УДК / UDC: 342.951
DOI: https://doi.org/10.37750/2616-6798.2026.1(56).357372

Олександр Павлович Федієнко
ORCID: https://orcid.org/0009-0008-5383-3504

ЗАГРОЗЛИВІ ТЕНДЕНЦІЇ ПОШИРЕННЯ КІБЕРТЕРОРИЗМУ

Анотація. *Визначені зміст, типові ознаки, мета та завдання кібертероризму. Розкрито об'єкти посягання актів кібертероризму. Узагальнено загрозливі тенденції поширення кібертероризму. Розглянуто найбільш поширені методи здійснення актів кібертероризму. Визначено особливості кібератаки терористичного спрямування. Наведено приклади кібертерористичних посягань у світовій практиці. Деталізовано співвідношення між кібертероризмом та кіберзлочинністю, хактивізмом та кібервійною. Окреслено ландшафт кіберзагроз як складову кібертерористичних посягань. Визначено сфери та об'єкти зацікавленості кібертерористів, розкрито напрями досягнення ними своїх цілей, що включає зокрема поширення пропаганди та ідеології тероризму, маніпулювання свідомістю та громадською думкою. Висвітлено загрози кібертерористичних посягань під час проведення виборів. Узагальнено подальші шляхи удосконалення вітчизняного законодавства щодо посилення заходів у сфері боротьби з кібертероризмом з урахуванням рекомендацій ЄС та національних потреб.*

Ключові слова: *кібертероризм, кіберпростір, кібердомен, кіберзагроза, кібератака, кіберзлочинність, мережа Інтернет, терористичний контент, дезінформація, пропаганда ідеології тероризму, антитерористична безпека, електронні комунікаційні системи, комп'ютерні мережі, хактивізм.*

Oleksandr P. Fedienko
ORCID: https://orcid.org/0009-0008-5383-3504

DANGEROUS TRENDS OF SPREADING CYBERTERRORISM

Summary. *The content, typical signs, purpose and tasks of cyberterrorism are determined. The targets of cyberterrorism attacks have been revealed. The threatening trends in the spread of cyberterrorism are summarized. The most common methods of committing acts of cyberterrorism are considered. The features of a terrorist cyberattack are determined. Examples of cyberterrorism attacks in world practice are given. The relationship between cyberterrorism and cybercrime, hacktivism and cyberwar are detailed. The landscape of cyberthreats as a component of cyberterrorism attacks is outlined. The spheres and objects of interest of cyberterrorists are determined, the directions for achieving their goals are revealed, which includes in particular the spread of propaganda and ideology of terrorism, manipulation of consciousness and public opinion. The threats of cyberterrorism attacks during elections are highlighted. Further directions of improving domestic legislation to strengthen measures in the field of combating cyberterrorism are summarized, taking into account EU recommendations and national needs.*

Keywords*: cyberterrorism, cyberspace, cyberdomain, cyberthreat, cyberattack, cybercrime, Internet, terrorist content, disinformation, propaganda of terrorist ideology, anti-terrorist security, electronic communication systems, computer networks, hacktivism.*

Постановка проблеми. Сучасна модель глобалізації сприяє розширенню географії міжнародного тероризму, зокрема і у кіберпросторі. Геополітична нестабільність посилює ризики масштабування і поширення катастрофічних кібератак. Такі атаки можуть бути спрямовані на викрадення даних та провокування системних збоїв у роботі важливих об'єктів: військової інфраструктури, систем охорони здоров'я, транспорту, енергетики, водопостачання, атомної енергетики, фінансових установ та інших об'єктів критичної інфраструктури. Масштабні кібератаки, які постійно та динамічно зростають у світових масштабах, тісно пов'язані та супроводжуються поширенням загрози кібертероризму, яка залишається одним із серйозних викликів як для національної безпеки держав, так і міжнародної. За таких умов в сучасному світі межа між цифровим і фізичним простором поступово стирається, що значно підсилює потенційні наслідки кібертерористичних атак та дозволяє розглядати кіберпростір як один із ключових інструментів впливу на критичну інфраструктуру держави.

Загалом кібертероризм – це явище глобального масштабу, яке виходить за межі національних кордонів, є багатоаспектним феноменом, який обумовлений безконтрольним використанням глобальних мереж, а його типовою ознакою є прояви насильства та поширення кіберзагроз. Кібертероризм являє собою терористичну діяльність, яка здійснюється у кіберпросторі або з його використанням та полягає у навмисному використанні комп'ютерних мереж для заподіяння шкоди критичній інфраструктурі, державним та приватним інформаційним мережам і ресурсам, електронним комунікаційним системам. Кібертероризм набуває обертів в умовах стрімкого розвитку інформаційних технологій та зростаючої залежності від цифрової інфраструктури, що створює можливості для кібератак на критичні інфраструктури, несанкціонованого доступу до конфіденційних даних, дестабілізації роботи урядових установ та порушення глобальної безпеки [1, с.154].

