

## ЕВОЛЮЦІЯ МІЖНАРОДНО-ПРАВОВОГО РЕГУЛЮВАННЯ БОРОТЬБИ З КІБЕРТЕРОРИЗМОМ

**ОНИЩЕНКО Олег Володимирович - аспірант кафедри міжнародного та європейського права Факультету права та міжнародних відносин Державного некомерційного підприємства «Державний університет «Київський авіаційний інститут»**

**DOI: <https://doi.org/10.71404/EP.2025.3.55>**

У статті досліджується еволюція міжнародно-правових механізмів протидії кібертероризму від перших спроб його концептуального осмислення у 1990-х роках до сучасного етапу цифрової трансформації суспільства. Автор підкреслює, що розвиток інформаційно-комунікаційних технологій, з одного боку, відкрив нові можливості для глобального співробітництва, а з іншого - створив передумови для виникнення нових форм терористичної діяльності, що здійснюється у кіберпросторі.

У цьому контексті кібертероризм розглядається як одна з найнебезпечніших форм транснаціональної злочинності, яка здатна порушити функціонування критичної інфраструктури держав, спричинити масштабні соціально-економічні наслідки та підірвати міжнародну безпеку. У роботі простежується формування понятійного апарату та правових підходів до визначення феномену кібертероризму у міжнародному праві. Зазначається, що відсутність єдиного офіційного визначення цього явища ускладнює ефективну правозастосовну діяльність та створює труднощі у кваліфікації відповідних діянь.

Проаналізовано ключові міжнародні документи, які заклали основи правового регулювання у сфері боротьби з кіберзлочинністю та кібертероризмом, зокрема Конвенцію Ради Європи про кіберзлочинність 2001 року (Будапештську конвенцію), резолюції та доповіді Генеральної Асамблеї і Ради Безпеки ООН, а також регіональні ініціативи Європейського Союзу, НАТО та Співдружності Незалежних Держав. Показано, що саме завдяки цим документам поступово формується міжнародно-правова база, спрямована на забезпечення колективної кібербезпеки та запобігання використанню інформаційних технологій у терористичних цілях.

Окрему увагу приділено питанням уніфікації термінології та розмежуванню понять «кіберзлочинність» і «кібертероризм». Підкреслюється, що

попри тісний зв'язок між цими явищами, вони мають різний правовий характер, об'єкти посягання та рівень суспільної небезпеки. Відсутність чітких дефініцій на міжнародному рівні створює передумови для колізій у національних законодавствах і ускладнює міжнародне співробітництво.

У статті також аналізуються проблеми юрисдикції у кіберпросторі, де територіальні межі держав фактично втрачають своє значення. Автор розглядає сучасні механізми міждержавної взаємодії, зокрема в межах Будапештської конвенції, діяльність спеціалізованих підрозділів Інтерполу та Європолу, а також створення національних і міжнародних центрів реагування на кіберінциденти (CERT/CSIRT). Підкреслюється важливість оперативного обміну інформацією між державами, спільного розслідування кіберінцидентів, узгодження процедур екстрадиції та доказування злочинів, скоєних у цифровому середовищі.

Зроблено висновок, що сучасна система міжнародно-правового регулювання боротьби з кібертероризмом перебуває на стадії активного становлення та потребує подальшого вдосконалення. Необхідною умовою ефективною протидії цьому явищу є вироблення універсальних стандартів безпеки, гармонізація національних законодавств, створення спільних інформаційно-аналітичних платформ та розвиток партнерства між державними структурами, приватним сектором і міжнародними організаціями. Саме консолідація зусиль усіх учасників міжнародного співтовариства дозволить сформувати цілісну систему превенції, реагування та відповідальності у сфері боротьби з кібертероризмом, що відповідає сучасним викликам глобальної безпеки.

Ключові слова: кібертероризм; міжнародне право; кіберзлочинність; Будапештська конвенція; міжнародне співробітництво; кібербезпека; юрисдикція; Організація Об'єднаних Націй; регіональні ініціативи; Інтерпол; Європол; цифровий простір.

