальної нестабільності.

Підготовлений міжнародною групою експертів під егідою Об'єднаного центр передових технологій з кібероборони НАТО (CCCCOE NATO) «Талліннський посібники про застосування міжнародного гуманітарного права до кібероперацій» (№ 1 і № 2) є лише аналітично-консультативними джерелом, але їх розробка відобразила відсутність консенсусу між експертами із низки принципових питань щодо меж законності проведення кібероперацій у контексті збройного конфлікту.

Реальні кейси масштабних кібератак росії на Україну, розуміння у світі значення фактичних наслідків таких атак, їх здатності до масштабування та впливу на критичні для функціонування держави і життя соціуму сервіси, – все це сприяло посиленню позиції щодо необхідності переосмислення міжнародно-правового змісту кібератак крізь призму міжнародного гуманітарного та міжнародного кримінального права. Україна є у фарватері цього процесу, а формування національної правової позиції щодо застосування МГП до кібероперацій, вірогідно, матиме визначальні міжнародно-правові наслідки у майбутньому.

Аналіз останніх досліджень і публікацій. Визначення міжнародно-правового змісту кібератак та меж дозволеності проведення кібероперацій у котексті міжнародного збройного конфлікту є невирішеним і суперечливим. Зазначене питання у глобальному дискурсі становить складну наукову проблему, а в Україні є новим, надзвичайно актуальним, але малодослідженим. У вересні 2024 року Національним координаційним центром кібербезпеки при РНБО України в рамках Національного кластера кібербезпеки із залученням науковців, експертів та практиків було проведено перший воркшоп, присвячений питанням визначення національної позиції України щодо застосування норм міжнародного гуманітарного

права до проведення кібероперацій [1]. Основні положення даної статті були презентовані під час зазначеного науково-експертного форуму.

Окремі аспекти визначення міжнародно-правового змісту кібероперацій у своїх наукових роботах висвітлювали Секретар НКЦК РНБО України Н. А. Ткачук [2] та Народний депутат України, голова підкомітету цифрової інфраструктури, електронних комунікацій та смарт-інфраструктури О. П. Федієнко [3]. Заслуговують також на увагу роботи таких вчених-юристів як К. В. Юртаєва [4], В. В. Музика [5], Г. В. Фещуков [6]. Інтерес становлять і праці іноземних наковців, зокрема, керівника проєкту «Tallin Manual» Michael N. Schmitt [7], а також Aisha Ayub [8] та Duncan B. Hollis [9].

Мета статті: розкрити сутність концепту «втрати функціональності» в контексті визначення міжнародно-правового зміту кібератк як воєнних злочинів та формування національної позиції України щодо застосування норм міжнародного гуманітарного права до проведення кібероперацій.

Виклад основного матеріалу. Занепокоєність на міжнародному рівні глобальною тенденцією стрімкої мілітаризації кіберпростору призвела до створення в структурі ООН робочих груп, метою яких була розробка певних універсальних правил поведінки держав у кіберпросторі. Зокрема:

– з 2004 по 2021 рік функціонувала так-звана група урядових експертів (GGE), яка мала окремі 3 скликання, і у своїх звітах 2010, 2013 років вперше сформувала позицію, що МГП застосовується до кіберпростору, а у фінальному звіті 2021 року – що МГП застосовується щодо кібератак під час збройних конфліктів;

– з 2018 року мандатом до 2025 функціонує відкрита робоча група (OEWG), яка також аргументує загальну обґрунтованість застосування МГП до кібероперацій. OEWG у звіті 2021 року висловлює позицію, що кібератаки, які призводять до пошкодження або виведення з ладу критичної інфраструктури, можуть бути розцінені як порушення міжнародного права, що підриває державний суверенітет та міжнародну безпеку.

Певним підсумком їх діяльності стало ухвалення у 2015 році резолюції Генеральної Асамблеї ООН 70/237, де зазначено, що МГП застосовується до кібероперацій, а держави повинні дотримуватися принципів гуманності, необхідності та пропорційності у використанні інформаційно-комунікаційних технологій у міжнародних конфліктах.

Резолюція задала загальний вектор, без конкретики щодо застосування МГП до кіберпорацій. Але слід наголосити, що вже на перших в цій сфері етапах, наприклад, під час формування звіту GGE 2017 року, такі країни як росія, Китай та Куба заперечували саму ідею застосування МГП до кіберпростору, аргументуючи це тим, що така регламентація МГП начебто стимулюватиме мілітаризацію кіберпростору.