Спектр розповсюдження загроз кібертероризму досить широкий: від незаконного втручання у сферу прийняття управлінських рішень, поширення паніки, страху, провокування масових заворушень і до протиправного проникнення в системи супутникового зв'язку, навігації, управління об'єктами енергетики, транспорту, фінансового та банківського секторів тощо. На відміну від звичайного терориста, який для досягнення своїх злочинних цілей використовує зброю або вибухівку, кібертерорист оперує сучасними інформаційними технологіями, комп'ютерними мережами, шкідливим програмним забезпеченням, яке спеціально призначене для несанкціонованого проникнення в комп'ютерні системи і організації дистанційної атаки на інформаційно-комунікацйні ресурси об'єкта нападу [2, с.35-36]. Кібертероризм може мати руйнівні наслідки, при цьому авторитет та імідж будь-якої держави світу можуть бути спотворені, а в деяких випадках кібертерористичні атаки навіть можуть призвести до загибелі людей. Таким чином, кібертероризм, зазвичай, стосується та включає протиправні різноманітні заходи, починаючи від звичайного поширення пропаганди ідеології тероризму в мережі Інтернет до фізичного знищення інформації і навіть планування й здійснення терористичних атак за допомогою комп'ютерних мереж. Об'єкти посягання актів кібертероризму охоплюють широкий спектр життєво важливих систем, цифрових ресурсів та суспільних відносин. Форми кібертероризму можуть проявлятися як у поширенні терористичного контенту, так і у вчиненні протиправних дій шляхом несанкціонованого доступу до державних і приватних інформаційних ресурсів, електронно-коммунікаційних систем та комп'ютерних мереж. Такі дії здатні спричиняти морально-психологічний тиск, залякування населення, провокування масових заворушень та дестабілізацію суспільно-політичної ситуації.

Кібертерористичні акти можуть завдати серйозної шкоди державним інтересам, заподіяти дестабілізацію будь-якого політичного режиму, підірвати економічну стійкість і спровокувати загострення соціальних конфліктів. За таких умов існує вірогідність збільшення переліку сфер та вразливостей, які можуть активно використовуватися кібертерористами, а їхніми потенційними цілями загрозливих кібертерористичних спрямувань можуть стати: комп'ютерні мережі, державні інформаційні ресурси та інформація, вимога щодо захисту яких встановлена законом в інформаційних, електронних комунікаційних системах, державна і банківська таємниця, автоматизовані та інтелектуальні системи управління технологічними процесами, транспортом, фінансами, водопостачанням, паливно-енергетичним комплексом, хімічною, медичною, металургійною, ядерною, космічною промисловістю, військові об'єкти та органи військового управління, об'єкти критичної інфраструктури, цифрові сервіси сфери надання послуг тощо.

Кібертерористичні посягання також можуть бути спрямовані на втручання через мережу Інтернет в навігаційні системи управління суднами й літаками, проведення дистанційної зміни конфіденційних даних, наприклад тих, що встановлюють компоненти та формули для виробництва ліків у фармацевтичній галузі тощо. Кібертерористи прагнуть проникнути до урядових та приватних комп'ютерних систем, паралізувати роботу або принаймні вивести з ладу військово-промисловий комплекс, банківсько-фінансовий сектор, інші галузі та державні сервіси. Окрім того, кібертерористичні атаки потенційно можуть спричинити значні людські втрати внаслідок порушення функціонування критичних систем життєзабезпечення, оскільки також посягають на життя громадян за наслідками масштабних збоїв у штатній роботі комп'ютерних та операційних систем, провокування ймовірного настання техногенних або екологічних катастроф.

Адже в Україні зберігається високий ризик техногенних аварій та екоциду, особливо в умовах тривалої російської військової агресії, цілеспрямованих ворожих кібератак на об'єкти критичної інфраструктури. Тобто кібертероризм залишається суттєвою загрозою для національної безпеки України, особливо в умовах правового режиму воєнного стану, що вимагає уточнення перспективних шляхів, спрямованих на удосконалення законодавчого забезпечення з метою вироблення ефективного механізму профілактики, запобігання та протидії цьому негативному явищу, що засвідчує актуальність обраного тематичного напряму цієї наукової статті.

Результати аналізу наукових публікацій. Поняття, зміст та феномен кібертероризму досліджували у своїх наукових працях: І. Білан [3], І. Діордиця [5], Ю. Когут [7], Д. Мельник [11], В. Топчій [13] та інші. Кібертероризм як загроза національній та міжнародній безпеці перебував у фокусі уваги: О. Геращенка [4], А. Драгоненка та І. Федорчака [6], В. Котлярова [8], Я. Мазура [10]. Науковий пошук оптимальних шляхів удосконалення міжнародної співпраці у сфері боротьби з кібертероризмом здійснювали: А. Лисеюк та Т. Свінцицька [9], О. Поляков [12], Р. Шелковський [14]. На сторінках зарубіжних видань та у авторитетних іноземних публікаціях особливу увагу кібертероризму приділяли: М. Грос, Д. Канетті, Д. Вашді [15], Д. Броєдс, Ф. Крістіано, Д. Веджеманс [16], С. Іфтіхар [17], Т. Стивенс [18]. Проте жоден із вказаних фахівців предметно не розглядав загрозу кібертероризму в умовах цифрової трансформації, динамічного технологічного розвитку з урахуванням факторів поширення тривалої російської військової агресії.

