Зінченко Олександра Ігорівна

Політичні проблеми розвитку кібертероризму в міжнародному просторі

УДК 32-042.3:[343.3/.7:004.056](100)
DOI https://doi.org/10.24195/2414-9616.2024-4.23

Зінченко Олександра Ігорівна
аспірантка кафедри політології
Харківського національного
університету імені В. Н. Каразіна
майдан Свободи, 4, Харків, Україна
ORCID: 0000-0003-1623-957X

Кібертероризм став однією з найзначніших загроз для міжнародного порядку, що викликано швидким розвитком технологій і зростанням залежності від комп'ютерних мереж. Ця загроза набуває дедалі більшої актуальності у світі, де цифрові технології проникають у всі сфери життя. Основні політичні проблеми, пов'язані з кібертероризмом, включають відсутність універсальних міжнародних стандартів, різні визначення тероризму в кіберпросторі, ризик ескалації міжнародних конфліктів і складність ідентифікації через анонімність в мережі Інтернет. Дослідження спрямоване на комплексний аналіз політичних проблем, які сприяють розвитку кібертероризму в міжнародному просторі, а також на визначення можливих шляхів їх вирішення з метою підвищення рівня міжнародної безпеки. В умовах швидкого зростання цифрових технологій і зростаючої глобальної залежності від комп'ютерних мереж, кібертероризм став однією з найзначніших загроз сучасного світу. Актуальність цього дослідження підтверджується стрімким зростанням кількості користувачів Інтернету по всьому світу, що створює нові виклики для безпеки. Особливо важливо враховувати, що в Україні кількість інтернет-користувачів теж продовжує зростати, що підвищує ризик кіберзагроз. Метою роботи є не тільки вивчення основних політичних проблем, що сприяють розвитку кібертероризму, але й пошук шляхів їх ефективного вирішення. Зокрема, дослідження зосереджене на вивченні теоретичних підходів до розуміння кібертероризму та його політичних аспектів, аналізі сучасного стану розвитку кібертероризму на глобальному рівні та виявленні ключових тенденцій. Для досягнення поставлених цілей було використано різноманітні методи дослідження, включаючи аналіз та узагальнення наукової літератури й документів, порівняльний аналіз політичних рішень у різних країнах, а також метод кейс-стаді для детального вивчення конкретних випадків кібертероризму. Системний підхід дозволив глибше зрозуміти взаємозв'язки між кібертероризмом та міжнародною політикою, що є критично важливим для формування ефективних стратегій боротьби з цією загрозою. Результати дослідження свідчать про те, що відсутність універсальних міжнародних стандартів та різні підходи до визначення кібертероризму значно ускладнюють боротьбу з цією загрозою. Це створює труднощі не лише для розслідування та покарання кіберзлочинців, але й для координації міжнародних зусиль даної сфери.

Ключові слова: *кібертероризм, міжнародний порядок, критична інфраструктура, політичні проблеми, міжнародне співробітництво, витік інформації, кібербезпека.*

Вступ. Кібертероризм, як явище, стає все більш значущим в умовах стрімкого розвитку інформаційних технологій та зростаючої залежності державних, економічних і соціальних систем від цифрових інфраструктур. Це явище представляє серйозну загрозу, оскільки створює можливості для атак на критичні інфраструктури, несанкціонованого доступу до конфіденційних даних, дестабілізації роботи урядових установ та порушення глобальної безпеки. З урахуванням глобалізаційних процесів і високого рівня обміну інформацією, кібертерористичні дії мають потенціал спричиняти міжнародні наслідки, що ускладнює боротьбу з ними та вимагає координації зусиль різних держав і міжнародних організацій. Дослідження політичних аспектів розвитку кібертероризму є ключовим для розуміння сучасних викликів та формування ефективних стратегій протидії цьому явищу.

Оглядаючи наукові праці, що досліджують кіберпростір як сучасну платформу для взаємодії політичних акторів і громадян, слід відзначити вагомі роботи Н. В. Василенко, Д. В. Дубової, Ю. В. Завгородньої, Д. С. Черняка, Р. О. Гриника та інших. Однак ці дослідження охоплюють лише окремі аспекти кіберпростору. Це підкреслює необхідність створення узагальненого підходу до сучасного протистояння політичних суб'єктів в інформаційному просторі, їхнього впливу та визначення територіальних факторів у таких конфліктах.

