УДК 342.951

КРАСНІКОВ С.А., провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України
ORCID: https://orcid.org/0000-0001-6548-5457

ГЕОПОЛІТИКА КІБЕРКОНФЛІКТІВ І КІБЕРВІЙН: МІЖНАРОДНО-ПРАВОВІ ВИКЛИКИ

DOI: https://doi.org/10.37750/2616-6798.2025.3(54).340522

Анотація. *У статті розглядається феномен геополітики кіберконфліктів і кібервійн у сучасному міжнародному праві. Аналізується еволюція кіберзагроз як інструменту стратегічного впливу в умовах гібридних війн. Визначається правова природа кібератак, що набувають ознак збройного нападу. Оцінюється можливість застосування основоположних принципів міжнародного гуманітарного права до дій у кіберпросторі. Особлива увага приділяється доцільності втілення ідей кримінальної відповідальності держави у сучасному міжнародному праві. На основі аналізу практики ООН, Європейського Союзу та ОБСЄ виявлено тенденції до консолідації підходів щодо врегулювання кіберконфліктів за допомогою норм міжнародного права. Висловлено пропозицію розроблення міжнародного договору, який би регламентував застосування принципів і норм міжнародного гуманітарного права у сфері використання кіберзброї.*

Ключові слова: *кібервійна, кіберконфлікт, кіберзброя, геополітика, міжнародне гуманітарне право, відповідальність держав.*

Summary. *The article examines the phenomenon of geopolitics of cyber conflicts and cyber wars in contemporary international law. It analyzes the evolution of cyber threats as a tool of strategic influence in hybrid wars. It defines the legal nature of cyberattacks that are becoming akin to armed attacks. It assesses the possibility of applying the fundamental principles of international humanitarian law to actions in cyberspace. Particular attention is paid to the feasibility of implementing the ideas of criminal responsibility of the state in contemporary international law. Based on an analysis of the practices of the UN, the European Union, and the OSCE, trends toward the consolidation of approaches to the settlement of cyber conflicts through international law are identified. A proposal has been made to develop an international treaty that would regulate the application of the principles and norms of international humanitarian law in the use of cyber weapons.*

Keywords*: cyberwarfare, cyber conflict, cyber weapons, geopolitics, international humanitarian law, state responsibility.*

Постановка проблеми. У сучасних геополітичних умовах кіберпростір став повноцінним театром воєнних дій та новою сферою геополітичної конкуренції, де традиційні засоби і методи війни трансформуються у цифрові форми впливу. Кіберконфлікти низької інтенсивності, які розпочалися як кіберінциденти, нині набувають ознак стратегічних кібероперацій, спрямованих на дестабілізацію критичної інфраструктури, втручання у виборчі процеси, масове поширення дезінформації та здійснення економічного тиску на конкурентів. У цьому контексті сучасна кібервійна є складовою гібридної війни, яка поєднує різноманітні елементи військової, інформаційної та економічної агресії.

Сучасний розвиток міжнародних процесів, на жаль, не зменшує, а, навпаки, продукує конфліктність, у т.ч. в кіберпросторі. Якщо у XXI ст. не прислухатися до набату конфлікту в міжнародних відносинах, то можна перейти ту межу конструктивної функціональності, за якою він перетворюється із суспільно корисного чинника у молох, який загрожує існуванню людства [1, с.19]. Саме тому розуміння природи кіберконфліктів та вироблення способів правового захисту від них є надзвичайно важливим завданням. Нова геополітична ситуація в світі потребує також і внесення змін до стратегії інформаційних війн у кібернетичному просторі. Прогнозується зростання інтенсивності міждержавного протиборства у кіберпросторі [2].

Результати аналізу наукових публікацій. Проблемні аспекти застосування інформаційної зброї в інформаційних війнах висвітлені у працях В. Брижка [3], О. Данильяна, О. Дзьобаня, В. Пилипчука, Г. Почепцова [4], М. Швеця, В. Цимбалюка[3].