### **Постановка проблеми**

Основна проблема полягає у невідповідності між динамічним розвитком кіберзагроз терористичного характеру та статичністю міжнародно-правових механізмів їх регулювання. Незважаючи на існування низки міжнародних документів у сфері кібербезпеки та протидії тероризму, жоден з них не забезпечує комплексного підходу до боротьби з кібертероризмом. Ключові проблемні аспекти включають: відсутність універсального міжнародно-правового визначення кібертероризму; фрагментованість міжнародно-правової бази; конфлікт між національним суверенітетом та необхідністю транскордонного співробітництва; складність атрибуції кібератак та збору доказів; розбіжності у національних законодавствах держав.

**Мета дослідження:** комплексний аналіз еволюції міжнародно-правового регулювання боротьби з кібертероризмом та виявлення тенденцій його подальшого розвитку. **Завданням дослідження** є комплексне вивчення становлення та розвитку міжнародно-правових підходів до боротьби з кібертероризмом, аналіз основних міжнародних і регіональних правових інструментів, що регулюють цю сферу, а також виявлення наявних прогалин і колізій у чинному міжнародно-правовому регулюванні. У роботі передбачається визначення перспективних напрямів удосконалення міжнародного співробітництва та формулювання практичних рекомендацій, спрямованих на підвищення ефективності міжнародно-правових механізмів протидії кібертероризму.

### **Стан опрацювання проблематики**

Проблематика міжнародно-правового регулювання кібертероризму перебуває у фокусі уваги багатьох вчених. Серед зарубіжних дослідників значний внесок зробили М.Н. Шмітт (M. Schmitt) [1], який розробив Таллінський посібник з міжнародного права застосовного до кібервійни, Д. Денінг (D. Denning) [2], що запропонувала одне з перших комплексних визначень кібертероризму, С. Бреннер (S. Brenner) [3], яка досліджувала юрисдикційні аспек-

ти кіберзлочинності. У вітчизняній науці питання кібербезпеки, кіберзлочинності та кібертероризму досліджували В.В. Аніщук [4], В.Л. Гончарук [5], Ю.В. Гурзель [6], С.М. Гусаров, М.І. Саєнко та інші, які аналізували концептуальні засади забезпечення кібербезпеки України. Проте комплексних досліджень еволюції міжнародно-правового регулювання кібертероризму в українській науці бракує, що зумовлює актуальність даного дослідження.

### **Виклад основного матеріалу**

За оцінками експертів, кількість кібератак з ознаками терористичної діяльності демонструє стійку тенденцію до зростання у період з 2015 по 2023 роки, що безпосередньо пов'язано з цифровізацією радикальних рухів, зростанням доступності кіберінструментів і розширенням можливостей для анонімної діяльності в Інтернеті [7]. З появою нових цифрових платформ терористичні угруповання отримали змогу створювати розгалужені мережі підтримки, організовувати фінансування через криптовалюту, проводити навчання та координувати атаки без фізичної присутності учасників. Сучасні терористичні організації активно використовують кіберпростір не лише як канал для пропаганди, вербування нових членів і поширення екстремістських ідеологій, але й як засіб безпосереднього впливу на безпеку держав — шляхом атак на критичну інфраструктуру, інформаційні системи урядових структур, енергетичні об'єкти та транспортні мережі.

У 2023 році терористичний напад Хамасу на Ізраїль 7 жовтня та подальша військова відповідь Ізраїлю в Газі стали не лише руйнівними подіями у військово-політичному сенсі, але й викликали потужну хвилю активності у кіберпросторі. Після початку конфлікту зафіксовано різке зростання кількості кібератак з боку пов'язаних або симпатизуючих угруповань, зокрема хакерських колективів, що атакували державні сайти, медіаресурси та банківські системи. Цей випадок показав, що сучасний тероризм виходить за межі фізичного простору й дедалі більше інтегрується у цифрову сферу, де межа між інформаційною війною та кібертероризмом стає дедалі розмитішою.