Але навіть за наявності зазначеної резолюції ключовою проблемою застосування міжнародного гуманітарного права, а з ним – і міжнародного кримінального права, до кібероперацій залишається питання: чи можуть комп'ютерні дані (зокрема цивільні) вважатися обєктом нападу у розумінні МГП, і, відповідно, чи рівнозначна кібератака поняттю «атака» за МГП, здійснення якої на цивільні об'єкти і цивільне населення заборонено, і є злочином згідно частини 2 статті 8 Римського Статуту Міжнародного Кримінального Суду (підпункти «i» «ii», «iv», «v», «xx» пункту «b») [10].

Детальна дефініція поняття «атака» у нормах МГП відсутня. Натомість певними «відправними точками» тут можна вважати положення:

– IV Гаазької конвенції про закони і звичаї війни на суходолі та додаток до неї: Положення про закони і звичаї війни на суходолі, де зазначено «Забороняється будь-яким способом атакувати чи бомбардувати незахищені міста, селища, житлові будинки чи споруди» (ст. 25);

– Додаткового протоколу I від 1977 року до Женевських конвенцій 1949 року, що стосується захисту жертв міжнародних збройних конфліктів, де, зокрема, атаку визначено як «акти насильства щодо супротивника, незалежно від того, здійснюються вони під час наступу чи під час оборони» (ст. 49-1) і встановлено, що «цивільне населення як таке, а також окремі цивільні особи не повинні бути об'єктом нападів. Заборонено акти насильства чи загрози насильства, що мають головною метою тероризувати цивільне населення» (ст. 51-2), «Нападиневибіркового характеру заборонено» (ст. 51-4); «Цивільні об'єкти не повинні бути об'єктом нападу або репресалій» (ст. 52-1) [11].

Але із цих міжнародно-правових положень неможливо однозначно встановити яким чином кібератаки корелюють з атакою в розумінні МГП. При роботі над так-званими «Таллінським посібниками» експерти також не були одностайним, тому закріплення отримала лише базова «мінімальна» позиція, із якою погодилися вони всі. Правило 92 Tallin Manual 2.0 2017-го року говорить «кібероперація» може вважатися «атакою» згідно МГП, якщо вона: «очікується, що призведе до смерті, поранень або фізичної шкоди» або «спрямована на заподіяння такої шкоди» або «є частиною більшої атаки, яка, очікується, призведе до такої шкоди». За таких умов кібератака, у випадку її спрямованості на цивільні об'єкти чи цивільне населення, становить воєнний злочин (правило 101, 102) [12]. Тобто згідно позиції Tallinn Manual 2.0 кібератака набуває правового змісту «атаки» за МГП лише тоді, коли її наслідки співрозмірні із наслідками атак кінетичною зброєю: смерть, поранення, фізичне руйнування об'єктів.

Так само і Червоний Хрест у своєму офіційному коментарі від 2020 р. до вищезазначеної Конвенції акцентував на певній експертній одностайності, що у випадку фізичних наслідків смерті, поранень, руйнувань, кібератака еквівалентна атаці з позиції МГП. Натомість Червоний Хрест вказує, що у випадку відсутності таких фізичних наслідків, а лише порушення (блокування) кібератакою функціонування інфраструктури, питання відповідності кібератаки порогу серйозності атаки згідно МГП залишається відкритим і ще належить визначити.

Визначення кореляції кібератаки із атакою за МГП спираючись виключно на критерій обов'язкових наслідків знищення об'єкта або смерті чи поранень людей у науці отримав назву «концепт прямих фізичних наслідків». Але практика кібератак на Україну засвідчує цілу низку його недоліків. Постає питання, чи взагалі логічним є механічне перенесення налаштованих для умов кінетичної війни запобіжних механізмів захисту цивільного населення на абсолютно новий кібернетичний театр бойових дій, де, на відміну від фізичного світу, функціонують зовсім інші кореляції взаємодій.