Мета та завдання. Метою роботи є визначення та аналіз політичних проблем, що сприяють розвитку кібертероризму в міжнародному просторі, а також дослідження можливих шляхів їх вирішення з метою підвищення рівня міжнародної безпеки. У ході дослідження необхідно визначити основні теоретичні підходи до розуміння кібертероризму та його політичних аспектів, проаналізувати сучасний стан розвитку кібертероризму на глобальному рівні та виявити основні тенденції. Крім того, дослідження охоплює аналіз впливу політичних рішень та міжнародної політики на розвиток кібертероризму, а також визначення ключових викликів, що постають перед міжнародною спільнотою у боротьбі з цим явищем.

Методи дослідження включають аналіз та узагальнення наукової літератури й документів, порівняльний аналіз політичних рішень, а також використання кейс-стаді для вивчення конкретних випадків кібертероризму. Крім того, застосовувалися методи системного підходу для оцінки

взаємозв'язків між кібертероризмом та міжнародною політикою.

Результати. Варто зазначити, що темпи технічного прогресу настільки високі, що суспільство часто не встигає усвідомити всі його наслідки до моменту, коли ситуація вже вимагає значних зусиль для її виправлення. Кількість користувачів Інтернету постійно зростає: у США їх число на 2024 рік становить 311 мільйонів, у Китаю – 1 мільярд, у Індії – 881 мільйонів, а в Азії – 1 мільярд. В Україні, за різними оцінками, число користувачів Інтернету варіюється від 25 до 29 мільйонів осіб [10].

Впровадження новітніх інформаційних технологій у сучасний світ призвело до радикальних змін у всіх сферах життя, включно з економікою, освітою, медициною, комунікаціями та багатьма іншими галузями. Однак, поряд з позитивними змінами, з'явилися й нові виклики, одним із яких є стрімке зростання кількості злочинів, пов'язаних із використанням комп'ютерних систем та інформаційних ресурсів. Це явище, яке отримало назву комп'ютерної злочинності, охоплює широкий спектр протиправних дій, таких як незаконне втручання в роботу комп'ютерних систем, крадіжка або вимагання комп'ютерної інформації, створення та поширення шкідливого програмного забезпечення.

Однією з найбільш небезпечних форм комп'ютерної злочинності є кібертероризм – явище, яке виходить за рамки простих злочинів із використанням інформаційних технологій. Кібертероризм передбачає політично вмотивовані атаки на інформаційні ресурси та інфраструктуру держав, компаній або окремих осіб з метою досягнення певних політичних, ідеологічних або релігійних цілей. Такі атаки можуть мати далекосяжні наслідки, включно із загрозою життю людей, підривом національної безпеки, порушенням функціонування критично важливих об'єктів інфраструктури, таких як енергетичні системи, транспорт, водопостачання та медичні установи.

Кібертероризм є особливо небезпечним через його високий рівень латентності, тобто прихованість та невидимість для правоохоронних органів. Сучасні технології дозволяють злочинцям здійснювати атаки з будь-якої точки світу, використовуючи складні методи маскування своїх дій та приховування слідів. Це ускладнює виявлення, розслідування та попередження таких злочинів. Крім того, кібертерористичні атаки часто вимагають міжнаціональної співпраці для їхнього розслідування та нейтралізації, оскільки злочинці можуть діяти на території однієї країни, а жертвами можуть бути громадяни або організації іншої. Враховуючи глобальний характер кібертероризму та його потенційні наслідки, важливою залишається розробка міжнародних стандартів та співпраці для боротьби з цим видом злочинності. Термін «кібертероризм» утворився з поєднання слів «кібер» (що стосується кіберпростору) і «тероризм». У сучасній літературі часто вживаються терміни «віртуальний простір» та «віртуальний світ». Виходячи з основного визначення тероризму і його інтеграції з віртуальним середовищем, кібертероризм можна визначити як цілеспрямовані політичні атаки на інформаційні системи, що створюють загрозу життю, здоров'ю людей або іншим важливим об'єктам, з метою порушення громадської безпеки, залякування населення або ініціювання військових конфліктів [2; 7].

У вітчизняній та зарубіжній науковій літературі щодо кіберзлочинності існують різні підходи до визначення кібертероризму. Наприклад, О. Г. Корченко бачить його як новий вид тероризму, що використовує інформаційні системи не лише як об'єкт злочину, але й як середовище його здійснення [4, с. 35].

Інші вчені вбачають у кібертероризмі дії з дезорганізації інформаційних систем, що загрожують життю людей або завдають значної шкоди, з метою порушення суспільної безпеки [6, с. 80]. Деякі дослідники також вважають, що комп'ютерний тероризм слід розглядати як неправомірний доступ до інформації з метою її модифікації або знищення, що створює небезпеку суспільно небезпечних наслідків [1, с. 318].