Крім того, розвиток штучного інтелекту, машинного навчання та інших технологічних інновацій створює нові ризики у сфері безпеки. Такі інструменти дедалі частіше додаються до арсеналу засобів, які використовують терористи та насильницькі екстремісти для підвищення ефективності своїх інформаційних кампаній, маскування власної діяльності та введення в оману громадськості. Зокрема, великі мовні моделі (LLM) і технології генерації зображень або відео (deepfake) використовуються для створення фальшивих ідентичностей, поширення дезінформації, підроблення офіційних заяв і підсилення пропагандистських повідомлень [8]. Такі технології дозволяють маніпулювати суспільною свідомістю, викликати паніку або недовіру до державних інституцій, що становить серйозну загрозу не лише для інформаційної безпеки, але й для стабільності міжнародного правопорядку.

У 2023 році в семи державах-членах Європейського Союзу було скоєно загалом 120 терористичних атак (98 завершених, 9 невдалих і 13 зірваних), що свідчить про помітне зростання рівня терористичної активності порівняно з попередніми роками. Найбільшу кількість завершених атак — 70 випадків — було скоєно сепаратистськими терористичними угрупованнями, тоді як 23 атаки належали до діяльності лівих та анархістських екстремістів. Особливо небезпечними залишаються джихадистські терористичні напади, серед яких 14 було зареєстровано у 2023 році, з них п'ять — успішно здійснені, що призвело до загибелі шести осіб і поранення дванадцяти. У той самий час два терористичні напади правих екстремістів вдалося попередити завдяки ефективним превентивним заходам правоохоронних органів.

Загалом у 2023 році правоохоронні органи ЄС заарештували 426 підозрюваних у злочинах, пов'язаних із тероризмом (порівняно з 380 у 2022 році), у 22 державах-членах ЄС. Із них 334 арешти стосувалися джихадистського тероризму, що підтверджує тенденцію до домінування цього виду терористичної активності. Крім того, суди держав-членів ЄС винесли 290 обвинувальних вироків і 68 виправдувальних, що свідчить

про стабільне функціонування судово-правових механізмів боротьби з тероризмом у межах європейського простору [8].

Актуальність зазначеної проблеми значно посилюється у контексті поширення кібертероризму, який дедалі частіше поєднується з традиційними формами насильства. Попри наявність численних міжнародних і національних ініціатив, міжнародна спільнота досі не виробила уніфікованого підходу до визначення кібертероризму, його кваліфікації та механізмів протидії. Відсутність загальновизнаної дефініції створює значні труднощі для кримінального переслідування осіб, причетних до таких злочинів, а також для координації діяльності між державами.

Юрисдикційні конфлікти, різний рівень технічної спроможності держав і складність доведення умислу у вчиненні кіберзлочинів створюють правовий вакуум, який активно використовують злочинні угруповання та терористи. До цього додається проблема анонімності кіберпростору, що ускладнює ідентифікацію правопорушників, а також використання децентралізованих технологій, зокрема криптовалют і зашифрованих платформ зв'язку.

Кіберзлочинність сьогодні охоплює широкий спектр протиправних дій, здійснюваних із використанням комп'ютерних систем або спрямованих проти них. Серед основних форм таких дій — несанкціонований доступ до інформаційних ресурсів, викрадення персональних і фінансових даних, злам державних і корпоративних мереж, фінансове шахрайство, шантаж, а також створення й поширення шкідливого програмного забезпечення. На відміну від звичайних кіберзлочинів, кібертероризм характеризується політичними або ідеологічними мотивами, оскільки його метою є не лише отримання матеріальної вигоди, а й дестабілізація державних інституцій, залякування населення та підриг довіри до уряду [9].

Натомість кібертероризм передбачає цілеспрямоване застосування цифрових технологій для залякування населення, тиску на урядові структури або дестабілізації суспільства з метою досягнення політичних, ідеологічних чи релігійних цілей.

Його відмінною рисою є поєднання інформаційно-психологічного впливу з руйнівним технічним потенціалом кіберзасобів. До найпоширеніших проявів кібертероризму належать втручання у функціонування критичної інфраструктури (енергетичної, транспортної, комунікаційної), блокування діяльності урядових установ, поширення терористичної пропаганди, а також координація нападів через онлайн-канали, соціальні мережі чи зашифровані платформи. Такий тип загроз відзначається високим рівнем суспільної небезпеки, оскільки його наслідки можуть виходити далеко за межі окремої держави, і має виразно транснаціональний характер, що ускладнює ідентифікацію та переслідування винних осіб [9].