Аналіз сучасних наукових публікацій свідчить про стійкий інтерес до кібервійни як різновиду кіберконфлікту. Цим питанням присвятили свої роботи І. Воєводин [5], Ю. Калайда [6], М. Камчатний [7], С. Руцький[8] та ін. Водночас, кіберконфлікти та кібервійни залишаються недостатньо дослідженими в сучасних геополітичних умовах, що зумовлює актуальність цієї статті. Про гостроту цієї проблеми свідчить і сучасна російсько-українська кібервійна.

Метою статті є дослідження геополітичних аспектів кібервійни з позиції конфліктологічного підходу та норм міжнародного гуманітарного права для удосконалення шляхів нормативного врегулювання цієї сфери.

Виклад основного матеріалу. Звернення до конфліктології в контексті кібервійни є цілком закономірним. Воно базується на сприйнятті кібервійни як різновиду кіберконфлікту, який логічно виникає у сучасних геополітичних умовах, а його суспільна небезпечність становить серйозну загрозу міжнародному правопорядку.

Не випадково конфлікт і конфліктність стають предметом уваги самих різних галузей знань. Поняттям “конфлікт” користуються різні наукові дисципліни, ототожнюючи його з різними соціальними явищами. Не є виключенням в цьому плані і дисципліни, які вивчають кібербезпеку.

Поняття “конфлікт” має латинське походження (conflict), яке означає зіткнення. Він може виникати між окремими особами, групами, або навіть між державами.

Існує кілька десятків визначень соціального конфлікту, на основі узагальнення яких пропонується вважати таким зіткнення суспільних сил, груп, окремих осіб в процесі вирішення усвідомленої ними суперечності [9, с.13].

Один із теоретиків конфлікту Р.Дарендорф вважає, що будь-який конфлікт зводиться до “відносин двох елементів”. Навіть якщо у конфлікті беруть участь декілька груп, між ними утворюються коаліції, а конфлікт знову отримує біполярну природу [10, с.142].

Під соціальним конфліктом зазвичай розуміється такий вид протистояння, в якому обидві сторони намагаються захопити територію або ресурси, загрожувати опозиційним індивідам чи групам, їх власності, культурі, забезпечити тим самим реалізацію питань, які є життєво важливими для кожної із сторін. Тим самим соціальний конфлікт обов’язково припускає “свідоме” зіткнення двох протиборчих соціальних сторін на основі суперечностей, які виникають з взаємовиключних інтересів або методів їх досягнення [11, с.86].

З нашої точки зору, застосування конфліктологічного підходу при дослідженні кібервійн є досить перспективним. Такий підхід до дослідження кібервійн та

кіберконфліктів фокусує увагу на соціальних, інформаційних і політичних процесах в термінах протиборства між людьми, соціальними групами за цінності, які мають соціальну значимість.

Під кіберконфліктом (cyberconflict) як різновидом соціального конфлікту розуміють протистояння між двома або більше сторонами в кіберпросторі, що включає в себе дії, спрямовані на порушення роботи комп'ютерних систем, мереж або даних з метою отримання переваги, контролю або завдання шкоди [12]. Це поняття охоплює широкий спектр дій – від незначних кібератак до масштабних кібервоєнних операцій. Кіберконфлікти можуть мати різні цілі, включаючи крадіжку конфіденційної інформації, порушення роботи критично важливої інфраструктури, втручання у вибори, шпіонаж, пропаганду та іншу злочинну мету [12].

Загострення суперечностей залежить від сторін конфлікту та об'єкту протиборства у кіберпросторі. Кіберконфлікт може бути продовженням політичного конфлікту або навпаки політичний конфлікт може розвиватись, як наслідок кіберпротидії суб'єктів політики (наслідок онлайн оголошення про збори на мітинги).

