УДК 341.3:327.5
DOI https://doi.org/10.32782/2524-0374/2024-5/131

РОСІЙСЬКІ ЗАСОБИ КІБЕРВІЙНИ: МІЖНАРОДНО-ПРАВОВИЙ АСПЕКТ

RUSSIAN CYBER WARFARE MEANS: INTERNATIONAL LEGAL ASPECT

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

У статті розглядається правовий зміст поняття «кіберзброя», що може застосовуватись як засіб нападу під час міжнародного збройного конфлікту. Охарактеризовано функціональне призначення програмного забезпечення «Скан-В» як складової «Програмно-апаратного комплексу централізованого управління силами спеціального призначення», розробленого російською кібербезпековою кампанією «НТЦ Вулкан» на замовлення воєнної розвідки рф для здійснення глобального автоматизованого збору даних про вразливості програмного забезпечення на об'єктах-цілях, керування проведенням кібератак шляхом експлуатації виявлених вразливостей. Визначено, що такий функціонал програмних засобів потенційно дозволяє припиняти роботу об'єктів кібератак без їх фізичного знищення чи руйнування. Розглянуто актуальні тенденції розвитку міжнародного права в частині застосування концепції «втрати функціональності» для визначення змістовної відповідності кібератак збройному нападу. Обґрунтовано, що кібератаки можуть бути рівноцінними атакам кінетичною зброєю та становити воєнні злочини у випадку, якщо вони спрямовуються проти критичної інфраструктури та призводять до припинення отримання цивільним населенням відповідних послуг. Це відбувається завдяки виведенню з ладу інформаційних систем та втрати об'єктами своєї функціональності. Наведені аргументи щодо помилковості раніше пропонованої експертами концепції «фізичних наслідків», згідно якої критерієм відповідності кібератак поняттю «атака» за міжнародним гуманітарним правом вважалося виключно спричинення нею руйнувань, загибелі чи поранення людей. Визначено умови, за яких розроблене «НТЦ Вулкан» програмне забезпечення обґрунтовано розглядати як зброю, тобто засіб нападу під час збройного конфлікту.

Ключові слова: кіберзброя, хакер, спецслужба, програмний засіб, SCADA, кібератака, злочин, агресія, самооборона, критична інфраструктура, міжнародний збройний конфлікт, Міжнародний кримінальний суд.

The article examines the legal content of the concept of «cyber weapon», which can be used as a means of attack during an international armed conflict. The functional purpose of the «Scan-V» software as a component of the «Software and hardware complex of centralized control of special purpose forces» developed by the russian cyber security campaign «NTC Vulkan» at the request of the russian military intelligence is conducting global automated data collection regarding target objects software vulnerabilities and managing cyber-attacks by exploiting identified vulnerabilities, is characterized. It is determined that such software functionality potentially allows stopping the objects functioning without their physical destruction. The current international law development trends regarding the application of the concept of «functionality loss» to determine the substantive equivalence of cyber-attacks to armed attacks are discussed. It is argued that cyber-attacks can be equivalent to kinetic weapon attacks and constitute war crimes if they are directed against critical infrastructure and lead to the cessation of civilian access to relevant services. This occurs through the disruption of information systems and loss of functionality by the objects. Arguments are provided regarding the fallacy of the previously proposed concept of «physical consequences», according to which the criterion for the correspondence of cyber-attacks to the concept of «attack» under international humanitarian law was considered exclusively in connection to destruction, death, or injury to people consequences. The conditions, under which the software developed by «NTC Vulkan» is justified as weapon during an armed conflict, are determined.

Key words: cyber weapon, hacker, intelligence service, software tool, SCADA, cyber-attack, crime, aggression, self-defense, critical infrastructure, international armed conflict, International Criminal Court.

Постановка проблеми. Масштаб кібератак рф на Україну, які відбуваються в контексті визнаного Міжнародним Кримінальним Судом (далі – МКС) міжнародного збройного конфлікту, є безпрецедентним.

Така безпрецедентність зумовлена:

а) високою інтенсивністю кібератак за кількістю їх технологічною складністю;

б) їх акторами, якими є спецслужби країни агресора, що виконують розпорядження вищого воєнно-політичного керівництва рф;

в) їх цілями, якими переважно є критична інфраструктура України, зокрема, цивільні (невоєнні) об'єкти.