Попри наявність очевидного зв'язку між кіберзлочинністю та кібертероризмом, відсутність уніфікованих міжнародних визначень цих понять значно ускладнює розроблення узгоджених правових механізмів реагування. Невизначеність термінології спричиняє прогалини у національних законодавствах, нерідко призводить до розбіжностей у кваліфікації правопорушень, а також перешкоджає ефективному міжнародному співробітництву у сфері запобігання, розслідування та покарання за подібні дії. Зокрема, проблеми виникають у питаннях екстрадиції, коли відсутність єдиного визначення складу злочину не дозволяє реалізувати принцип подвійної криміналізації, а також у сфері обміну інформацією та проведення спільних слідчих дій між компетентними органами різних держав.

Уніфікація термінології та гармонізація правових підходів є необхідною умовою для побудови цілісної міжнародної політики протидії загрозам у кіберпросторі. Це, у свою чергу, сприятиме формуванню міжнародно-правових стандартів реагування на кібертероризм, визначенню меж державної юрисдикції в кіберпросторі, а також посиленню ролі міжнародних організацій у координації спільних заходів.

Події останніх років наочно продемонстрували масштаб і глобальність кіберзагроз. Так, кібератаки на енергетичну інфраструктуру України у 2015–2024 роках, що призводили до масштабних відключень

електроенергії, засвідчили здатність кібертерористичних дій впливати на критично важливі системи держави. Атака програмивимагача WannaCry (2017 року) уразила понад 200 тисяч комп'ютерів у більш ніж 150 країнах, що спричинило мільярдні збитки та паралізувало діяльність низки державних і приватних структур. Інцидент із Colonial Pipeline у США (2021 року), який тимчасово зупинив постачання пального на східному узбережжі країни, став показовим прикладом того, як кібернапади можуть безпосередньо впливати на національну безпеку, економіку та добробут населення.

Ці приклади засвідчують, що кібертероризм має глобальний, системний характер, який виходить за межі національних кордонів і потребує скоординованої міжнародної відповіді, заснованої на спільних правових стандартах, обміні інформацією та взаємній довірі між державами [10].

Перші спроби міжнародно-правового врегулювання питань кібербезпеки датуються початком 1990-х років, коли стрімке поширення мережі Інтернет актуалізувало проблему транскордонної комп'ютерної злочинності та необхідність вироблення спільних стандартів її запобігання. Уже в 1990 році на VIII Конгресі ООН з питань запобігання злочинності та поведження з правопорушниками було вперше офіційно порушено питання комп'ютерних злочинів на міжнародному рівні [11]. Це стало відправною точкою для подальшого формування міждержавних механізмів взаємодії у сфері кібербезпеки, зокрема у напрямі гармонізації національного законодавства та обміну інформацією між правоохоронними органами.

Сам термін «кібертероризм» вперше з'явився в академічному дискурсі ще у 1980-х роках, однак його концептуалізація відбулася пізніше — у 1997 році, коли Б. Коллін визначив його як «конвергенцію кіберпростору та тероризму», наголошуючи на новій якості загроз, що поєднують технологічні можливості з ідеологічною мотивацією [12]. Уже через рік, у 1998 році, Федеральне бюро розслідувань США (ФБР) запропонувало одне з перших робочих визначень кібертероризму, під яким розумілося «на-

вмисне, політично вмотивоване здійснення атак проти інформації, комп'ютерних систем, програм і даних, наслідком яких є насильство проти невійськових цілей» [13]. Це визначення фактично окреслило межі між кіберзлочинністю та кібертероризмом, підкресливши політичну спрямованість останнього.

Ключовою віхою у становленні міжнародно-правового режиму кібербезпеки стало прийняття у 2001 році Будапештської конвенції про кіберзлочинність Ради Європи, яка стала першим міжнародним договором, спрямованим на боротьбу зі злочинами, вчиненими з використанням комп'ютерних мереж [14]. Конвенція запровадила уніфіковані стандарти криміналізації основних форм кіберзлочинів (зокрема, несанкціонованого доступу, перехоплення даних, втручання у роботу систем), а також механізми міжнародної співпраці у сфері розслідування, збереження цифрових доказів та екстрадиції осіб, підозрюваних у таких діяннях.