Візьмемо положення згаданого Додаткового протоколу I до Женевських конвенцій про заборону атак на цивільні об'єкти, історію їх появи. Вони з'явилося як частина реакції за результатами обговорення делегатами на конференції наслідків бомбардувань Другої світової війни таких міст як Дрезден, Лондон, Хіросіма і Нагасакі, що стали однією з основних причин численних жертв серед цивільного населення. На той час (за відсутності систем комп'ютеризації) механічна цілісність об'єкта означала виконання ним життєзабезпечувальної функції для населення, наприклад функції електропостачання. В умовах сьогодення ця критична функція може бути припинена і без бомбардування приміщень, де розміщене певне технологічне устаткування, а шляхом точкового виведення з ладу цього устаткування завдяки кібератаці, зокрема, без перспективи оперативного віднофлення функціонування системи. Тобто маємо ті самі наслідки, що і у випадку зруйнованої споруди – її необхідно відбудовувати так само

як і відновлювати роботу комп'ютерної системи, наприклад типу SCADA, після кібератаки і знищення її даних і управляючих програм.

Протягом останніх років набуває розвитку інша науково-експертна позиція, відома під назвою «концепт втрати функціональності». Низка західних науковців, зокрема, Aisha Ayub [8] та Duncan B. Hollis [9], а також і керівник проєкту Tallin Michael Schmitt [7] у своїх роботах приходять до висновків, що сучасні кібератаки, навіть якщо вони не спричиняють фізичної шкоди, можуть мати серйозні гуманітарні наслідки, що вказує на необхідність розширення тлумачення «атаки» за МГП, щоб охопити такі нематеріальні атаки як атаки на критичну інфраструктуру, оскільки втрати функціональності таких систем, як енергетичні чи комунікаційні мережі, можуть мати серйозний вплив на цивільне населення, навіть за відсутності фізичного руйнування об'єктів. Вони обґрунтовують, що поріг серйозності для воєнних злочинів, який визначає Римський статут, базується на застарілих уявленнях про війну.

Поворотними етапами розвитку концепту втрати функціональності можна вважати:

1) два послідовних звернення Центру прав людини Каліфорнійського університету в Берклі (Berkeley Human Rights Center), направленого прокурору Міжнародного Кримінального Суду у 2022 році;

2) очевидно, його реакцію на це звернення, яка відображена у опублікованій на сайті Foreign Policy у 2023 році статті «Technology Will Not Overcome Our Humanity», промовиста назва якої відсилає до відомого вислову Албьерта Енштейна [13].

Щодо першого. В запитах містилося юридичне обґрунтування клопотання: «розширити сферу розпочатого розслідування, включивши до нього кібердомен поряд із традиційними театрами бойових дій враховуючи приклади агресивної кіберактивності рф в Україні». Запит був направлений прокурору МКС одразу після визнання ним у березні 2022 року у своєму зверненні до Ради Безпеки ООН факту міжнародного збройного конфлікту на території України, що триває з 20.02.2014, та оголошення про початок розгляду справи щодо можливих воєнних злочинів, вчинених на території України у межах розслідування, що охоплює «будь-які минулі та теперішні звинувачення у воєнних злочинах, злочинах проти людяності чи геноциді, скоєних на будь-якій частині території України будь-якою особою». Останнє, зокрема, поряд з тим, що МКС не визнає імунітети навіть глав держав, є вкрай важливим в контексті виходу рф зі складу МКС – цей факт ніяким чином не може і не обмежує юриздикцію МКС щодо воєнних злочинів громадян рф на території України в міжнародно-визнаних кордонах 1991 року.

Перший із запитів групи Берклі 2022 року, стосувався звинувачення proxy ГУ ГШ ЗС рф хакерського угрупування Sandworm у кібератаках на об'єкти енергетики України, а саме на підстанції «Прикарпаттяобленерго» у 2015 році та на підстанцію «Північна» «Укренерго» у 2016 році. Другий – щодо кібератки «NotPetya» та кібератаки на Viasat. У зазначених запитах, а так само і в низці особистих наукових статей керівник зазначеної правозахисної групи, пані Ліндсі Фрімен, наголошувала на декількох аргументах, чому відповідні звинувачення є обґрунтованими та мають перспективи судового розслідування. Зокрема, вони є вже детально розслідуваними як приватними структурами, так і в межах американської судової системи, де висунуто офіційне звинувачення російським хакерам Sandworm, ідентифікованим як співробітники ГУ ГШ рф. Ці кібератаки здійснювалися в контексті міжнародного збройного конфлікту, факт якого офіційно визнаний. Чітка цивільна ціль кібератк, хоча б тому, що на момент їх проведення ні Західна Україна, ні Київ не були зоною бойових дій.