Сучасні кіберконфлікти є відображенням сучасної геополітичної боротьби за домінування в кіберпросторі. Зокрема, конфліктологічний підхід міститься у стратегіях забезпечення кібербезпеки провідних держав світу, зокрема США і Китаю, які активно використовують свій кіберпотенціал для досягнення конкретних політичних, економічних та військових цілей. Так, на початку травня 2024 року Державний департамент США оприлюднив Стратегію міжнародного кіберпростору та цифрової політики, для того щоб стримати цифровий вплив росії та Китаю в країнах, що розвиваються, і зробити ймовірні спроби цих країн втручатися у вибори менш ефективними[14]. Цю Стратегію можна схарактеризувати як намагання США створити коаліцію проти Китаю.

Крім того, існує також і широкий спектр інших ліній протиборства у кібернетичному просторі ситуативного, регіонального, локального та іншого характеру. Зокрема, прикладами цього є протистояння НАТО і ЄС з Росією, в т. ч. у кібернетичному просторі[15]. Як показує практика європейських країн, переважно реакція на кібератаки відбувається в момент виникнення проблеми, або при аналізі наслідків, які заподіяли шкоду суспільству чи органам управління[8, с. 61].

Виходячи з базових принципів стратегії кібернетичних війн у новій геополітичній ситуації, стратегія кібернетичних війн має базуватись на таких основних принципах: організація протиборства у кібернетичному просторі в рамках загальних планів ведення війни, а також налагодження тісної координації з бойовими діями військ в інших середовищах; застосування адаптивного підходу у веденні кібернетичних війн проти широкого спектру противників, який передбачає адекватне реагування на різного роду загрози і ситуації; забезпечення можливості маневру силами та засобами в цілях: зосередження зусиль на найбільш важливих напрямах; оптимального використання різних компонентів кіберпростору в залежності від ситуації; безперервність ведення кібернетичних війн, в т. ч. і в мирний час[15]. На відміну від класичних війн, протистояння у кібернетичному просторі не припиняється ні за яких обставин, за виключенням повної руйнації світових комп'ютерних мереж; досягнення рішучої переваги над противником у технічному та інтелектуальному потенціалах, які можуть бути залучені до проведення війн у кібернетичному просторі; перехід до мережецентричних принципів, а саме — налагодження тісної взаємодії між різними підрозділами кібернетичних війн як всередині однієї країни та союзу країн, так і з їх партнерами на основі спільних планів дій та оперативного обміну інформацією;

здійснення комплексної і регулярної підготовки сил та засобів кібернетичних війн до ведення бойових дій в цій сфері, в т. ч. активних оборонних, розвідувальних та превентивних наступальних операцій; всебічна підтримка дій у кібернетичному просторі, в т. ч. розвідувальна, науково-технологічна, матеріально-технічна, кадрова та ін. [15].

В цьому контексті кіберпростір стає полем геополітичного протистояння, де держави використовують кіберінструменти для: дестабілізації внутрішньої політики суперника; втручання у демократичні процеси (наприклад, вибори в США у 2016 році); шпигунства та збору розвідувальної інформації; підготовки масштабних кібератак на об'єкти критичної інфраструктури супротивника. Така поведінка відображає логіку гібридної війни, де кібероперації плануються та здійснюються для стратегічного впливу на супротивника.

Україна також тривалий час була об'єктом кібератак. Найбільш відомою є масштабна хакерська атака 27 червня 2017 року на об'єкти критичної інфраструктури із використанням комп'ютерного хробака сімейства Petya [16].

Атрибутовані рф кібератаки на енергетичну систему України у 2015 – 2016 рр. стали першими в історії випадками масштабного відключення електропостачання внаслідок кібероперації [17].

З цього приводу у Стратегії кібербезпеки України зазначається: "Російська Федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України… Держава-агресор невпинно нарощує арсенал кіберзброї наступального призначення, застосування якої може викликати невиправні, незворотні руйнівні наслідки. Кібератаки російської федерації спрямовані, насамперед, на інформаційно-комунікаційні системи державних органів України та об'єкти критичної інформаційної інфраструктури з метою виведення їх з ладу (кібердиверсія), отримання прихованого доступу і контролю, здійснення розвідувальної та розвідувально-підривної діяльності. Кібератаки також активно використовуються державою-агресором як елемент спеціальних інформаційних операцій з метою маніпулятивного впливу на населення, втручання у виборчі процеси та дискредитації української державності" [1].