Хоча Будапештська конвенція не охоплювала безпосередньо питання кібертероризму, вона стала правовою основою для формування системи міжнародного співробітництва у боротьбі з кіберзлочинністю, у тому числі з діяннями, що можуть мати терористичний характер. Надалі її положення стали базою для розроблення додаткових протоколів, зокрема щодо посилення відповідальності за расистські та ксенофобські прояви в Інтернеті, що відображає поступову еволюцію міжнародного підходу до кіберзагроз.

Надалі терористичні атаки 11 вересня 2001 року кардинально змінили міжнародний порядок денний у сфері безпеки, спричинивши перегляд підходів до протидії не лише традиційним, але й новим формам тероризму, зокрема тим, що здійснюються у кіберпросторі. У відповідь на ці події Рада Безпеки ООН прийняла резолюцію 1373 (2001), яка зобов'язала всі держави-члени вживати ефективних заходів для запобігання фінансуванню терористичної діяльності, заморожувати фінансові активи осіб, причетних до тероризму, а також посилити міжнародне співробітництво у сфері обміну інформацією та кримінального пересліду-

вання терористів [15]. Хоча у документі не містилося прямих згадок про кібертероризм, його норми стали правовою основою для боротьби з використанням цифрових технологій терористичними угрупованнями, зокрема в аспектах кіберфінансування, вербування та пропаганди.

Подальший розвиток міжнародно-правових механізмів продемонструвала Рада Європи, яка у 2003 році ухвалила Додатковий протокол до Будапештської конвенції про кіберзлочинність, спрямований на криміналізацію розповсюдження расистських і ксенофобських матеріалів через комп'ютерні системи [16]. Протокол закріпив перші міжнародно-правові підходи до боротьби з мовою ненависті в Інтернеті, що стало важливим кроком у запобіганні радикалізації та ідеологічному підґрунті терористичних дій у кіберпросторі.

У 2005 році Організація Об'єднаних Націй ухвалила Міжнародну конвенцію про боротьбу з актами ядерного тероризму, яка передбачає комплекс заходів із захисту ядерних об'єктів і матеріалів, що є складовою критичної інфраструктури держав [17]. Попри те, що конвенція не містить прямих положень про кібербезпеку, її реалізація опосередковано охоплює цифрові аспекти безпеки, адже захист ядерних об'єктів неможливий без протидії потенційним кіберзагрозам, які можуть бути використані для втручання в їхню роботу.

Того ж року, у 2005 році, значного значення набуло прийняття Європейської конвенції про запобігання тероризму, яка запровадила нову криміналізацію – публічне підбурювання до вчинення терористичних актів, у тому числі через Інтернет та електронні засоби комунікації [18]. Цей документ став першим міжнародним актом, який прямо визнав онлайн-активність терористичного характеру складовою терористичних злочинів, створивши прецедент для подальшої імплементації норм про кібертероризм у національні законодавства держав-членів Ради Європи.

Загалом, у першому десятилітті XXI століття міжнародне співтовариство заклало фундамент для сучасного міжнародно-пра-

вового регулювання у сфері кібербезпеки, що поступово розширювався від боротьби з комп'ютерною злочинністю до включення елементів, пов'язаних із терористичною діяльністю у цифровому середовищі.

Початок 2010-х років ознаменувався якісним ускладненням кіберзагроз та усвідомленням їх потенціалу для впливу на національну безпеку. Виявлення у 2010 році комп'ютерного вірусу Stuxnet стало першим задокументованим прикладом цілеспрямованого використання кібератаки проти об'єктів критичної інфраструктури держави, що продемонструвало реальність кібероперацій як інструменту гібридного впливу [19]. Ця подія стимулювала міжнародну спільноту до розроблення нових нормативно-правових механізмів реагування на кіберзагрози.