Також кібертероризм визначається як використання комп'ютерних систем та мереж для здійснення терористичних актів з метою створення страху, дестабілізації суспільства або порушення функціонування критичних інфраструктур. Автори, що активно займаються цією проблематикою, включають Стюарта Макадональда, Лі Джарвіса, Томаса М. Чена та Саймона Левіса [12].

Габріель Вайман у своїй праці «Кібертероризм: Наскільки реальна загроза?» визначає кібертероризм як злочинні атаки та загрози проти комп'ютерних систем і мереж, спрямовані на залякування або примушування урядів і населення для досягнення політичних чи соціальних цілей. Для кібертероризму характерні насильство або значна шкода, яка викликає страх [15].

Кібертероризм відрізняється від традиційного тероризму, зберігаючи лише основні елементи та ознаки, але має свої специфічні особливості. Хоча кібертероризм реалізується через інформаційні системи та засоби, він може мати наслідки, що наближаються до реального тероризму.

Основна мета інформаційного тероризму – це викликати значний суспільний резонанс і страх, при цьому вимоги терористів часто супроводжуються загрозою повторення атак без конкретних цілей. Кібертероризм переважно проявляється у вигляді атак на комп'ютерні системи, мережі передачі даних та іншу частину інформаційної інфраструктури, що можуть здійснюватися як органі-

зованими угрупованнями, так і окремими особами. Такі атаки можуть включати проникнення в системи, перехоплення управління або блокування інформаційного обміну. Ефективність кібертероризму залежить від специфіки інформаційної інфраструктури та її захищеності [2].

У цьому контексті наше дослідження зосередилося на політичних проблемах розвитку кібертероризму в міжнародному просторі. Ми проаналізували, як кібертероризм вплинув на політику, економіку та соціальну стабільність держав, а також розглянули приклади кібертерористичних атак, які мали значний вплив на політичні процеси.

Одним з таких прикладів є атака на ядерні об'єкти Ірану у 2010 році. Зокрема, розвідувальні служби США підозрювалися у причетності до створення зловмисного програмного забезпечення Stuxnet, яке було використано під час атаки на ядерні об'єкти Ірану у 2010 році. Обидві кіберкоманди США та GCHQ Великобританії відкрито визнавали застосування кібератак для боротьби з терористичними групами, включаючи ІДІЛ [3].

Протягом останніх 20 років російські угруповання, деякі з яких мають зв'язки з урядом росії, нібито здійснили численні кібератаки на інфраструктуру інших країн. Одним із перших великих прикладів державного спонсорованого кібертероризму є атака на естонський парламент, банки та телевізійні станції у 2007 році, що була реакцією на суперечку про радянські військові могили в країні.

Російські спецслужби також були звинувачені у зламі електронної пошти Національного комітету Демократичної партії США в 2015 та 2016 роках, що сприяло кампанії впливу на результати виборів 2016 року в США.

У 2015 році російське угруповання відповідало за атаку на енергосистему України. У 2017 році зловмисне програмне забезпечення NotPetya, ймовірно розроблене російською розвідкою, поширилося на системи одного з найбільших у світі контейнерних перевізників, «A.P. Moller – Maersk», завдавши збитків до 300 мільйонів доларів [14].

Наступний приклад, кібератака SolarWinds у 2020 році була складною операцією зловмисного програмного забезпечення, спрямованою на програмний продукт Orion фірми SolarWinds, що використовувався для управління IT-ресурсами. Ця атака, яка залишалася непоміченою протягом кількох місяців, дозволила хакерам шпигувати за клієнтами SolarWinds і встановлювати шкідливе програмне забезпечення в їхні системи. Цілями атаки стали фірми з кібербезпеки, урядові установи США та Microsoft, і знову було звинувачено російські спецслужби.

Злом Microsoft Exchange, виявлений у січні 2021 року, вважався прямою атакою спонсорованих китайським урядом хакерів на локальні сервери обміну Microsoft, що вплинуло на уряд, промисловість та організації громадянського суспільства. Атака використовувала вразливості нульового дня, і хакери могли мати доступ до адрес електронної пошти та паролів Microsoft ще до виявлення зламу.

Цей випадок продемонстрував розширену постійну загрозу (APT), де хакери тривалий час збирали інформацію, перш ніж атакувати. Також США підозрювали китайських хакерів у використанні кібератак як частини великомасштабної крадіжки інтелектуальної власності та промислового шпигунства [9; 11].