На думку Ю.Калайди, можна виділити такі етапи кібервійни рф проти України: перший етап – з початку анексії Криму в 2014 році, під час якої інформаційно-обчислювальні системи України стали об'єктами атак з боку Росії; другий етап – 23.12.2015 – 23.02.2022 – період хакерських атак, інтенсивність і масштаб яких лише збільшувався з часом; третій етап – 24.02.2022 – по теперішній час – триваючий період неприкритої агресії рф, важливим елементом якої стала повномасштабна кібервійна [6, с.193-194].

Етапи кібервійни в Україні підтверджують тезу про те, що кіберзброя може мати реальні фізичні наслідки, які є не менш небезпечними, ніж наслідки застосування традиційної збройної агресії.

Наслідки таких конфліктів вимагають адекватного правового реагування на підставі міжнародного гуманітарного права, норми якого сьогодні стикаються з викликами, пов'язаними з визначенням правової природи кібероперацій, кваліфікацією кібератак як проявів збройного нападу та встановленням відповідальності держави за такі дії.

Стосовно питань застосування норм міжнародного гуманітарного права в кіберпросторі, слід зазначити, що переважна більшість його норм формувалася досить давно, коли людство навіть не уявляло можливість проведення війну нову "кіберплощину" і автори текстів міжнародних актів не могли описати правила поведінки, які б поширювали свою дію на ще не існуючий простір, новітній театр ведення війни [5, с.46].

Однією з найбільших дискусійних правових проблем є визначення моменту, коли кібератака набуває ознак злочинного діяння, яке у міжнародному гуманітарному праві трактується як збройний напад.

Відповідно до ч. 4 ст. 2 Статуту ООН усі члени Організації Об'єднаних Націй повинні утримуватися в своїх міжнародних відносинах від погрози силою або її застосування як проти територіальної недоторканності або політичної незалежності будь-якої держави, так і якимось іншим чином, несумісним із цілями Об'єднаних Націй[18].

Викладене дає змогу зробити проміжний висновок, що підтримана державою кібератака є своєрідною формою нападу на іншу державу, що, безумовно, суперечить нормам Статуту ООН. Між тим норми міжнародного гуманітарного права безпосередньо застосовуються лише під час збройних конфліктів міжнародного та неміжнародного характеру. Йдеться про Додатковий протокол до Женевських конвенцій 1949 року, що стосується захисту жертв міжнародних збройних конфліктів 1977 року (Протокол №1) та Додатковий протокол до Женевських конвенцій 1949 року, що стосується захисту жертв збройних конфліктів неміжнародного характеру 1977 року (Протокол №2).

В 2013 р. Об'єднаним центром передового досвіду з кібероборони НАТО було прийнято акт, відомий як "Таллінське керівництво щодо застосування юридичних норм міжнародного гуманітарного права до військових дій у кіберпросторі." За таллінською доктриною основоположні принципи міжнародного гуманітарного права визнані такими, що застосовуються до дій у кіберпросторі. Той факт, що комп'ютерні атаки в ході збройного конфлікту не мають безпосередньої динамічної, фізичної чи насильницької форми, не виходить за межі дії міжнародного гуманітарного права[19, с.18]. За такого підходу кібероперація може вважатися збройним нападом. Наприклад, під цю кваліфікацію підпадає кібератака на ядерний об'єкт, що спричинила вибух чи виток чи розсіювання радіактивного матеріалу.

У 2013 р. Група урядових експертів ООН (Group of Governmental Experts (UN GGE) прийняла консенсусну доповідь, в якій зауважено, що "міжнародне право і, зокрема, Статут Організації Об'єднаних Націй, є застосовним і необхідним для підтримки миру, стабільності та сприяння відкритому, безпечному, середовищу інформаційно-комп'ютерних технологій" [20]. Цю позицію підтвердила інша GGE UN у 2015 р., яка також схвалила низку юридично необов'язкових норм відповідальної поведінки держави[21].