У 2013 році було опубліковано Таллінський посібник з міжнародного права, застосовного до кібервійни (Tallinn Manual), який став одним із ключових доктринальних джерел, що адаптувало положення міжнародного гуманітарного права до реалій кіберпростору [20]. У 2017 році з'явилася розширена редакція – Tallinn Manual 2.0, яка поширила сферу застосування міжнародно-правових норм на кібероперації, що здійснюються у мирний час, і стала важливим кроком до формування єдиного міжнародно-правового режиму кібербезпеки [21].

Подальший розвиток міжнародно-правових механізмів протидії кіберзагрозам відбувся у другій половині 2010-х років. Рада Безпеки ООН у резолюції 2341 (2017) вперше визнала кібератаки проти критичної інфраструктури потенційною загрозою міжнародному миру та безпеці, закликавши держави-члени вжити ефективних заходів для зміцнення захисту критичної інфраструктури від терористичних дій, зокрема з використанням кіберзасобів [22].

Значущим кроком у розвитку регіональних правових стандартів стало прийняття у 2017 році Директиви (ЄС) 2016/1148 про безпеку мережевих та інформаційних систем (NIS Directive), яка вперше на рівні Європейського Союзу встановила мінімальні вимоги до кіберстійкості операторів критичної інфраструктури та передбачила ме-

ханізми координації між державами-членами у випадку кіберінцидентів [23].

У 2019 році ЄС ухвалив Регламент (ЄС) 2021/784 про запобігання поширенню терористичного контенту онлайн, що зобов'язав цифрові платформи видаляти терористичний контент протягом однієї години з моменту отримання розпорядження компетентного органу, тим самим зміцнивши нормативну базу боротьби з кібертероризмом [24].

Пандемія COVID-19 стала каталізатором глобальної цифрової трансформації, що водночас призвело до суттєвого зростання кіберзагроз. За даними оцінки INTERPOL щодо впливу COVID-19 на кіберзлочинність (серпень 2020 року), кількість зловмисних кіберінцидентів зросла майже на 600 % протягом першого місяця пандемії, а основний вектор атак змістився з фізичних осіб і малих підприємств на великі корпорації, уряди та об'єкти критичної інфраструктури [25]. У цей період терористичні організації почали активніше використовувати криптовалюти для фінансування, децентралізовані платформи для комунікації та технології штучного інтелекту (зокрема глибокого навчання) для створення і поширення дезінформації.

У відповідь на ці тенденції міжнародне співтовариство посилює нормативну базу кібербезпеки. У 2021 році було прийнято Другий додатковий протокол до Будапештської конвенції про кіберзлочинність, який розширив механізми міжнародного співробітництва, передбачив спрощені процедури отримання електронних доказів і посилення гарантій захисту персональних даних [26]. У 2022 році набрала чинності Директива (ЄС) 2022/2555 (NIS2 Directive), що значно розширила перелік суб'єктів, на яких поширюються вимоги щодо забезпечення кіберстійкості, та встановила більш суворі стандарти управління ризиками й реагування на інциденти [27].

Окрім глобальних механізмів, важливе значення у формуванні міжнародно-правових стандартів протидії кіберзагрозам відіграють регіональні організації, які адаптують загальні принципи до специфіки власних безпекових середовищ. Так, Шанхайська організація співробітництва у 2009

році підписала Угоду про співробітництво у сфері забезпечення міжнародної інформаційної безпеки, що стала правовою основою для обміну інформацією, координації дій і спільного реагування на інциденти в кіберпросторі [28]. Африканський союз у 2014 році ухвалив Конвенцію про кібербезпеку та захист персональних даних (Малабську конвенцію), яка закріпила стандарти кіберзахисту, електронної комерції та гарантії приватності на континентальному рівні [29]. Організація американських держав розробила низку документів, зокрема Міжамериканську стратегію кібербезпеки (2004), спрямовану на підвищення спроможності держав-членів у протидії кіберзлочинності [30].

У 2021 році АСЕАН затвердила Регіональний план дій з кібербезпеки, який визначив пріоритети співробітництва в галузі управління кіберінцидентами, розбудови довіри та зміцнення стійкості інформаційних систем [31].