Напади на цивільні об'єкти, цивільне населення та застосування невибіркової зброї заборонено міжнародним гуманітарним правом і є злочином згідно Римського статуту МКС. Але за відсутності профільної міжнародної конвенції питання порядку поширення цієї загальна заборона на кіберпростір є невирішеним. Дискусійним є за яких умов кібератака підпадає під поняття «напад» та, відповідно, чи можуть комп'ютерні програми розглядатися як засіб нападу, тобто як зброя.

Важливою віхою у цій дискусії стала заява Прокурора МКС у серпні 2023 року. Він визнав, що за певних обставин кібератаки можуть становити воєнний злочин та повідомив про свій намір у подальшому розслідувати їх. Хоча безпосередньо він не вказував на кібератаки проти України, але його заява відбулася невдовзі після звернення правозахисної групи Берклі з Каліфорнійського університету із аргументацією, що безпрецедентні кібератаки на критичну інфраструктуру України мають розглядатися як воєнні злочини.

Невдовзі після повномасштабного вторгнення рф в Україну завдяки так-званому «зливу» даних російської приватної ІТ-кампанії « НТЦ Вулкан» вперше стало відомо про комп'ютерні програми, які були розроблені нею для російських спецслужб. І хоча у відкритому доступі наразі нема інформації щодо їх використання для кібератак проти України, аналіз функціоналу відповідних програмних засобів в контексті дослідження здійснених росією кібератак на цивільні об'єкти критичної інфраструктури як нашої країни, так низки західних держав дозволяє вперше предметно розглянути технологічні можливості цих програмних засобів під призмою міжнародного права як засобу нападу, тобто як зброї, що застосовується у кіберпросторі. Розвиток наукової думки у цій сфері сприятиме формуванню теоретичного підґрунтя для ухвалення конкретних процесуальних рішень у межах розслідувань кібератак рф проти України як воєнних злочинів.

Аналіз останніх досліджень і публікацій. Визначення змісту поняття «кіберзброя» як засобу нападу в контексті міжнародного збройного конфлікту знаходиться на межі права і технології, є складним, багатоаспектним та недостатньо дослідженим. На національному рівні воно лише опосередковано піднімалося у наукових роботах, присвячених тенденціям російської деструктивної кіберактивності та перспективам інституційного формування українських кіберсил таких експертів-практиків як Олександр Федієнко [1; 2] та Наталія Ткачук [3]. Серед останніх про-

фільних досліджень також слід відмітити роботи іноземних вчених-юристів Freeman L. [4] та Chan Yoon Onn [5].

Мета статті: охарактеризувати функціональне призначення програмних засобів «Скан-В» та «Кристал-2В», розроблених компанією «НТЦ Вулкан» для потреб ГУ ГШ рф, визначити міжнародно-правовий зміст діянь із застосування таких засобів для кібератак на цивільні об'єкти та цивільне населення в контексті міжнародного збройного конфлікту.

Виклад основного матеріалу. У 2022 році через декілька днів після повномасштабного вторгнення рф в Україну на адресу німецької газети Süddeutsche Zeitung було анонімно направлено архів внутрішніх файлів російської недержавної IT-кампанії «НТЦ Вулкан», який містив понад 1000 документів з грифами обмеження доступу – 5299 сторінок тексту технічної документації на три розроблені компанією пакети програмного забезпечення «Амезіт», «Скан-В» та «Кристал-2В», а також відповідне внутрішнє листування 2016–2021 років. Було проведене масштабне журналістське розслідування із залученням 10 авторитетних світових ЗМІ з 8 країн (Der Spiegel, Guardian, Washington Post, Der Standard, Le Monde, DR, Tamedia Group, IStories), а також провідних кібербезпекових кампаній Mandiant, Dragons, Spiderlabs. Автентичність файлів була підтверджена п'ятьма західними спецслужбами.

«Скан-В» – програмний засіб, розроблений «НТЦ Вулкан», який заслуговує особливої уваги в контексті теоретичного осмислення поняття «кіберзброя» в його міжнародно-правовому розумінні як засобу нападу. Згідно технічної документації програмний засіб обробляє дані із ступнем секретності «Цілком таємно». «Скан-В» є частиною більшої системи, яка називається «Програмно-апаратний комплекс централізованого управління силами спеціального призначення («ПАК ЦУСС»)», та призначена для «комплексного управління спеціальними силами та засобами і підтримки прийняття рішень щодо підготовки та проведення спеціальних заходів».