Слід зазначити, що право держави на самооборону передбачено ст. 51 Статуту ООН, яка проголошує, що: "Цей Статут жодним чином не зачіпає невід'ємного права на індивідуальну або колективну самооборону, якщо відбудеться збройний напад на члена Організації, доти, поки Рада Безпеки не вдасться до заходів, необхідних для підтримки міжнародного миру й безпеки" [18].

Однак більшість кіберінцидентів (DDoS-атаки, крадіжка даних, втручання у політичні вибори) важко оцінити у термінах збройного нападу особливо з позиції їх суспільно небезпечних наслідків, що ускладнює застосування права на самооборону у

порядку, передбаченому статтею 51 Статуту ООН. Складно також визначити склад учасників кіберконфлікту, адже від цього залежить не тільки кваліфікація конфлікту, але й обсяг захисту, що надається кожній стороні, визначення законних цілей для нападу і можливості притягнення до відповідальності [22; 8, с. 61].

Якщо кібероперація визнається складовою збройного конфлікту, до неї мають застосовуватися основоположні принципи міжнародного гуманітарного права: пропорційності; незастосування невибіркової зброї; розмежування між військовими цілями та цивільними особами і недопущення віроломства.

Проте практичне застосування цих принципів у кіберпросторі на підставі норм міжнародного гуманітарного права ускладнюється через анонімність, посередництво та можливість вторинних наслідків (наприклад, кібератака на військовий сервер може вплинути на цивільну медичну мережу).

Відсутність чітко визначених норм міжнародного гуманітарного права щодо визначення кіберзброї та порядку її застосування призводить до правової невизначеності, якою, на жаль, користуються держави-агресори для здійснення кібероперацій за відсутності правового реагування на такі злочинні дії.

На думку Метью С. Ваксмана (Matthew C. Waxman), кібератаки – це національний потенціал, для якого міжнародне право та норми є невизначеними [23, с. 1–6].

Саме тому вельми важливим питанням порядку денного ООН має стати відповідальність держави за кібероперації у кібепросторі.

Концепція кримінальної відповідальності держави розроблялася і підтримується видатними фахівцями міжнародного права різних націй. Серед розробників цієї концепції слід назвати праці Р. Аго, А. Бустаманте, Г. Доннедьє де Вабра, Ф. Малекяна, П. Каржо, Г. Кельзена, В. Пелла, Е. Сендстрема та ін. Серед вітчизняних дослідників проблеми кримінальної відповідальності держави слід виділити праці В. Антипенка, С. Андрейченко, Н. Зелінської, К. Важної та ін.

На думку В. Ф. Антипенка, квінтесенція ідеї кримінальної відповідальності держави, її міжнародно-правова кваліфікація зводиться до міжнародного-кримінологічного препарування феноменального симбіозу, а якому людська кримінальна поведінка зливається з прилаштованою під цю кримінальність порочністю державних механізмів, втілених у відповідному державному апараті [24, с. 31].

До основоположних ідей концепції кримінальної відповідальності держави належать: 1) визнання того, що держава може вчиняти міжнародні злочини, а тому повинна нести за них відповідальність; 2) необхідність встановлення різних режимів відповідальності держави за міжнародні правопорушення (делікти) і за міжнародні злочини (серозні порушення міжнародних норм загального міжнародного права); 3) необхідність створення спеціального міжнародного судового органу для держав із юрисдикцією розглядати справи і виносити рішення щодо відповідальності держав за міжнародні злочини; 4) необхідність прийняття міжнародного кримінального кодексу, який би містив перелік міжнародних злочинів та перелік форм відповідальності держави; 5) форми і міри відповідальності держави за міжнародні злочини можуть передбачати тимчасове правомірне обмеження суверенітету злочинної держави [24, с. 235-236].

Проекти міжнародного кримінального кодексу та статуту міжнародного кримінального суду, в яких містилася цілісна концепція кримінальної відповідальності держави, були предметом розгляду органів Ліги Націй та ООН (зокрема, Комісії з міжнародного права ООН).