І ключове, у запитах обґрунтовується застосування до кейсів кібератак на Україну концепту «втрати функціональності»: зазначається, що втрата функціональності цивільних критичних інфраструктур (енергетичних, медичних, комунікаційних) через кібератаки повинна розглядатися як напад у контексті МГП, навіть якщо фізичного руйнування не відбулося, оскільки може мати такий самий руйнівний вплив, як і фізичні атаки

Прокурор МКС прийняв до розгляду звернення групи Берклі Каліфорнійського Університету. І у серпні 2023 Карім Хан у своїй опублікованій статті заявив про свій намір розслідувати кібератаки як воєнний злочин: «Спроби вплинути на критично важливу інфраструктуру… можуть призвести до негайних наслідків для багатьох, особливо для найбільш уразливих… Хоча жодне положення Римського статуту не стосується кіберзлочинів, така поведінка потенційно може відповідати елементам багатьох основних міжнародних злочинів… У рамках своїх розслідувань мій офіс збиратиме та розглядатиме докази такої поведінки. У статті також засуджується використання кібероперацій як частини «гібридної стратегії» або «сірої зони» та наголошується, що наразі між державами з'являється консенсус, що кіберпростір «не є особливою сферою, вільною від регулювань», напроти, міжнародне право «має відігравати тут чітку роль». Акцентовано увагу на історичній ролі МКС в контексті формування правил поведінки держав у кіберпросторі: «Міжнародне кримінальне правосуддя може і повинно адаптуватися до нового ландшафту…Юрисдикція МКС може стати важливою частиною колективної відповіді… МКС може стримувати порушників…, його провадження можуть допомогти пом'якшити неоднозначність гібридних стратегій…, допомогти державам та іншим органам діяти відповідно до їх чинного законодавства».Прокурор МКС також апелює до попередньо висловленої позиції Міжнародного комітету Червоного Хреста, що «кібератаки мають відповідати основним принципам розрізнення та пропорційності та мають бути спрямовані лише проти воєнних цілей» [13]. Пізніше речник Офісу Прокурора МКС підтвердив, що відповідне розуміння кібератак є офіційною позицією організації.

Таким чином існують реальні передумови та перспективи юридичного закріплення концепту «втрати функціональності» в контексті порядку застосування МГП до кібероперацій. Це може відбутися в межах прецеденту за результатами розслідування Прокурором МКС російських кібератак на критичну інфраструктуру України як воєнних злочинів. Концепт «втрати функціональності» є більш прогресивним ніж концепт «фізичних наслідків» і певною мірою корелює із положеннями, ст. 52 (2) Додаткового протоколу до Женевських конвенцій 1949 року ,що напад можна вважати таким, що мав місце коли ціль «нейтралізована», а не повністю знищена. Стосовно кібератак вона вперше була запропонована у 2021 році так званою «Радою радників», міжнародною групою юристів, створеною відповідно до резолюції Генеральної Асамблеї ООН A/RES/73/262 під егідою Постійної місії Ліхтенштейну при ООН у відповідь на стурбованість низки держав зростаючою загрозою кібератак. У підготовленому групою звіті «Щодо застосування Римського статуту МКС до кібервійни» міститься рекомендація вважати, що «припинення функціонування критичної інфраструктури держави чи створення перешкод військовим можливостям, навіть якщо критична інфраструктура чи військова техніка фізично не знищені, може кваліфікуватися як напад відповідно до МГП» [14].

Спираючись на концепцію «наслідків втрати функціональності», група юристів Каліфорнійського Університету наголошувала, що кібератаки на критичну інфраструктуру є атаками на кожного споживача відповідних життєво-важливих послуг: «це були не просто атаки на кон-

кретні інфраструктурні об'єкти, а на опалення, яке зігріває людей взимку; системи охолодження, які перешкоджають псуванню їжі, світлофори, що забезпечують громадську безпеку; фінансові послуги, які надають засоби для існування та підтримують обмін найважливішими товарами та послугами; медичні установи, які забезпечують життя та здоров'я населення; системи, які ізолюють небезпечні ядерні та хімічні об'єкти; а також транспорт, комунальні послуги та зв'язок, які з'єднують українську громаду в середині країни та із зовнішнім світом».