Мета статті передбачає на підставі проведеного аналізу узагальнити сучасні загрозливі тенденції поширення кібертероризму, уточнити пріоритети і подальші шляхи

удосконалення законодавчої бази у сфері боротьби з терористичною та диверсійною діяльністю у частині формування системи протидії кібертероризму та кібердиверсіям.

Виклад основного матеріалу. У сучасних умовах цифровізації суспільства залежність від інформаційних технологій значно зростає, що актуалізує проблему кібертероризму. Страх перед кібертероризмом призводить до необхідності збільшення витрат на заходи у сфері посилення стану забезпечення кібербезпеки як з боку урядів, так і приватних компаній, оскільки він може призвести до чисельних фінансових втрат й збитків як для бізнесу, так і для урядів держав світу, а також заподіяти шкоду економічній стабільності та економічній безпеці. Для досягнення своїх цілей кібертерористи можуть здійснювати як кібератаки високої інтенсивності, так і вчиняти акти кібертероризму з використанням кіберможливостей з основною метою викликати масовий страх, паніку, занепокоєння або спровокувати масові безлади, порушення громадського порядку. Акти кібертероризму зазвичай включають політично, ідеологічно або соціально мотивовані кібератаки, спрямовані на критичну інфраструктуру, призводять до значної шкоди або становлять серйозну загрозу національній безпеці. Таким чином, як вже зазначалося, кібертероризм як загроза може посягати не тільки на державні чи приватні інтереси, а також спрямовуватися на ключові сфери державної політики, зокрема: основи національної безпеки, конституційного ладу, територіальної цілісності, громадську безпеку, державні електронні комунікаційні системи тощо.

Світова спільнота розглядає кібертероризм не як різновид хакерства, а саме як особливо тяжкий злочин проти людяності, оскільки його кінцевою метою є залякування населення та спричинення тиску на органи державної влади для досягнення своїх політичних, військових або інших цілей шляхом проведення кібератак або в інший спосіб. На відміну від звичайної кіберзлочинності та хактивізму, де головною мотивацією виступають збагачення та фінансова вигода, кібертероризм завжди має **ідеологічне підґрунття** і спрямований на провокування масштабних негативних соціальних наслідків, включаючи зокрема психологічний вплив на свідомість громадян, демонстрацію хибності та уразливості держави, її інституцій перед загрозою кібертероризму. Кібертероризм передбачає підбурювання до терору, провокування дестабілізації, переслідуючи при цьому політичні або ідеологічні цілі. Основною метою кібертерористичних дій є створення атмосфери страху та дестабілізація суспільних процесів. Вказана ознака відрізняє кібертероризм від звичайних суміжних кримінальних правопорушень, а також від кіберзлочинів, таких як: комп’ютерне шахрайство, розповсюдження шкідливого програмного забезпечення, несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж тощо. Навіть якщо кібертероризм завдає шкоди або загрожує індивідуальним інтересам, таким як життя чи здоров’я людей, це є непрямим впливом та не є його кінцевою метою, оскільки такі протиправні злочинні дії спрямовані і посягають, у першу чергу, переважно саме на державні інтереси у сфері національної безпеки.

В умовах тривалої російської військової агресії проти України держава-терорист застосовує гібридні форми та методи впливу на громадську та суспільну думку (зокрема через інтернет-ресурси, електронні видання), активно використовує представників уразливих соціально-демографічних та радикально налаштованих груп населення як механізм поширення терористичної активності. В сучасних умовах Інтернет-простір формує унікальне середовище для поширення терористичної ідеології. Транснаціональні терористичні угруповання, хакери та інші злочинні суб’єкти активно використовують

його для підготовки майбутніх терористичних актів. Крім того, кіберпростір залишається ідеальним середовищем для індоктринації і організації навчання прихільників і членів (кібер)терористичних організацій. У цьому контексті члени (кібер)терористичного угруповання можуть обмінюватися думками, ідеями, поширювати ідеологію тероризму, включаючи технічні знання (наприклад поширювати стадії процесу виготовлення вибухівки або алгоритми розробки шкідливого програмного забезпечення) з метою здійснення терористичних кібератак у майбутньому.

Саме поширення пропаганди ідеології тероризму з використанням мережі Інтернет є досить простим процесом, який не вимагає наявності спеціальних знань, вмінь та навичок, а технічні витрати на передавання певного повідомлення, зберігаючи при цьому анонімність його відправника, є досить низькими, при цьому відповідне повідомлення може поширюватися та тиражуватися без попередньої цензури чисельну кількість разів на абсолютній високій швидкості. Це дозволяє широкому загалу користувачів дізнаватися про повідомлення, які поширює (кібер)терористична група, навіть тим, хто не є прямими одержувачами такого виду кореспонденції. Завдяки цьому (кібер)терористична організація отримує розголос або набуває скандальної популярності та, зрештою формує штат нових прихильників. Так само мережа Інтернет дозволяє (кібер)терористичній організації анонсувати про майбутнє здійснення тієї чи іншої (кібер)терористичної атаки або взяти на себе відповідальність за скоєне. Мережа Інтернет забезпечує належні умови для формування стратегій фінансування кібертерористичних груп. Будь-яке терористичне угрупування може загрожувати електронно-комунікаційним системам, розташованим будь-де навколо світу, а виявити та своєчасно нейтралізувати віртуального терориста досить складно. Акти кібертероризму можуть бути вчинені декількома різноманітними способами, зокрема, це може бути: несанкціоноване отримання доступу до відомостей та інформації, які становлять державну або банківську таємницю, інформації з обмеженим доступом, викрадення персональних даних; втручання у сферу інформаційного простору – знищення мереж зв’язку та електропостачання, створення перешкод, використання шкідливого програмного забезпечення, викрадення або знищення даних, програм, технічних ресурсів шляхом зламу систем захисту, поширення вірусів, програмних закладок; втручання у програмне забезпечення, дезінформації, демонстрація потужностей та можливостей терористичної організації, висування ними своїх ультиматумів і вимог, проведення інформаційно-психологічних операцій тощо.