«Скан-В» призначений для автоматизованого пошуку і збору великих обсягів даних щодо наявних вразливостей програмного забезпечення, встановленого у комп'ютерних системах заздалегідь визначених у «ПАК ЦУСС» об'єктів пошуку по всьому світу. Такі об'єкти розглядаються як цілі майбутніх кіберударів. Зібрана програмним засобом інформація щодо них дозволяє індивідуально структурувати кібератаки заздалегідь, орієнтуючись на конфігурацію апаратного і програмного забезпечення на об'єкті-цілі та наявні вразливості, які експлуатуються для деструктивного впливу. Він складається з таких компонентів:

1) база даних, де накопичується інформація про ідентифіковані вразливості та мережеву інфраструктуру об'єктів;

2) інструменти збору даних: автоматизовані сканери, веб-скрепери для виявлення вразливостей;

3) платформа обробки та керування, яка призначена для координації діяльності операторів із збору, аналізу даних та проведення кібератак [6].

Вищезазначений програмний засіб об'єднує різні методи сканування, щоб зібрати всю можливу інформацію про комп'ютерну систему об'єкта-цілі кібератаки, включаючи управлінські та організаційні дані. Використовується як невідомий спеціалізований веб-скенер російської розробки, так і загальнодоступні продукти: Nmap, Nessus Network Monitor, інформаційні ресурси: ripe.net, arin.net, Shodan, mitre.org, nist.gov. Цільовими елементами сканування є параметри Cisco, файли електронної пошти, бази даних електронної пошти, трафік Pcaps.

«Скан-В» має графічний інтерфейс, який підтримує візуалізацію мережі та цільової географії. У файлах вищезазначеного архіву містяться знімки екрану інтерфейсу «Скан-В», аналіз яких відображає розташування основних об'єктів-цілей кібератак, чимало з яких розміщені в США. Серед цілей – об'єкти енергетики, наприклад, атомна електростанція поблизу м. Берн, Швейцарія.

«Скан-В» є складовою вищезазначеного «ПАК ЦУСС», який у свою чергу є інструментом управління цільовою підготовкою і проведенням кібератак, дозволяє розподіляти ролі операторів, ставити задачі та перевіряти їх виконання. Функціонально передбачено можливість синхронної командної роботи над одним завданням територіально віддалених операторів [7].

Згідно технічної документації «ПАК ЦУСС» забезпечує: постановку завдань при підготовці та проведенні спеціальних заходів та делегування завдань з урахуванням розподілених систем введення-виведення інформації та ієрархії ролей користувачів; подання ситуаційної інформації в графічній формі операторам підсистеми управління абонентським шлейфом (PU-L); передачу даних про об'єкти в АПК «Скан-АС» (підсистема «Сховище»); зберігання бланків об'єктів і сценаріїв спеціальних заходів; обмін даними між перспективними територіально розподіленими спецпідрозділами; комплексне управління перспективними територіально розподіленими спецпідрозділами; тиражування даних із зовнішніх джерел на локальне сховище АПК «Скан-АС» (підсистема «Збір»); агрегування отриманої інформації з можливістю децентралізованої обробки даних; оновлення інформації про інформаційно-комунікаційні мережі та уразливості елементів, що зберігаються в децентралізованій базі даних, на основі даних із зовнішніх джерел; візуалізація інформації з бази даних на неоднорідному графі з можливістю оновлення топології мережі та вразливостей на основі даних із зовнішніх джерел; ручне введення даних про персонал, штатну структуру та прив'язку до топології мережі (назва підрозділів, посади, e-mail, коментарі тощо); побудова, редагування та візуалізація графів багаторівневої гетерогенної мережевої інфраструктури.

Інформаційні потоки в середині «ПАК ЦУСС» побудовані з урахуванням рівнів обмеження доступу, взаємодії між вузлами системи за допомогою API, «ручного» перенесення інформації фізичним носієм (CD/DVD/USB) із «відкритого» серверу на так-званий «закритий контур» [8].