Незважаючи на розвинену нормативну базу, практична реалізація міжнародно-правових норм стикається з численними перешкодами. Головною проблемою залишається відсутність універсального визначення кібертероризму. Різні держави по-різному тлумачать цей феномен, що унеможливує уніфіковану відповідь [32]. Технічна складність атрибуції кібератак створює проблему доказування. На відміну від традиційних злочинів, у кіберпросторі надзвичайно складно встановити справжнього виконавця через використання проксі-серверів, VPN, мереж Tor та інших технологій анонізації [33]. Юрисдикційні конфлікти також ускладнюють боротьбу з кібертероризмом. Транскордонний характер кібератак породжує питання: законодавство якої держави застосовувати, якщо сервер розташований в одній країні, зловмисник діє з іншої, а жертва перебуває у третій? [34]. Проблема цифрового суверенітету посилюється через різне розуміння державами балансу між безпекою та правами людини. Авторитарні режими використовують антитерористичне законодавство для обмеження свободи слова та політичних опонентів [35].

---

## Висновки

Еволюція міжнародно-правового регулювання боротьби з кібертероризмом демонструє поступовий рух від фрагментарних ініціатив до формування комплексної системи норм та інституцій. За три десятиліття міжнародна спільнота пройшла шлях від визнання проблеми до створення багаторівневої архітектури протидії, яка включає універсальні конвенції, регіональні механізми та національні законодавства. Проте аналіз виявив суттєві прогалини у чинному регулюванні. По-перше, відсутність загальноприйнятого визначення кібертероризму перешкоджає уніфікації підходів держав. По-друге, технологічний розвиток випереджає правове регулювання, створюючи нові виклики (штучний інтелект, квантові комп'ютери, метавесвіт). По-третє, геополітична фрагментація призводить до формування конкуруючих нормативних режимів.

Подальший розвиток міжнародно-правового регулювання потребує: розробки універсальної конвенції ООН щодо боротьби саме з кібертероризмом, яка б містила узгоджене визначення термінології, механізми реагування та гарантії дотримання прав людини; створення глобального центру реагування на кіберінциденти під егідою ООН; гармонізації національних законодавств шляхом запровадження типових моделей правового регулювання; розвитку технічних стандартів атрибуції кібератак; забезпечення балансу між заходами безпеки та гарантіями прав людини. Для України, яка безпосередньо стикається з проявами кібертероризму, особливо важливою є активна участь у міжнародних ініціативах, імплементація європейських стандартів та розбудова національних спроможностей у сфері протидії кіберзагрозам.

## Література

1. Michael N. Schmitt and Durward E. Johnson. URL: <https://digital-commons.usnwc.edu/ils/vol97/iss1/15>
2. Denning D.E. Cyberterrorism: The Logic Bomb versus the Truck Bomb. *Global Dialogue*. 2000. Vol. 2, № 4. P. 29-37.