До найбільш поширених методів здійснення кібертерористичних атак належать: 1). поширення шкідливого програмного забезпечення, зокрема це віруси, хробаки, трояни та програми-вимагачі, які можуть використовуватися для компрометації комп’ютерних систем та з метою викрадення конфіденційної інформації, порушення штатної роботи критично важливої інфраструктури або створення паніки чи хаосу; 2). Фішингові атаки, які передбачають використання оманливих електронних листів, веб-сайтів або повідомлень, щоб обманом змусити розкрити конфіденційну інформацію, таку як облікові дані для входу в систему, фінансові або особисті дані, також ці тактики можуть бути використані для збору розвідувальних даних або доступу до критично важливих систем, зокрема як частину фішингового повідомлення кібертерористи зазвичай надсилають посилання на шкідливі вебсайти, закликають користувача завантажити шкідливе програмне забезпечення або запитують конфіденційну інформацію безпосередньо через електронну пошту, системи обміну текстовими повідомленнями або платформи соціальних мереж; 3). Атаки відмови в обслуговуванні (DoS або DDoS) — це спеціальні атаки на комп’ютерну систему, які перевантажують її та позбавляють змоги виконувати

запити користувачів, при цьому DDoS-атаки відрізняються від DoS-атак тим, що вони використовують декілька комп'ютерів (хостів) одночасно, щоб перевантажити цільову систему, що своєю чергою, робить цю атаку більш потужною та складнішою для організації кіберзахисту; 4). Атаки типу "людина посередині" (Man-in-the-Middle (MITM)), коли кібертерористи здійснюють кібератаку, щоб отримати інформацію саме під час з'єднання з мережею Інтернет, тобто відбувається перехоплення та зміна зв'язку між двома сторонами, без їхнього відома, що дозволяє кібертерористам використовувати ці атаки задля отримання конфіденційної інформації, маніпулювання повідомленнями або ініціювати порушення безпеки каналів зв'язку, у тому числі за допомогою такого з'єднання кібертерористи можуть отримати доступ до персональних даних, змінити їх або навіть відправити власні дані від імені користувача, щодо якого здійснювалася атака; 5). Використання кібертерористами SQL-ін'єкцій з метою несанкціонованого доступу до конфіденційних даних (паролів, фінансових або особистих даних); 6). Атаки, подібні до Stuxnet, які спрямовані на виведення з ладу та порушення штатної роботи промислових систем управління, таких як ті, що використовуються на ядерних об'єктах з метою здійснення кібератаки на системи, які забезпечують живучість та стійкість критичної інфраструктури, щоб завдати фізичної шкоди або знищити їх; 7). Експлойти нульового дня (Zero-day exploits) — це метод кібератак, під час якого використовуються невідомі розробникам програмного забезпечення вразливості для отримання несанкціонованого доступу або контролю над системами, при цьому наявні вразливості залишаються невідомими постачальнику програмного забезпечення; 8). Використання методів соціальної інженерії, що включає маніпулювання свідомістю людей для розкриття конфіденційної інформації або виконання дій, які можуть призвести до появи загроз й небезпеки, при цьому кібертерористи можуть видавати себе за довірених осіб або представників благонадійних організацій з метою отримання доступу до конфіденційних даних або систем. Кібертерористи часто використовують комбінацію цих методів для досягнення своїх злочинних цілей, при цьому їхня мотивація може бути досить різноманітною, включаючи політичну, ідеологічну, фінансову основу або просто ініціювання спричинення хаосу й безладів. За таких умов важливого значення набуває впровадження ефективних заходів кібербезпеки, спрямованих на запобігання та протидію кібертерористичним загрозам.