«Кристал-2Б» – це інший програмний продукт, розроблений «НТЦ Вулкан», який безпосередньо пов'язаний із «Скан-Б». Згідно технічної документації його метою є «всебічна підготовка спеціалістів з інформаційного протиборства». «Кристал-2Б» є навчальною платформою, яка забезпечує підготовку операторів до використання різноманітних сценаріїв наступальних і оборонних дій у кіберпросторі, зокрема, здійснення цільових атак на критичну інфраструктуру. Це включає кібернетичний вплив на промислові SCADA системи з метою «виведення з ладу систем управління електро- і водопостачанням, залізничним, авіаційним і морським транспортом, інших життєво-важливих сфер». Основна увага приділяється «несанкціонованому доступу» до критичних мереж і «виявленню слабких місць» у цільовій системі, плануванню і проведенню кібератак різноманітних типів. «Кристал-2Б» передбачає одночасну підготовку до 30 операторів, навчання включає як теоретичні блоки, так і виконання практичних і лабораторних занять у симульованій віртуальній інфраструктурі.

Аналіз технічної документації та службового листування «НТЦ Вулкан» свідчить про розробку вищезазначених програмних засобів безпосередньо для профільного кіберпідрозділу російської армії, відповідального за здійснення масштабних кібератак на об'єкти критичної інфраструктури як в Україні, так і в низці країн ЄС і в США. Компанія-розробник «НТЦ Вулкан» публічно позиціонує себе як кібербезпекова організація із штатом 120 співробітників і формально є недержавною. Водночас вона має тісні зв'язки із російськими спецслужбами і була заснована у 2010 році двома старшими офіцери у відставці, які є випускниками Санкт-Петербурзької військової академії, а з 2011 року отримала право працювати із секретними воєнними проектами.

Формальним замовником «Скан-В» є Інститут інженерної фізики, який тісно пов'язаний з ГУ ГШ рф. Аналіз файлів вищезазначеного архіву свідчить, що фактичним замовником є військова частина № 74455. У листуванні містяться згадки про візити співробітників «НТЦ Вулкан» на режимний об'єкту у м. Хімки, де розміщена згадана військова частина. У документації описується «протокол обміну даними» із вже існуючими російськими військовими базами даних «PU-L», «PSAP» та Scan-AS», що містять інформацію про вразливості програмного та апаратного забезпечення. Крім того, під час роботи над «Скан-В» «НТЦ Вулкан» отримував значне фінансування на суми до кількох мільйонів євро від інститутів, тісно пов'язаних із російськими спецслужбами. У призначеннях платежу безпосередньо фігурують назви розроблюваного програмного забезпечення «Скан-В», «Амезит» і «Кристал-2В». На титульному аркуші технічної документації міститься позначка «Затверджую» від імені керівника військової частини № 74455 [6; 7].

Зазначена військова частина № 74455 є структурою ГУ ГШ ВС рф і одним із ключових російських підрозділів кібервійни, який відомий за назвою хакерської групи, що сформована і діє на базі цього підрозділу – «Sandworm». Широкого публічного розголосу інформація про її діяльність отримала після оприлюднення розслідування спецпрокурора США Роберта Мюллера про вплив рф на американські президентські вибори у 2016 році, в якому було оприлюднено інформацію про розміщену у м. Хімки у сучасному офісному центрі названому «Вежа» в/ч № 74455, яка здійснювала деструктивну активність у кіберпросторі щодо передвиборчого штабу Гілларі Клінтон та вплив з метою перемоги у виборах Дональда Трампа. В подальшому саме «Sandworm» звинувачувався керівництвом СБ України, ДССЗЗІ України, а так само низкою авторитетних міжнародних кібербезпекових організацій у здійсненні найбільш резонансних кібератак на Україну, серед яких однією з нещодавніх є кібератака на мережу мобільного оператора «Київстар» наприкінці 2023 року. Окрім офіційних заяв і аналітичних матеріалів кібербезпекових організацій діяльність «Sandworm» була визнана злочинною і судовою системою США, де у 2020 році було висунуто публічне обвинувачення шістьом громадянам росії, яких було ідентифіковано військовослужбовцями ГУ ГШ ВС рф та учасниками відповідної хакерської організації та оголошено у розшук Федеральним Бюро Розслідувань США. Американська судова система звинувачує їх у кібератаках як на конкретні об'єкти в США, такі і у Франції, Республіці Корея, Великобританії, Грузії та Україні (а саме атаки 2015-2016 років на «Прикарпаттяобленерго» підстанцію «Північна» «Укренерго», Міністерство фінансів, Державне казначейство) [9].