У березні 2022 року кілька значних кібертерористичних атак продемонстрували вплив кіберзагроз на політичну ситуацію. Наприклад, атака DDoS на Національне управління телекомунікацій Маршаллових островів порушила Інтернет-послуги на островах понад тиждень, що могло вплинути на соціальну та економічну стабільність регіону. Хакери, пов'язані з урядом Пакистану, атакували індійських державних службовців, створюючи підроблені урядові веб-сайти для доставки шкідливого ПЗ, що загострило політичну напруженість між Індією та Пакистаном.

Атака на супутниковий широкосмуговий доступ Viasat порушила інтернет-послуги по всій Європі та українські військові комунікації на початку російського вторгнення, що вплинуло на оперативну здатність українських військ. Того ж місяця хакери проникли на веб-сайти кількох російських агентств, розміщуючи антиурядові матеріали, що продемонструвало можливості впливати на внутрішню політику через кіберзагрози [13].

Міністерство юстиції США висунуло звинувачення проти російських державних службовців за хакерські кампанії, спрямовані на критичну інфраструктуру, що підкреслило міжнародну напруженість і загрози для глобальної енергетичної безпеки. Проникнення в мережі Національної дослідницької ради Канади та атака китайських хакерів на американські державні мережі виявили вразливість важливих наукових і дослідницьких інститутів, а також загрозу кібершпигунства, що могло загрожувати національній безпеці США. Ці інциденти ілюструють, як кібертероризм може суттєво вплинути на політичну ситуацію, економічну стабільність та національну безпеку.

Зазначимо, що у період січень–лютий 2024 року команда CERT-UA здійснила заходи для запобігання деструктивним атакам на три українські організації в урядовому та енергетичному секторах. Аналіз виявив, що зловмисники отримали несанкціонований доступ до інформаційно-комунікаційних систем (ІКС) заздалегідь, використовуючи скомпрометовані облікові записи VPN і вразливості програмного забезпечення публічних систем.

Водночас проведено аналіз кібершпигунства, зокрема, дій угруповань UAC-0028 (APT28) та UAC-

0003 (Turla) з використанням модифікованого шкідливого програмного забезпечення KAZUAR. У першому кварталі 2024 року активно діяло угрупування UAC-0050, пов'язане з правоохоронними структурами росії, що застосовувало різноманітні шкідливі програми, такі як REMCOS RAT, QUASAR RAT, VENOM RAT, REMOTE UTILITIES і LUMMASTEALER. Це угрупування активно використовує тактику викрадення автентифікаційних даних, що може створити технічні умови для подальших атак.

CERT-UA вживає ефективні заходи протидії щодо угрупування UAC-0010, проте масштабність загроз вимагає об'єднання зусиль не лише на рівні національних органів кібербезпеки України, але й з міжнародними технологічними стейкхолдерами [8].

Кібертероризм є однією з найбільших і найсерйозніших загроз для міжнародного порядку в умовах стрімкого розвитку сучасних технологій. Це явище виходить далеко за межі традиційного розуміння тероризму, оскільки воно включає використання комп'ютерних мереж, інформаційних систем та інших технологічних засобів для здійснення терористичних актів. Кібертероризм охоплює широкий спектр дій, які можуть мати катастрофічні наслідки для держав, підприємств і громадян по всьому світу. До таких дій належать атаки на критично важливу інфраструктуру, наприклад, енергетичні мережі, транспортні системи, водопостачання та комунікації, які є життєво важливими для нормального функціонування суспільства та економіки. Крім того, кібертерористи можуть здійснювати крадіжку або витік конфіденційної інформації, що може поставити під загрозу національну безпеку, приватне життя громадян і роботу державних установ.

Політичні проблеми, пов'язані з кібертероризмом, є надзвичайно складними і багатогранними, оскільки вони торкаються різних аспектів міжнародних відносин, правового регулювання, національної безпеки та соціальної стабільності. Однією з головних труднощів, з якою стикаються уряди та міжнародні організації у боротьбі з кібертероризмом, є складність правового регулювання цього явища. Кожна країна має свої унікальні правові системи, що ускладнює створення єдиного міжнародного підходу до визначення та боротьби з кібертероризмом. Це призводить до того, що багато аспектів кібертероризму залишаються юридично не врегульованими, що створює можливості для злочинців уникати відповідальності та продовжувати свою діяльність безкарно. У таких умовах виникає необхідність у створенні нових правових механізмів і міжнародних угод, які б дозволили ефективніше боротися з цією загрозою.