На переконання О. Полякова, до визначальних ознак кібертероризму належать: кібератаки (форми); здійснення в кіберпросторі або з його використанням (просторова дія); організовані хакерські групи та організації (суб'єкти кібертероризму); залякування населення (спосіб); заподіяння шкоди об'єктам критичної інформаційної інфраструктури або міжнародному правопорядку(терористичні цілі) [12, с.235]. І. Білан вважає, що основною ознакою кібертероризму є кібератаки, які здійснюються у кіберпросторі [3, с.67]. Я. Мазур зазначає, що характерною рисою кібертероризму є те, що всі відомі хакерські групи та особи не прагнуть рекламувати свої дані, а діють лише під псевдонімом, при цьому хакера-терориста слід відрізняти від простого хакера, який діє з корисливих чи хуліганських мотивів. На його переконання, одним із способів кібертероризму є політично мотивована атака на інформацію, превентивне залякування суспільства. Другий спосіб кібертероризму – інформаційна атака на комп'ютерну інформацію та системи, пристрої передачі даних, інші компоненти інформаційної інфраструктури, що здійснюється групами або окремими особами, яка надає можливість проникнути в систему, перехопити або придушити контроль над мережевими інформаційними обмінами та досягти інших руйнівних ефектів [10, с. 281-282]. Науковці В. Трофіменко та А. Мішанчук дійшли висновку, що до ознак кібертероризму

відносяться: наявність політичної вмотивованості як обов'язкова складова, що підкреслює його специфіку; на відміну від традиційного тероризму, в якому виконавець у результаті вербування або вживання наркотичних препаратів може не усвідомлювати протиправність своїх дій і всю повноту наслідків, під час кібертероризму атака завжди є усвідомленою, оскільки її реалізація вимагає від суб'єкта тривалої, клопіткої, зосередженої мозкової роботи; формат акту кібертероризму передбачає вчинення кібератак [19, с.97].

Узагальнюючи викладене, до загальноприйнятих типових ознак, які характеризують кібертероризм, відносяться: анонімність, оскільки кібертероризм відрізняється від звичайних методів здійснення тероризму; використанням кібертерористами онлайн-пседонімів або відвідування ними веб-сайтів у якості неідентифікованого "гостя", що значно ускладнює їхню ідентифікацію та визначення справжньої особи того чи іншого терориста; мішенню кібертерористів можуть бути ядерні об'єкти, об'єкти критичної інфраструктури, комп'ютерні мережі національних урядів, міжнародних організацій, підприємств, установ та організацій усіх організаційно-правових форм власності, авіакомпаній, інших перевізників, окремих приватних осіб, що засвідчує чималий перелік величезної кількості посягань і одночасну складність потенційних цілей, що гарантує, що кібертерористи можуть знайти слабкі місця та вразливості для вчинення своїх кібертерористичних атак; кібертероризм може здійснюватися дистанційно, що вимагає значної меншої фізичної та психологічної підготовки, що автоматично виключає ризик смертності, порівняно із звичайними формами тероризму, що значно полегшує терористичним угрупуванням вербування та утримання у своєму штаті вмотивованих хакерів й програмістів. Проте не усі кібератаки можна вважати терористичними, оскільки до переліку таких відносяться лише ті, які здійснюються саме кібертерористами і які спрямовуються на досягнення певного ефекту, при цьому кібертероризм має потенціал впливати безпосередньо на більшу аудиторію людей, ніж традиційні терористичні методи. Будь-яке терористичне угрупування може використовувати кіберпростір для досягнення різних цілей: у першому випадку може відбуватися цілеспрямований терористичний напад а у другому – використання мережі Інтернет для здійснення низки підготовчих дій, пов'язаних з цілями, які воно переслідує, при цьому такі заходи не обов'язково вважаються кібертероризмом, проте можуть призвести до сприяння майбутній (кібер)терористичній поведінці.

В сучасних умовах світовий досвід не оперує прикладами, коли міжнародні терористичні організації намагалися влаштувати потужні кібератаки саме в контексті вчинення актів кібертероризму. Першим відомим актом кібертероризму, який був ідентифікований світовими експертами, стало здійснення екстреміським угрупуванням "Тамільські тигри" на Шрі-Ланці у 1998 році терористичної кібератаки, яка передбачала спрямування понад 800 електронних листів щодня на адресу національного уряду протягом двох тижнів із повідомленням "Ми-Чорні тигри Інтернету, і робимо це, щоб порушити ваш зв'язок". Метою акту кібертероризму стало чинення психологічного тиску та залякування посадових осіб Шрі-Ланки, демонстрація нездатності урядовців припинити таке свавілля. Пропалестинська хакерська група "Nightmare" (активна з 2023 року) здійснювала DDoS-атаки на ключові ізраїльські ресурси, включаючи Тель-Авівську фондову біржу та Перший міжнародний банк, аргументуючи це протидією ізраїльській окупації та необхідністю початку нової ери електронної війни проти єврейської держави.

Останнім часом в США не зафіксовано жодного випадку спроб поширення загроз кібертероризму, оскільки як урядові комп'ютерні системи, так і ті, які перебувають на балансі та в управлінні федеральних відомств оборони й розвідки, повністю ізольовані та автономні від мережі Інтернет, проте системи, якими керують приватні компанії й корпорації залишаються більш вразливими до загроз терористичних кібератак. Тобто ці системи захищені спеціальним "повітряним зазором", оскільки вони не підключені до мережі Інтернет чи будь-якої відкритої комп'ютерної мережі і тому до них не можуть отримати доступ кібертерористи чи хакери. Так, наприклад, Міністерство оборони США захищає чутливі системи, ізолюючи їх від мережі Інтернет та навіть від власної внутрішньої мережі Пентагону. Засекречені комп'ютерні системи ЦРУ також мають повітряний зазор, як і вся ІКТ-система ФБР. Адже після терактів в США 11 вересня 2001 року кібертероризм набув важливого значення у питаннях гарантування національної безпеки.