Проект статей про відповідальність держав розроблено Комісією міжнародного права ООН ще у 1976 році.

У резолюції 56/83 від 12 грудня 2001 року Генеральна Асамблея взяла до відома статті про відповідальність держав за міжнародно-протиправні діяння, текст яких міститься в додатку до вищезазначеної резолюції.

6 грудня 2010 року Генеральна Асамблея ухвалила резолюцію 65/19, в якій запропонувала включити до попереднього порядку денного своєї шістдесят восьмої сесії у 2013 ро. пункт, який має назву "Відповідальність держав за міжнародно-протиправні діяння" (A/65/96 і Add.1), а також продовжити в рамках робочої групи Шостого комітету з метою ухвалення рішення розгляд питання про конвенцію про відповідальність держав за міжнародно-протиправні діяння.

Текст ст. 19 Проекту статей про відповідальність держав Комісії міжнародного права ООН 1976 року передбачає, що діяння держави, що порушує міжнародні зобов'язання, є міжнародно-правовим діянням, незалежно від об'єкта порушеного зобов'язання. Міжнародно-правове діяння, яке виникає внаслідок порушення міжнародного зобов'язання, настільки важливого для забезпечення життєво важливих інтересів міжнародного співтовариства, що його порушення розглядається як міжнародний злочин у цілому, становить міжнародний злочин [26].

Стаття 8 Розділу II Проекту статей про відповідальність держав встановлює, що держава несе відповідальність за будь-яку дію, яка порушує міжнародне зобов'язання, якщо ця дія може бути атрибутована цій державі.

В даному контексті проблема полягає в атрибуції, зміст якої полягає у встановленні зв'язку між кібератакою та конкретною державою. Через використання проксі-серверів, ботнетів та недержавних груп (наприклад, "хактивістів") держави часто ухиляються від відповідальності, посилаючись на "приватні дії".

З цього приводу заслуговує на увагу звіт Генерального секретаря ООН від 2021 року, у якому зазначається, що "держави мають обов'язок утримуватися від шкідливих дій у кіберпросторі та не допускати використання своєї території для агресивних кібероперацій" [27].

На жаль, сьогодні відсутній універсальний міжнародний договір, який би регулював застосування кіберзброї.

З цього приводу Б. Данкан Холліс (Duncan B. Hollis) зазначає, що глобальні зусилля держав співпрацювати за допомогою міжнародних правил у боротьбі з кіберзагрозами дали, у кращому випадку, неоднозначні результати [23].

Водночас, заслуговують на увагу важливі ініціативи у цьому напрямку.

Так, група урядових експертів ООН з міжнародної безпеки в цифровому просторі затвердила ряд принципів, серед яких передбачено заборону кібератак на критичну інфраструктуру з урахуванням дотримання Статуту ООН. Також встановлюється зобов'язання держав щодо проведення консультацій з усіма компетентними представниками влади, взяття до уваги всіх деталей, пов'язаних зі зловмисним використанням інформаційно-комунікаційних технологій, а також створення чи посилення національних структур та підходу до розслідування таких кіберінцидентів [28].

У свою чергу, ОБСЄ розробила Віденські директиви щодо добросусідства в кіберпросторі[29].

Резолюцією A/RES/74/247 Генеральної Асамблеї ООН (27 грудня 2019 р.) створено спеціальний міжурядовий комітет відкритого складу експертів і представників усіх регіонів для розроблення всеосяжної міжнародної конвенції про протидії використанню

інформаційних і комунікаційних технологій зі злочинною метою[30]. А в Резолюції ГА ООН A/RES/75/282 (26 травня 2021 р.) було вирішено, що спеціальний комітет скличе принаймні шість сесій для завершення роботи над документом, щоб представити проєкт Конвенції на 78-й сесії Генеральної Асамблеї ООН (12–30 вересня 2023 р.) [31]. Це сприятиме зменшенню ризику виникнення конфліктів, що є суттєво важливою для забезпечення міжнародної безпеки[21].