Одним із найскладніших питань, пов'язаних із кібертероризмом, є визначення тероризму в кіберпросторі. Через те, що кібертероризм відрізняється від традиційних форм тероризму використанням сучасних технологій, він потребує нового підходу до його розуміння та визначення. Відсутність єдиного визначення кібертероризму ускладнює процес розробки ефективних правових норм і політик, спрямованих на запобігання та боротьбу з цим явищем. Це також призводить до розбіжностей у підходах до розслідування і покарання кібертерористів, що, своєю чергою, знижує ефективність міжнародної співпраці в цій сфері.

Ризик ескалації конфліктів є ще одним важливим політичним аспектом кібертероризму. Атаки на критично важливу інфраструктуру можуть призвести до серйозних економічних, соціальних та політичних наслідків, які в свою чергу можуть стати каталізатором для виникнення міжнародних конфліктів. Наприклад, кібертерористичні атаки на енергетичні системи можуть спричинити масові відключення електроенергії, що призведе до порушення роботи підприємств, лікарень, транспортних систем та інших життєво важливих служб. Це може спричинити паніку серед населення, завдати значних економічних збитків і навіть спровокувати соціальні заворушення. У випадку, коли кібертерористичні атаки здійснюються з території однієї країни на іншу, це може призвести до серйозного дипломатичного конфлікту, а в деяких випадках навіть до військових дій. Отже, кібертероризм має потенціал до швидкої ескалації конфліктів, що підкреслює важливість міжнародної співпраці у боротьбі з цією загрозою. Одним з найбільш проблемних аспектів кібертероризму є анонімність, яку забезпечує Інтернет. Кібертерористи можуть діяти приховано, використовуючи складні методи шифрування та маскування своїх дій, що значно ускладнює їхнє виявлення та притягнення до відповідальності. Це означає, що кібертерористи можуть здійснювати атаки з будь-якої точки світу, не ризикуючи бути ідентифікованими або заарештованими. Така анонімність створює серйозну проблему для правоохоронних органів, оскільки вони часто не мають можливості ефективно розслідувати такі злочини та притягнути винних до відповідальності. Крім того, відсутність міжнародних стандартів для боротьби з кібертероризмом ускладнює координацію зусиль між державами, що ще більше знижує ефективність боротьби з цією загрозою.

Таким чином, кібертероризм є надзвичайно серйозною і складною загрозою для міжнародного порядку та безпеки в сучасних умовах. Він вимагає нових підходів до правового регулювання, визначення тероризму в кіберпросторі, а також посилення міжнародної співпраці для запобігання ескалації конфліктів і боротьби з анонімністю кібертерористів. Тільки через спільні зусилля та гармонізацію правових норм країни можуть ефективно

протистояти цій новітній загрозі та забезпечити безпеку в глобальному масштабі.

По-перше, відсутність універсальних міжнародних стандартів для боротьби з кібертероризмом ускладнює розслідування та покарання злочинців. Різні країни мають різні рівні захисту та законодавчі підходи до кібербезпеки, що створює правові прогалини та перешкоди для міжнародної співпраці. Наприклад, у грудні 2015 року в Україні відбулася масштабна атака на електричну інфраструктуру, що призвела до відключення електрики в кількох областях. Ця атака показала, як кібертероризм може безпосередньо вплинути на фізичну інфраструктуру та продемонструвала складність міжнародного правового регулювання.

По-друге, визначення, що саме є кібертероризмом, може варіюватися в залежності від юрисдикції. Це створює труднощі у формулюванні спільних стратегій і політик для боротьби з кібертероризмом. Конфлікт між різними визначеннями тероризму в кіберпросторі ускладнює координацію міжнародних зусиль. У 2016 році атака на електронні листи кампанії Хілларі Клінтон продемонструвала, як витік конфіденційної інформації може вплинути на політичний клімат і результати виборів, підкреслюючи важливість чіткого визначення кібертероризму.

По-третє, атаки на комп'ютерні системи критичної інфраструктури можуть призвести до серйозних наслідків для національної безпеки, економіки та суспільства, що може спричинити ескалацію міжнародних конфліктів. Наприклад, атака на компанію Sony Pictures у 2014 році, ймовірно здійснена північнокорейськими хакерами, призвела до витоку конфіденційної інформації і фінансових збитків, підкреслюючи ризик ескалації конфліктів через кібертероризм.

По-четверте, анонімність в інтернеті та глобальна природа кібернетичних інфраструктур ускладнюють ідентифікацію та затримання кібертерористів. Багато атак здійснюється з територій, де відсутні відповідні закони або контроль за діяльністю, що робить боротьбу з кібертероризмом ще більш складною.