Загалом переважна більшість кібератак здійснюється саме хакерами, які не мають політичних завдань або ідеологічних цілей й мотивації, не демонструють прагнення та досягення мети спричинити хаос або масові безлади про які, у свою чергу, мріють терористи. Загалом, кібертероризм може мати глибокі негативні наслідки для політичного ландшафту будь-якої держави, призвести до соціальної та політичної нестабільності й напруги. Кібертероризм також може мати значний вплив на політику кількома способами, включаючи зрив виборів, поширення дезінформації, пропаганди тощо. Кібертерористи можуть використовувати мережу Інтернет, соціальні мережі, месенджери для поширення пропаганди та маніпулювання громадською думкою, що може впливати як на політичні події, так і на процес формування державної політики у цій сфері. Якщо метою зловмисників є зрив проведення виборів, цілеспрямовані кібератаки на виборчі системи або відповідну інфраструктуру, то вони можуть порушити процес проведення голосування. Кібертерористи можуть поширювати дезінформацію або пропаганду ідеології тероризму через соціальні мережі та інші онлайн-платформи, щоб вплинути на свідомість громадян та навіть на результати виборів. Своєю чергою, втручання у виборчі системи може підірвати довіру до виборчого процесу, призвести до втрати впевненості в об'єктивності результатів виборів (президенських, парламентських, місцевих). За таких умов для світової спільноти актуальним питанням є необхідність розмежування загроз кібертероризму, саме від кіберзлочинності, хактивізму та кібервійн, які стають його альтернативою.

На підставі аналізу Європолу про ситуацію та сучасні тенденції тероризму в ЄС (EU TE-SAT) 2025 року слід вказати, що терористична загроза для ЄС залишається досить високою, особливо через активізацію ісламістських угруповань та поширення радикалізації. Занепокоєння держав-членів ЄС викликає і джихадистський тероризм і на цьому фоні тенденційне поширення загроз кібертероризму [20]. В Україні проблематика законодавчого забезпечення боротьби з кібертероризмом, особливо в умовах правового режиму воєнного стану, є актуальною та своєчасною. Наша держава з 2014 року залишається об'єктом кіберагресії з боку рф, саме тому протидія кібертероризму є не лише пріоритетом державної політики у сфері забезпечення кібербезпеки, але й елементом міжнародної безпеки [12, с.233]. Держава-агресор залишається одним із 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, що створює реальну загрозу вчинення

актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури [21].

На фоні російської військової агресії радикалізація процесів у суспільно-політичній сфері є одним із чинників посилення потенційних терористичних кіберзагроз. В сучасних умовах радикалізація та підбурювання до вчинення актів насильства через соціальні мережі та відеоплатформи постійно зростають також завдяки зусиллям російських спецслужб та прихільників ідеології "руського миру". Це у свою чергу, вимагає вжиття заходів, спрямованих на своєчасне виявлення, недопущення і припинення, у т.ч. шляхом проведення заходів профілактичного характеру, підготовки та поширення в мережі Інтернет деструктивних інформаційних матеріалів із закликами до вчинення терористичних актів, насильницької зміни чи повалення конституційного ладу, захоплення державної влади, порушення територіальної цілісності, а також, які розпалюють національну, расову чи релігійну ворожнечу, пропагують ідеї расизму, ксенофобії та екстремізму або інші антиконституційні та протиправні діяння тощо.

Слушно вказує В. Котляров, що найбільшою проблемою є відсутність законодавства, у якому було би чітко визначено поняття "кібертероризм", а пріоритетним напрямом у боротьбі з кібертероризмом має стати організація взаємодії між правоохоронними органами та спецслужбами, судовими органами з метою протидії і розслідування злочинів терористичної спрямованості [8, с. 321]. У зв'язку з цим необхідним є прискорення розробки теоретико-правових засад й алгоритмів реагування на кросдоменні загрози терористичного характеру, які поєднують як фізичну, так і кібернетичну складові. Попри війну, Україна робить важливі кроки, спрямовані на розробку та удосконалення національного законодавства, присвяченого боротьбі з кібертероризмом.

Адже наявність чисельних діючих нормативно-правових актів, спрямованих на посилення кіберзахисту державних інформаційних ресурсів, запобігання тероризму, зокрема Правил антитерористичної безпеки [22], закріплення на урядовому рівні оновлених мінімальних вимог до інформаційних, електронних комунікаційних, технологічних систем [23], затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури [24], затвердження Національного плану реагування на кіберіциденти, кібератаки та кіберзагрози [25], Порядку здійснення державного контролю за додержанням вимог законодавства у сфері кіберзахисту [26], на жаль, відсутня уніфікована національна законодавча база з питань боротьби з кібертероризмом. Україна в рамках євроінтеграційного процесу гармонізує національне законодавство у відповідності з актами права ЄС, при цьому особлива увага приділяється питанням боротьби з терористичною діяльністю, у тому числі й з кібертероризмом. У відповідності до представлених висновків Європейської Комісії потребує додаткового нормативного врегулювання превентивна складова боротьби з тероризмом. Окрім того, у положеннях Звіту Європейської Комісії щодо прогресу України в межах Пакета розширення Європейського Союзу 2025 року [27] вказується, що системна боротьба з тероризмом та запобігання радикалізації залишаються важливими завданнями в контексті здійснення євроінтеграційного курсу.