Варто також згадати укладену ще у 2001 році Конвенцію ООН про кіберзлочинність, яка стала першим багатостороннім договором у сфері протидії кіберзлочинності, приписи якої, на жаль, також не регулюють питання застосування кіберзброї.

Все це свідчить про численні спроби врегулювання кіберконфліктів за допомогою норм міжнародного права, яке, як ми переконалися, потребує вдосконалення в цій частині. Сьогоднішні реалії формують усе нові вимоги щодо розвитку кіберконфліктів, а відповідно вимагають і нові уніфіковані нормативно-правові механізми й підходи з питань забезпечення безпеки кіберпростору. Насамперед, це стосується розробки міжнародних принципів правового регулювання застосування кіберзброї.

Висновки. Кібервійна як форма кіберконфлікту відтворює глибину існуючих соціальних суперечностей, що свідчить про кризу світоустрою. Кіберконфлікти є невід'ємною складовою сучасної геополітики, в умовах якої кіберзброя використовуються як один із інструментів стратегічного впливу на супротивника. Кібероперації в сучасних геполітичних умовах потребують правового регулювання на підставі норм міжнародного гуманітарного права, зміст якого має бути адаптований до цифрової реальності. Явно недостатніми в цьому плані є приписи Статуту ООН щодо права держави на самооборону. Діяння, які складають кіберагресією, як правило, визначаються і підтримуються державною політикою, яка відповідає стратегічним цілям геополітики цієї держави. Кіберагресія не може бути реалізованою без підтримки та участі держави. Саме тому ефективність міжнародно-правового впливу на державу значно підвищиться за умови реалізації концепції кримінальної відповідальності держави. Це дозволить покращити систему міжнародної кібербезпеки, підвищити ефективність міжнародного гуманітарного права у боротьбі з кіберзлочинами.

Для підвищення ефективності правового регулювання кіберпростору необхідно розробити та ухвалити міжнародний договір, який би регламентував застосування принципів і норм міжнародного гуманітарного права у сфері використання кіберзброї (аналогічні договорам про хімічну, біологічну чи ядерну зброю). Позиція України, яка постійно стикається з кіберагресією, повинна бути більш активною у частині розробки міжнародних норм з питань кібербезпеки та удосконалення національного законодавства у цій частині. Для формування потенціалу кіберстримування стратегічною метою для нашої держави залишається створення підрозділів з повноваженнями ведення збройного протиборства в кіберпросторі[2].

Використана література

1. Антипенко В.Ф. Конфликтология в антитеррористическом правотворчестве. О.: Фенікс, 2014. 404 с.

2. Стратегія кібербезпеки України: затвердж. Указом Президента України від 26 серпня 2021 року № 447. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

3. Брижко В., Швець М., Цимбалюк В. Е-боротьба в інформаційних війнах та інформаційне право. за ред. М. Швеця. К.: ТОВ "ПанТот", 2007. 218 с.

4. Почепцов Г.Г. Информационные войны. (Серия: Образовательная библиотека). М.: Рефл-бук, 2001. 576 с.

5. Воєводін С. Кібервійна як сучасний метод ведення збройних конфліктів. Протидія кіберзагрозам та торгівлі людьми (м. Харків, 2019 р.). С.45-47. URL: https://univd.edu.ua/general/publishing/konf/26_11_2019/pdf/11.pdf

6. Калайда Ю.П. Агресія рф у кіберпросторі як загроза національній безпеці України. Інформація і право. 2024. № 1(48). С. 188-194. DOI:https://doi.org/10.37750/2616-6798.2024.1(48).300810.

7. Камчатний М.В. Основні ознаки поняття «кібервійна» у сучасному міжнародному праві.URL: http://inlawalmanac.mgu.od.ua/v15/4.pdf.

8. Руцький С.В. Кіберконфлікти у протиборстві суб'єктів політики на території європейських країн. *Сучасні виклики соціально - політичного розвитку: політико-правові та соціально-економічні виміри*: матеріали всеукраїнської студентської науково-практичної конференції (м. Одеса, 24 травня 2024 року). Одеса : ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського», Центр соціально-політичних досліджень «Politicus», 2024. С. 60-63. URL: http://dspace.pdpu.edu.ua/bitstream/123456789/19629/1/60-62.pdf.