По-п'яте, кібертероризм не тільки становить загрозу національній безпеці та економіці, але й має потенціал призводити до серйозних політичних суперечок між окремими представниками країн або навіть між самими країнами. Коли одна держава підозрює іншу у підтримці або здійсненні кібертерористичних атак, це може викликати напруженість, дипломатичні конфлікти та підвищення ризику ескалації до військових дій [5; 11].

Наприклад, коли атаки пов'язані з політично чутливими питаннями або впливають на критично важливі національні інтереси, країни можуть вдатися до відповідних заходів, які включають санкції, кібервійни або навіть військові дії. У світі, де Інтернет є невід'ємною частиною глобальної інфраструктури, політичні конфлікти, спричинені кібертероризмом, можуть швидко виходити за межі віртуального простору, перетворюючись на реальні загрози міжнародній безпеці та миру.

Варто зазначити, що боротьба з кібертероризмом потребує комплексного підходу, в основі якого лежить важливість міжнародного співробітництва та технологічних інновацій. Міжнародне співробітництво є критично важливим, оскільки кібертероризм є глобальною загрозою, яка не зупиняється на національних кордонах. Для ефективного реагування на такі загрози країни повинні обмінюватися інформацією про кіберзагрози, координувати дії під час атак і розробляти спільні міжнародні угоди та стандарти кібербезпеки.

Окрім цього, технологічні інновації є надзвичайно важливими для боротьби з кібертероризмом. Розвиток новітніх технологій, таких як штучний інтелект та блокчейн, сприяє вдосконаленню систем захисту від кіберзагроз і допомагає виявляти та нейтралізувати атаки. Підвищення рівня кібербезпеки включає впровадження сучасних систем захисту, регулярні оновлення програмного забезпечення та навчання персоналу. Ці заходи є критично важливими для забезпечення надійного захисту як державних, так і приватних структур від потенційних кібертерористичних атак [5; 13].

Висновки. Таким чином, політичні проблеми, пов'язані з кібертероризмом, є складними й багатогранними, адже вони охоплюють різноманітні аспекти, що включають правові, технологічні, соціальні та навіть культурні виміри. Однією з головних труднощів, яка стоїть на шляху до ефективної боротьби з кібертероризмом, є відсутність єдиного правового визначення цього явища на міжнародному рівні. Кожна держава по-різному інтерпретує термін «кібертероризм», що призводить до різних підходів у розробці законодавства, спрямованого на його попередження та боротьбу з ним. Ця неоднорідність у визначеннях створює правові прогалини, які можуть бути використані злочинцями для уникнення відповідальності, переховування від правосуддя або мінімізації наслідків своїх дій. Відсутність єдиного підходу до визначення кібертероризму ускладнює процес формування ефективного законодавства, яке б охоплювало всі можливі форми та прояви цього небезпечного явища. Крім того, однією з ключових загроз, що випливають з кібертероризму, є його потенціал до швидкої ескалації конфліктів. Атаки, здійснені в кіберпросторі, можуть бути спрямовані на критичну інфраструктуру, таку як енергетичні системи, транспортні мережі, водопостачання, фінансові установи або навіть системи охорони здоров'я. Від успішності цих інфраструктурних систем залежить нормальне функціонування держави та її суспільства. Якщо кібертерористи вдаються до атак на

такі об'єкти, це може мати катастрофічні наслідки, що виходять далеко за межі локальних проблем. Це можуть бути серйозні економічні, соціальні, політичні наслідки, які вплинуть на життя мільйонів людей, зруйнують економіки, спровокують масові безлади та навіть призведуть до політичної дестабілізації в окремих регіонах або державах. Атаки на критичну інфраструктуру можуть спровокувати ланцюгову реакцію, коли одна атака призводить до серії інших, що може призвести до ще більш масштабних наслідків.