Висновки. Глобального масштабу набуває використання кіберпростору терористичними організаціями, при цьому пріоритетними цілями кібертероризму залишаються об'єкти атомної енергетики, електро- та водопостачання, сфери електронних комунікацій, фінансової і банківської сфери, авіа- та залізничного транспорту, сховищ стратегічних видів сировини, хімічні й біологічні об'єкти тощо. Терористичні акти можуть завдати серйозної шкоди державним інтересам, призвести до

дестабілізації політичного режиму, спровокувати підрив економічної стійкості держави і призвести до загострення соціальних конфліктів. Кібертероризм характеризується використанням новітніх інформаційних технологій і передбачає підбурювання до терору, провокування хаосу, дестабілізації, переслідує політичні або ідеологічні цілі, при цьому вказана ознака відрізняє кібертероризм від звичайних суміжних кримінальних правопорушень, а також від кіберзлочинів та хактивізму. Враховуючи тенденції поширення кібертерористичних загроз у сучасному світі, міжнародна спільнота прагне максимально запобігти використанню Інтернету і соціальних мереж з метою вчинення актів кібертероризму, радикалізації суспільства. З цією метою проводиться системна робота, яка спрямована на удосконалення національного та міжнародного законодавства, передбачається створення організаційно-правових засад задля розробки механізмів швидкого й оперативного видалення терористичного контенту у мережі Інтернет. При цьому, під час розробки ефективних засобів правового захисту в контексті заборони поширення терористичного контенту вимагається обов'язкове дотримання основних прав людини і громадянина, гарантованих як національному так і міжнародному рівнях.

Відповідно до розділу 24 "Юстиція, свобода, безпека" Дорожньої карти з питань верховенства права [28] Україна протягом 2026 -2027 років має розробити та схвалити пріоритети державної політики у сфері боротьби з тероризмом до 2030 року, прискорити імплементацію у національне законодавство положень Регламенту ЄС 2021/784 щодо боротьби з поширенням терористичного контенту в мережі Інтернет [29], створити ефективну національну систему боротьби з тероризмом та радикалізацією відповідно до нормативних вимог у рамках Директиви (ЄС) 2017/541 [30]. У зв'язку з цим доцільним є прискорення розробки законодавчих ініціатив, які мають адаптувати право ЄС до національного законодавства у сфері боротьби з тероризмом з урахуванням його глобального характеру, удосконалити правове регулювання заходів у сфері боротьби з тероризмом та радикалізацією, у тому числі й у кіберпросторі.

В сучасних умовах для України кібертероризм залишається суттєвою небезпекою та актуальною загрозою для національної безпеки. За таких умов набувають актуальності питання уточнення пріоритетів і удосконалення законодавчої бази у сфері боротьби з терористичною та диверсійною діяльністю у частині формування системи протидії кібертероризму та кібердиверсіям в умовах тривалої російської військової агресії проти України та викликів, пов'язаних із сучасним геополітичним становищем України у світі.

ПОДЯКИ: Немає

КОНФЛІКТ ІНТЕРЕСІВ: Немає

Використана література

1. Зінченко О.Г. Політичні проблеми розвитку кібертероризму в міжнародному просторі. *Науковий журнал «Політикус».* 2024. Випуск 4. С.154-160. URL: http://politicus.od.ua/4_2024/25.pdf

2. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: Монографія. Київ: Видавничий дім «АртЕк», 2017. 107 с.

3. Білан І.А. Кібертероризм: інформаційно-правовий аспект. *Інформація і право*. 2023. № 4. С. 64-71.

4. Геращенко О. С. Кібертероризм як фактор загрози національній безпеці України: генеза поняття та шляхи протидії. *Південноукраїнський правничий часопис.* 2016. № 5. С. 39-42.

5. Діордиця І.В. Поняття та зміст кібертероризму. *Прикарпатський юридичний вісник.* 2016. Вип.3 (12). С.61-68.

6. Драгоненко А.О., Федорчак І.В. Проблеми актів кібертероризму в умовах воєнного стану. *Науковий вісник Ужгородського Національного Університету* 2024. Випуск 84. Частина 3. Серія Право. С. 285-290.

7. Когут Ю.І. Кібертероризм (історія, цілі, об'єкти): *Практичний посібник.* – Київ: Консалтингова компанія «СІДКОН», 2023. – 304 с.

8. Котляров В.О. Кібертероризм як загроза міжнародній безпеці. *Український журнал прикладної економіки та техніки.* 2023. № 2. Том 8. С. 314-321.

9. Лисеюк А.М, Свінцицька Т. Розвиток міжнародного співробітництва у сфері кібербезпеки: нормативно-правові засади та перспективи. *Право та інноваційне суспільство.* 2024. № 23. С. 89-95.

10. Мазур Я.П. Кібертероризм як фактор загрози національній безпеці. *Юридичний науковий електронний журнал.* 2024. №10. С. 280-283.

11. Мельник Д.С. Кібертероризм: зміст, форма та перспективні заходи протидії. *Вісник ХНУВС.* 2023. № 3 (102). С. 144-158.