9. Коваленко Б.В., Пирогов А.И., Рыжов О.А. Политическая конфликтология. М.,: Ижица, 2000. 400 с.

10. Дарендорф Р. Современный социальный конфликт. Очерк политики свободы. М., 2002. 228 с.

11. Антипенко В.Ф. Теории мирового развития и антитеррористическое право. К. 2007. 440 с.

12. Shevchenko S , Zhdanova Y., Astapenya V., Nehodenko O., Spasiteleva S. Conflicting Subsystems in the Information Space: A Study at the Software and Hardware Levels. URL: https://elibrary.kubg.edu.ua/id/eprint/48768/1/S_Shevchenko_Y_Zhdanova_V_Astapenya_t%D0%B0__in_CEUR_3654_2024_FITM.pdf

13. Завгородня Ю.В. «Кіберконфлікти» та «політичні конфлікти»: співвідношення понять. URL: http://app.nuoua.od.ua/archive/70_2022/15.pdf.

14. Огляд подій в сфері кібербезпеки. травень 2024. URL:https://ufss.com.ua/news/ohliad-podiy-v-sferi-kiberbezpeky-traven-2024.html.

15. Гвоздь В. Кіберконфлікт і геополітика — новий фронт «холодної війни». URL: https://bintel.org.ua/nash_archiv/arxiv-voyenni-pitannya/arxiv-gibridnia-vijna/09_05_krynica/.

16. Російсько-українська кібервійна. URL:https://uk.wikipedia.org/wiki.

17. Zetter K. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. New York : Crown Publishing, 2016. 400 p.

18. Статут Організації Об'єднаних Націй. URL:https://unic.un.org/aroundworld/unics/common/documents/publications/uncharter/UN%20Charter_Ukrainian.pdf.

19. Гриняев С. Таллинское руководство по применению юридических норм к военным действиям в киберпространстве в оценках западных экспертов. Обзор НЦТПИ. 2015. №3. С.18-22.

20. Duncan B. Hollis, Matthew C. Waxman Promoting International Cybersecurity Cooperation: Lessons from the Proliferation Security Initiative (PSI) Temple University Beasley School of Law Legal studies research paper NO. 2018-03 January 26, 2018. С. 147-159.

21. Брацук І. Міжнародно-правове регулювання забезпечення інформаційної безпеки в рамках ООН. *Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки*. 2023. №1(125). С.21-26.

22. Применение международного права в киберпространстве Индекс безопасности. 2015. №3(114). Т.21. С. 101-118.

23. Mukundan N. R., Prakash Sai L. Perceived information security of internal users in Indian IT services industry. Information Technology and Management. 2014. № 15 (1). P. 1–8.

24. Антипенко В.Ф. Теория уголовной ответственности государства. О.: Фенікс, 2016. 328 с

25. Важна К.А. Концепція кримінальної відповідальності держави. К.: Вид-во Ліра-К, 2017. 292 с.

26. Проект статей про відповідальність держав Комісії міжнародного права ООН 1976 року. URL: https://pns.hneu.edu.ua/mod/url/view.php?id=499798

27. United Nations. Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (A/76/135). New York, 2021.

28. Report of the GGE on Advancing responsible State behaviour in cyberspace in the context of international security. URL: https://front.un-arm. org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf 3.

29. Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies. Vienna, 2016.

30. Resolution adopted by the General Assembly on 27 December 2019 [on the report of the Third Committee (A/74/401)] 74/247. Countering the use of information and communications technologies for criminal purposes URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/440/28/PDF/ N1944028.pdf?OpenElement.

31. Resolution adopted by the General Assembly on 26 May 2021 [without reference to a Main Committee (A/75/L.87/ Rev. 1 and A/75/L.87/ Rev.1/Add.1)] 75/282. Countering the use of information and communications technologies for criminal purposes. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/133/51/PDF/N2113351.pdf?OpenElement.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~