Однак, не менш важливим аспектом кібертероризму є проблема анонімності, яку забезпечує Інтернет. У мережі кібертерористи можуть діяти практично безкарно, використовуючи складні методи шифрування, анонімні облікові записи, фальшиві ідентифікатори та інші технології, що ускладнюють їх виявлення і притягнення до відповідальності. Анонімність надає злочинцям відчуття безпеки, що стимулює їх до здійснення нових атак. Інтернет дає їм можливість діяти з будь-якої точки світу, що робить їх переслідування і арешт вкрай складним завданням для правоохоронних органів. Крім того, відсутність загальноприйнятих міжнародних стандартів для боротьби з кібертероризмом ще більше ускладнює координацію зусиль між державами. Кожна країна може мати свої власні підходи та законодавчі ініціативи в цій сфері, що призводить до розбіжностей у трактуванні дій та застосуванні покарань. Ця ситуація підкреслює нагальну потребу в посиленні міжнародної співпраці та розробці спільних підходів до виявлення, попередження і покарання кібертерористичних актів. Лише через тісну співпрацю та гармонізацію правових норм країни можуть ефективно протистояти загрозам кібертероризму. Це передбачає обмін інформацією між державами, спільні розслідування кібертерористичних актів, розробку загальноприйнятих правових норм і процедур для переслідування злочинців, а також впровадження освітніх програм, що підвищують рівень обізнаності про кібертероризм серед населення. У сучасному світі, де технології розвиваються з неймовірною швидкістю, а кібертероризм стає все більш актуальною загрозою, міжнародна співпраця є єдиним шляхом досягнення ефективної протидії цьому явищу.

ЛІТЕРАТУРА:

1. Бутузов В.М.,Тітутіна К.В. Сучасні загрози: комп'ютерний тероризм. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2007. №17. С. 316-324.

2. Гриник Р.О., Пилипенко В.М. Кібертероризм як нова форма міжнародного тероризму. *Актуальні задачі та досягнення у галузі кібербезпеки. Матеріали Всеукраїнської науково-практичної конференції 34-35 листопада 2016 року м. Кропивницький.* 2016. С. 61-62.

3. Іран звинуватив США у кібератаці на ядерні об'єкти. URL: https://ua.korrespondent.net/world/1174673-iran-zvinuvativ-ssha-u-kiberataci-na-yaderni-obekti

4. Корченко О.Г. Ознаковий принцип формування класифікацій кібератак. *Вісник Східноукраїнського національного університету імені Володимира Даля*. №1, 2010. С. 32-38.

5. Котляров, В. Кібертероризм як загроза міжнародній безпеці. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління, 2023. №*(5(71), С. 46-54.

6. Погорецький М.А. Поняття кіберпростору як середовища вчинення злочину. *Інформаційна безпека людини, суспільства, держави*. №2 (2), 2009. С. 80.

7. Соколов А.В., Степанюк О.М. Захист від комп'ютерного тероризму. Довідковий посібник. СПб.: БХВ – Петербург; Арліт 2002. 496 с.

8. Щодо обстановки в сфері кібер на 23-24 лютого 2024 року. URL: https://cert.gov.ua/article/6277822

9. Arora B. Exploring and analyzing Internet crimes and their behaviours. Perspect Sci. 2016;8:540–2.

10. *Internet Users by Country 2024*. (б. д.). World Population by Country 2024 (Live). https://worldpopulationreview.com/country-rankings/internet-users-by-country

11. Lee CS, Choi KS, Shandler R, Kayser C. Mapping global cyberterror networks: an empirical study of Al-Qaeda and ISIS cyberterrorism events. J Contemp Crim Justice. 2021;37(3):333–55.

12. Macdonald, S., Jarvis, L., Chen, T. & Lavis, S. (2013). Cyberterrorism: A Survey of Researchers. Cyberterrorism Project Research Report (No. 1), Swansea University. URL: www.cyberterrorism-project.org

13. Plotnek JJ, Slay J. Cyber terrorism: a homogenized taxonomy and definition. Comput Secur. 2021;102:1–9

14. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

REFERENCES:

1. Butuzov, V., & Titutina, K. (2007). Suchasni zahrozy: komp'yuternyy teroryzm. [Modern threats: computer terrorism]. Borot'ba z orhanizovanoyu zlochynnistyu i koruptsiyeyu (teoriya i praktyka) [Fight against organized crime and corruption (theory and practice)], (17), 316-324.

2. Hrynyk R., & Pylypenko V. Kiberteroryzm yak nova forma mizhnarodnoho teroryzmu [Cyberterrorism as a new form of international terrorism]. Aktual'ni zadachi ta dosyahennya u haluzi kiberbezpeky. Materialy Vseukrayins'koyi naukovo-praktychnoyi konferentsiyi [Actual tasks and achievements in the field of cyber security. Materials of the All-Ukrainian Scientific and Practical Conference], 34-35 October 2016,Kropyvnytskyi. 2016. S. 61-62.