Таким чином інтегрована робота розроблених формально недержавною кампанією «НТЦ Вулкан» програмних компонентів «Скан-В» забезпечує для її реального замовника, військової частини № 74455 ГУ ГШ ВС рф, яка є організаційно-штатною структурою хакерського угрупування «Sandworm», процес автоматизованої розвідки цілей по всьому світу шляхом ідентифікації потенційно вразливих серверів і мережевих пристроїв, фіксації та систематизації розвідувальних даних для подальшого здійснення кібератак у потрібний момент, а програмний засіб «Кристал-2Б» є засобом підготовки операторів таких кібератак. На думку Габбі Ронкоун, експерта кібербезпекового підрозділу Google кампанії Mandiant функція «Скан-В» може бути порівняна із «націлюванням артилерії у традиційних війнах, тобто програмний засіб дозволяє зрозуміти, де стоять танки противника і навести засоби ураження щоб у необхідний момент одразу прорвати лінію оборони» [7; 8].

Аналіз формалізованих у технічній документації «НТЦ Вулкан» функціональних спроможностей вищезазначених програмних продуктів дозволяє їх розглянути як зброю, що використовується для нападу у збройному конфлікті крізь призму jus ad bellum в контексті положень щодо підстав самооборони згідно Статуту ООН та крізь призму jus in bello в контексті норм міжнародного гуманітарного та міжнародного кримінального права щодо заборони нападів на цивільне населення та цивільні об'єкт.

Римський статут Міжнародного Кримінального Суду для позначення кримінально-караних діянь стосовно цивільних об'єктів та цивільного населення в період збройного конфлікту натомість використовує термін «навмисна атака» (частини 2 статті 8) [10], натомість у статуті ООН використано термін «збройний напад». Такий напад є умовою реалізації права на індивідуальну або колективну самооборону (стаття 51) та є підставою визначення Радою Безпеки ООН на підставі Резолюції Генеральної Асамблеї ООН від 14 грудня 1974 року № 3314 (XXIX) факту наявності «акту агресії». Слід зазначити, що у відповідній резолюції є уточнення, що суб'єктами нападу можуть бути не тільки «збройні сили держави» (пункти «a», «d» статті 3), але і «озброєні банди, групи, іррегулярні сили чи найманці», за умови, якщо вони «направлені державою» і «здійснюють акти застосування збройної сили проти іншої держави, які мають настільки серйозний характер, що це рівносильно переліченим вище актам, або його значну участь у них». Зазначена конкретизація є вкрай корисною в контексті тлумачення кібератак хакерських угрупувань, наприклад «Sandworm», які повністю управляються російськими спецслужбами.

За відсутності чіткої деталізації на міжнародно-правовому рівні змісту поняття «напад» широко відомим є підхід, сформований у так-званому «Другому талліннському посібнику» («Tallinn Manual 2.0»), підготовленому у 2017 році групою експертів Центру передового досвіду з кібербезпеки НАТО (NATO Cooperative Cyber Defence Centre of Excellence, CCDCOE), згідно якого кібероперація підпадає під вищезазначене поняття, якщо вона призводить (або має призвести) до смерті, поранень або фізичних руйнувань (правило 92) [11; 12].

Натомість інший підхід, який, зокрема, закріплений у французькому законодавстві, передбачає ототожнення міжнародно-правового поняття «напад» не лише із руйнуванням або знищенням певної цілі, але і з блокуванням її діяльності в результаті кібератаки, коли об'єкт фізично не ушкоджений, але уражене його програмне забезпечення і функція об'єкта, наприклад, виробництво і постачання електроенергії, не виконується. Саме цей підхід, який також відомий як «концепція втрати функціональності», був використаний для аргументації у запитах групи юристів Центру прав людини Каліфорнійського університету в Берклі (Berkeley Human Rights Center) до Прокурора МКС [13] щодо розширення ним розслідування ситуації в Україні на кібердомен в контексті визнання низки кібератак рф воєнним злочином.