Висновки. Наразі відсутня узгоджена міжнародна позиція щодо порядку застосування МГП до кіберопераций. Існує ряд досить ініціатив, зокрема, щодо створення нової, так-званої "Цифрової Женевської конвенції", створення багатостороннього механізму відповідальності для протидії зловмисній кіберактивності, створення міжнародного органу, подібного за функціями до Міжнародного агентства з атомної енергії, який міг би забезпечити нагляд і розслідування зловживань державами у проведенні кібероперацій. Але в існуючих геополітичних реаліях перспективи їх імплементації малореалістичні. Натомість низка країн, таких як Франція, Нідерланди, Фінляндія та Естонія на рівні внутрішнього законодавства, а також на рівні офіційних урядових заяв щодо національної позиції стосовно застосування міжнародного права в кіберпросторі вже використовують саме концепт «втрати функціональності». Наприклад, Франція визнає, що втрата функціональності об'єктів, зокрема енергомереж або телекомунікацій, навіть без фізичного руйнування або жертв, може мати катастрофічні наслідки для держави та цивільного населення і може розглядатися як атака за МГП та класифікуватися як воєнний злочин. Саме таку на правову позицію має спиратися Україна розслідуючи кібератаки рф на свою критичну інфраструктуру як воєнні злочини. Такий підхід має бути використаний і Міжнародним кримінальним судом.

ЛІТЕРАТУРА

1. НКЦК провів воркшоп щодо застосування міжнародного гуманітарного права до проведення кібероперацій. *Рада національної безпеки і оборони України* : веб-сайт. URL: https://www.rnbo.gov.ua/ua/Diialnist/6998.html (дата звернення: 30.10.2024).
2. Ткачук Н. А. Досвід США зі створення та розбудови Кіберкомандування: уроки для України. *Інформація і право*. 2024. № 1 (48). С. 139-149.
3. Федієнко О. П. Загрозливі тенденції використання державою-агресором шкідливого програмного забезпечення в умовах правового режиму воєнного стану. *Інформація і право*. 2023. № 3 (46). С. 142-153.
4. Юртаєва К. В. Кримінальна відповідальність за кіберзлочини, вчинені під час збройного конфлікту: міжнародні тенденції та українські реалії. *Юридичний науковий електронний журнал.* 2012. № 12. С. 409-414.
5. Музика В. В. Атрибуція кібератак проти об'єктів критичної інфраструктури: визначення основних проблем та шляхів їх вирішення : дис. … д-ра філософії : 081 / Нац. ун-т. «Одеська юридична академія». Одеса, 2021. 219 с.
6. Фещуков Г. В. Застосування МГП по відношенню до кібероперацій, що проводяться під час збройних конфліктів. *Юридичний науковий електронний журнал*. 2023. № 9. С. 437-439.
7. A Policy Approach for Addressing the "Cyber Attacks" and "Data as an Object" Debates. *Lieber Institute*. *West Point* : веб-сайт. URL: https://lieber.westpoint.edu/policy-approach-addressing-cyber-attacks-data-object-debates/ (дата звернення: 30.09.2024).
8. Cyber Operations falling under "Attack" in IHL. *DLP Forum. Diplomacy. Law. Policy* : веб-сайт. URL: https://www.dlpforum.org/2023/09/06/cyber-operations-falling-under-attack-in-ihl/ (дата звернення: 30.09.2024).
9. A Victim's Perspective on International Law in Cyberspace. *Lawfare* : веб-сайт. URL: https://www.lawfaremedia.org/article/a-victim-s-perspective-on-international-law-in-cyberspace (дата звернення: 30.09.2024).
10. Римський статут Міжнародного кримінального суду. *Міністерство юстиції України* : веб-сайт. URL: https://minjust.gov.ua/m/mijnarodniy-kriminalniy-sud (дата звернення: 30.09.2024).
11. Що стосується захисту жертв збройних конфліктів неміжнародного характеру : Додатковий протокол до Женевських конвенцій від 9 чер. 1977 р. URL: https://zakon.rada.gov.ua/laws/show/995_200#Text (дата звернення: 30.09.2024).
12. Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare. *Cambridge University* : веб-сайт. URL: https://assets.cambridge.org/ 97811071/77222/frontmatter/9781107177222_frontmatter.pdf (дата звернення: 30.09.2024).
13. Technology Will Not Exceed Our Humanity. *Digitalfrontlines* : веб-сайт. URL: https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/: (дата звернення: 30.09.2024).
14. The Council of Advisers' Report on the Application of the Rome Statute of the International Criminal Court to Cyberwarfare Prepared by the Permanent Mission of Liechtenstein to the United Nations. *The Global Institute for the Prevention of Agression* : веб-сайт. URL: https://crimeofaggression.info/the-campaign/the-council-of-advisers-on-the-application-of-the-rome-statute-to-cyberwarfare/ (дата звернення: 30.09.2024).