3. Iran zvynuvatyv SSHA u kiberatasi na yaderni ob'yekty [Iran accused the US of a cyberattack on nuclear facilities]. (2011, 18 January). https://ua.korrespondent.net/world/1174673-iran-zvinuvativ-ssha-u-kiberataci-na-yaderni-obekti

4. Korchenko O. Oznakovyy pryntsyp formuvannya klasyfikatsiy kiberatak. Visnyk Skhidnoukrayins'koho natsional'noho universytetu imeni Volodymyra Dalya. №1, [The characteristic principle of forming classifications of cyberattacks. Bulletin of the Eastern Ukrainian National University named after Volodymyr Dahl] 2010. S. 32-38.

5. Kotlyarov V. Kiberteroryzm yak zahroza mizhnarodniy bezpetsi. Naukovi pratsi Mizhrayonoyi Akademiyi upravlinnya personalom. Politychni nauky ta publichne upravlinnya, [Cyberterrorism as a threat to international security. Scientific works of the Interregional Academy of Personnel Management. Political science and public administration] 2023. №5(71). S. 46-54.

6. Pohorets'kyy M.A. Ponyattya kiberprostoru yak seredovyshcha vchynennya zlochynu. *Informatsiyna bezpeka lyudyny, suspil'stva, derzhavy*. The concept of cyberspace as an environment for committing a crime. *Information security of a person, society*, state. №2(2), 2009. S. 80.

7. On the situation in the cyber sector as at February 23-24, 2024. (2024, 23 лютого). cert.gov.ua. https://cert.gov.ua/article/6277822

8. Arora B. Exploring and analyzing Internet crimes and their behaviours. Perspect Sci. 2016;8:540–2.

9. Internet Users by Country 2024. URL: https://worldpopulationreview.com/country-rankings/internet-users-by-country

10. Lee C.S., Choi K.S., Shandler R., Kayser C. Mapping global cyberterror networks: an empirical study of Al-Qaeda and ISIS cyberterrorism events. J Contemp Crim Justice. 2021;37(3):333–55.

11. Macdonald S., Jarvis L., Chen T., Lavis S. Cyberterrorism: A Survey of Researchers. Cyberterrorism Project Research Report (No. 1), Swansea University. URL: www.cyberterrorism-project.org

12. Plotnek J.J., Slay J. Cyber terrorism: a homogenized taxonomy and definition. Comput Secur. 2021;102:1–9.

13. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

14. Weimann G. Cyberterrorism. How Real Is the Threat? United States Institute of Peace. URL: https://www.usip.org/sites/default/files/sr119.pdf

Political issues in the development of cyberterrorism in the international space

Zinchenko Oleksandra Ihorivna

Postgraduate Student at the Department of Political Science
V. N. Karazin Kharkiv National University
Svobody Sq., 4, Kharkiv, Ukraine
ORCID: 0000-0003-1623-957X

Cyberterrorism has become one of the most significant threats to the international order, driven by the rapid development of technology and growing dependence on computer networks. This threat is becoming increasingly relevant in a world where digital technologies are penetrating all spheres of life. The main political issues related to cyberterrorism include the lack of universal international standards, different definitions of terrorism in cyberspace, the risk of escalation of international conflicts and the difficulty of identification due to anonymity on the Internet. The study aims to provide a comprehensive analysis of the political issues that contribute to the development of cyberterrorism in the international space, as well as to identify possible ways to address them in order to improve international security. In the context of the rapid growth of digital technologies and growing global dependence on computer networks, cyberterrorism has become one of the most significant threats to the modern world. The relevance of this study is confirmed by the rapid growth in the number of Internet users around the world, which creates new security challenges. It is especially important to take into account that the number of Internet users in Ukraine also continues to grow, which increases the risk of cyber threats. The purpose of this paper is not only to study the main political issues that contribute to the development of cyberterrorism, but also to find ways to effectively address them. In particular, the study focuses on theoretical approaches to understanding cyberterrorism and its political aspects, analysing the current state of cyberterrorism at the global level and identifying key trends. To achieve these goals, various research methods were used, including analysis and synthesis of scientific literature and documents, comparative analysis of policy decisions in different countries, and a case study method for a detailed study of specific cases of cyberterrorism. The systematic approach allowed for a deeper understanding of the relationship between cyberterrorism and international politics, which is critical for the development of effective strategies to combat this threat. The results of the study show that the lack of universal international standards and different approaches to the definition of cyberterrorism significantly complicate the fight against this threat. This creates difficulties not only for the investigation and punishment of cybercriminals, but also for the coordination of international efforts in this area.

Key words: *cyberterrorism, international order, critical infrastructure, political issues, international cooperation, information leakage, cybersecurity.*