Висновки. Спираючись на «концепцію втрати функціональності», яка отримала активний розвиток як реакція на зухвалу деструктивну діяльність росії у кіберпросторі, необхідно визнати спеціальне програмне забезпечення засобом нападу, тобто зброєю (кіберзброєю), у тому випадку, якщо воно надає можливість здійснювати такий вплив на програмну та/або апаратну складову об'єкта атаки, завдяки якому цей об'єкт перестає виконувати свою основну функцію. Розроблений кампанією «НТЦ Вулкан» програмний засіб «Скан-Б» за умови його комплексного використання російським спецслужбами та підконтрольними них хакерськими угрупуваннями для припинення функціонування іноземних об'єктів-цілей кібератак, має розглядатися як засіб нападу аналогічно до кінетичної зброї, що спричиняє припинення функціонування об'єкта завдяки його фізичному пошкодженню. Відповідне застосування кіберзброї незалежно від факту оголошення війни має вважатися збройним нападом та актом агресії згідно Статуту ООН. У випадку застосування кіберзборої як засобу нападу на цивільні об'єкти і цивільне населення під час міжнародного збройного конфлікту такі діяння мають вважатися злочином згідно Римського статуту Міжнародного кримінального суду.

ЛІТЕРАТУРА

1. Федієнко О. П. Сучасні тенденції нормативного забезпечення інституційного формування кібервійськ (кіберсил): досвід деяких країн НАТО. *Інформація і право.* 2024. № 1 (48). С. 150–161.

2. 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.

3. Ткачук Н. А. Досвід США зі створення та розбудови Кіберкомандування: уроки для України. *Інформація і право.* 2024. № 1 (48). С. 139–149.

4. The Gravity of Russia's Cyberwar against Ukraine. OpinioJuris : веб-сайт. URL: https://opiniojuris.org/2023/04/19/the-gravity-of-russiascyberwar-against-ukraine/ (дата звернення: 28.04.2024).

5. The Prosecutor's New Policy on 'Cyber Operations' before the International Criminal Court (and its Implications for Ukraine). Blog of the European Journal of International Law : веб-сайт. URL: https://www.ejiltalk.org/the-prosecutors-new-policy-on-cyber-operations-before-theinternational-criminal-court-and-its-implications-for-ukraine-some-preliminaryreflections/ дата звернення: 28.04.2024).

6. The «Vulkan Files». A Look Inside Putin's Secret Plans for Cyber-Warfare. *Spiegel International* : веб-сайт. URL: https://www.spiegel.de/international/world/the-vulkan-files-a-look-inside-putin -s-secret-plans-for-cyber-warfare-a-4324e76f-cb20-4312-96c8-1101c5655236 (дата звернення: 28.04.2024).

7. Analyzing the NTC Vulkan Leak: What it Says About Russia's Cyber Capabilities. *Trustwave* : веб-сайт. URL: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/analyzing-the-ntc-vulkan-leak-what-it-says-about-russias-cyber-capabilities/ (дата звернення: 28.04.2024).

8. Contracts Identify Cyber Operations Projects from Russian Company NTC Vulkan. *Mandiant on Google Cloud* : веб-сайт. URL: https://cloud.google.com/blog/topics/threat-intelligence/cyber-operations-russian-vulkan/ (дата звернення: 28.04.2024).

9. US Indicts Sandworm, Russia's Most Destructive Cyberwar Unit. Wired : веб-сайт. URL: https://www.wired.com/story/us-indictssandworm-hackers-russia-cyberwar-unit/ (дата звернення: 28.04.2024).

10. Римський статут Міжнародного кримінального суду. Міністерство юстиції України : веб-сайт. URL: https://minjust.gov.ua/m/mijnarodniy-kriminalniy-sud (дата звернення: 28.04.2024).

11. Tallinn Manual on the International Law Applicable to Cyber Warfare. Nowandfutures : веб-сайт. URL: https://www.nowandfutures.com/large/Tallinn-Manual-on-the-International-Law-Applicable-to-Cyber-Warfare-Draft-.pdf (дата звернення: 28.04.2024).

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: 28.04.2024)

13. The Prosecutor's New Policy on 'Cyber Operations' before the International Criminal Court (and its Implications for Ukraine). Blog of the European Journal of International Law : веб-сайт. URL: https://www.ejiltalk.org/the-prosecutors-new-policy-on-cyber-operations-before-theinternational-criminal-court-and-its-implications-for-ukraine-some-preliminaryreflections/ (дата звернення: 28.04.2024).