12. Поляков О.М. Міжнародне співробітництво України у сфері боротьби з кібертероризмом. *Інформація і право.* 2025. №4 (55). С. 233-240.

13. Топчій В.В. Кібертероризм в Україні: поняття та запобігання кримінально-правовими та кримінологічними засобами. *Науковий вісник Херсонського державного університету.Серія: «Юридичні науки».* 2015. Вип. 6(3). С. 65–68.

14. Шелковський Р.Р. Міжнародна співпраця в галузі кібербезпеки та захисту інформації після війни. *Трансформація українського суспільства в цифрову еру : матеріали II Всеукраїнської науково-практичної конференції* (м. Одеса, 23 березня 2023 р.) – Одеса: Нац. ун-т «Одес. юрид. акад.», 2023. – С. 112-113.

15. Michael L. Gross, Daphna Canetti, Dana R. Vashdi. Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity.* 2017,Volume 3, Issue 1, P. 49–58. https://doi.org/10.1093/cybsec/tyw018. URL: https://academic.oup.com/cybersecurity/article/3/1/49/2999135?login=false

16. Broeders D, Cristiano F, Weggemans D. Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy. *Studies in Conflict & Terrorism.* 2023. № 46(12). P. 2426–2453. https://doi.org/10.1080/1057610X.2021.1928887. URL: https://www.tandfonline.com/doi/epdf/10.1080/1057610X.2021.1928887?needAccess=true

17. Iftikhar S. Cyberterrorism as a global threat: a review on repercussions and countermeasures. *PeerJ Computer Science*. 2024. №1. P. 1-32. URL: https://peerj.com/articles/cs-1772.pdf

18. Stevens T. Strategic cyberterrorism: Problems of ends, ways and means. *Handbook of Terrorism and Counter Terrorism Post 9/11*. 2022. P. 42-52. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4031628

19. Трофименко В.А., Мішанчук А.В. Кібертероризм: спроба філософсько-правового осмислення. *Вісник Національного юридичного університету імені Ярослава Мудрого.* 2021. Серія. «Філософія, філософія права, політологія, соціологія». № 2 (49). С. 93-104. URL: http://fil.nlu.edu.ua/article/view/229782

20. EU Terrorism Situation & Trend Report (EU TE-SAT) 2025. URL: https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf

21. Стратегія кібербезпеки України: Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

22. Про затвердження Правил антитерористичної безпеки: Постанова Кабінету Міністрів України від 15 жовтня 2024 року № 1172. URL: https://zakon.rada.gov.ua/laws/show/1172-2024-%D0%BF#Text

23. Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем: Постанова Кабінету

Міністрів України від 26 листопада 2025 року № 1531. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text

24. Про затвердження Національного плану захисту та забезпечення безпеки та стійкості критичної інфраструктури від 19 вересня 2023 року № 825. URL: https://www.kmu.gov.ua/npas/pro-zatverdzhennia-natsionalnoho-planu-zakhystu-ta-zabezpechennia-bezpeky-ta-stiikosti-krytychnoi-infrastruktury-i190923-825

25. Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози: Постанова Кабінету Міністрів України від 26 листопада 2025 року № 1533. URL: https://zakon.rada.gov.ua/laws/show/1533-2025-%D0%BF#Text

26. Про затвердження Порядок здійснення державного контролю за додержанням вимог законодавства у сфері кіберзахисту: постанова Кабінету Міністрів України від 17 грудня 2025 року № 1668. URL: https://zakon.rada.gov.ua/laws/show/1668-2025-%D0%BF#Text

27. COMMISSION STAFF WORKING DOCUMENT Ukraine 2025 Report Accompanying the document COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS 2025 Communication on EU enlargement policy. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025SC0759

28. Дорожня карта з питань верховенства права. URL: https://eu-ua.kmu.gov.ua/wp-content/uploads/UA_Dorozhnya_karta_z_pytan_verhovenstva_prava_2.pdf

29. Regulation (EU) 2021/784 of the European Parliament and of the Council of 29.04.2021 on addressing the dissemination of terrorist content online. 17.05.2021. URL: https://eur-lex.europa.eu/eli/reg/2021/784/oj/eng

30. Directive (EU) of the European Parliament and of the Council of 15.03.2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. 31.03.2017. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017L0541

Олександр Павлович Федієнко
здобувач наукового ступеня
народний депутат України
email: fediienko@rada.gov.ua

Oleksandr P. Fedienko
applicant for a scientific degree
people's Deputy of Ukraine
email: fediienko@rada.gov.ua

Рекомендоване цитування: Федієнко О.П. Загрозливі тенденції поширення кібертероризму. *Інформація і право.* № 1(56)/2026. 2026. С. 146-157. https://doi.org/10.37750/2616-6798.2026.1(56).357372.

Suggested Citation: Fedienko O. (2026) Dangerous Trends of Spreading Cyberterrorism. *Information and Law*. 1(56)/2026. 146-157. https://doi.org/10.37750/2616-6798.2026.1(56).357372.

Дата надходження статті до редакції: 11.03.2026 р.
Дата прийняття статті до друку після рецензування: 14.03.2026 р.
Дата публікації (оприлюднення): 01.04.2026 р.

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