3. Brenner S. W. *Cybercrime Jurisdiction. Crime, Law and Social Change*. 2006. Vol. 46, № 4-5. P. 189-206.
4. Аніщук В.В., Зицик С.Г. Проблема протидії кіберзлочинності: порівняльно-правовий аналіз. *Науковий вісник Ужгородського Національного Університету*. Випуск 83 (3). 2024. С. 19-23. URL: <https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/07/4-2.pdf>
5. Гончарук В.Л. Правові механізми боротьби з кіберзлочинністю: світова практика та вітчизняний контекст. *Питання боротьби зі злочинністю*. Випуск 49. 2025. С. 178-184.
6. Гурзель Ю.В. *Кіберзлочинність: основні причини та методи боротьби. Протидія кіберзагрозам та торгівля людьми*. Харків. 2019. С. 49-51. URL: [https://univd.edu.ua/general/publishing/konf/26\\_11\\_2019/pdf/12.pdf](https://univd.edu.ua/general/publishing/konf/26_11_2019/pdf/12.pdf)
7. Europol. *Internet Organised Crime Threat Assessment (IOCTA) 2023*. The Hague: Europol, 2023. 52 p.
8. Europol TE-SAT 2024. URL: [https://eucrim.eu/news/europol-te-sat-2024/?utm\\_source=chatgpt.com](https://eucrim.eu/news/europol-te-sat-2024/?utm_source=chatgpt.com)
9. Brenner S.W. «At Light Speed»: Attribution and Response to Cybercrime/Terrorism/Warfare. *The Journal of Criminal Law and Criminology*. 2007. Vol. 97, № 2. P. 379-475.
10. Greenberg A. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. New York: Doubleday, 2019. 368 p.
11. UN General Assembly. *Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders*. A/CONF.144/28/Rev.1.1990. URL: [https://www.unodc.org/documents/congress/Previous\\_Congresses/8th\\_Congress\\_1990/028\\_ACONF.144.28.Rev.1\\_Report\\_Eighth\\_United\\_Nations\\_Congress\\_on\\_the\\_Prevention\\_of\\_Crime\\_and\\_the\\_Treatment\\_of\\_Offenders.pdf](https://www.unodc.org/documents/congress/Previous_Congresses/8th_Congress_1990/028_ACONF.144.28.Rev.1_Report_Eighth_United_Nations_Congress_on_the_Prevention_of_Crime_and_the_Treatment_of_Offenders.pdf)
12. Collin B.C. *The Future of CyberTerrorism: Where the Physical and Virtual Worlds Converge*. *Crime and Justice International*. 1997. Vol. 13, № 2. P. 15-18.
13. FBI. *Cyberstalking: A New Challenge for Law Enforcement and Industry*. Washington, D.C.: U.S. Department of Justice, 1999. 24 p.
14. Council of Europe. *Convention on Cybercrime*. Budapest, 23.XI.2001. (European Treaty Series; No. 185). URL: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185>
15. UN Security Council. *Resolution 1373 (2001)*. S/RES/1373. New York: United Nations, 2001. URL: [https://docs.un.org/en/S/RES/1373\(2001\)](https://docs.un.org/en/S/RES/1373(2001)).
16. Council of Europe. *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*. Strasbourg, 28.I.2003. (European Treaty Series; No. 189). URL: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=189>
17. UN General Assembly. *International Convention for the Suppression of Acts of Nuclear Terrorism*. A/RES/59/290. 2005. URL: [https://treaties.un.org/doc/source/RecentTexts/English\\_18\\_15.pdf](https://treaties.un.org/doc/source/RecentTexts/English_18_15.pdf)
18. Council of Europe. *Council of Europe Convention on the Prevention of Terrorism*. Warsaw, 16.V.2005. (European Treaty Series; No. 196). URL: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=196>
19. Langner R. *Stuxnet: Dissecting a Cyberwarfare Weapon*. *IEEE Security & Privacy*. 2011. Vol. 9, № 3. С. 49-51.
20. Schmitt M. N. (Ed.). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013. URL: [https://assets.cambridge.org/9781107024434/frontmatter/9781107024434\\_frontmatter.pdf](https://assets.cambridge.org/9781107024434/frontmatter/9781107024434_frontmatter.pdf)
21. Schmitt M. N. (Ed.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017. URL: <https://www.cambridge.org/core/books/tallinn-manual-20-on-the-international-law-applicable-to-cyber-operations/E4FFD83EA790D7C4C3C28FC9CA2FB6C9>
22. UN Security Council. *Resolution 2341 (2017)*. S/RES/2341. New York: United Nations, 2017. URL: [https://docs.un.org/en/S/RES/2341\(2017\)](https://docs.un.org/en/S/RES/2341(2017)).

23. European Parliament and Council. Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems (NIS Directive). OJ L 194, 19.7.2016. P. 1-30.

24. European Parliament and Council. Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online. OJ L 172, 17.5.2021. P. 79-109.

25. Alarming rate of cyberattacks during COVID-19. URL: <https://www.sbsc.se/en/it-security-is-threatened-by-the-corona-pandemic>

26. Council of Europe. Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. Strasbourg, 12.V.2022. (European Treaty Series; No. 224). URL: <https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatyid=224>

27. European Parliament and Council. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity (NIS2 Directive). OJ L 333, 27.12.2022. P. 80-152. URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>

28. Shanghai Cooperation Organisation. Agreement on Cooperation in the Field of International Information Security. 2009. URL: <https://lawinfochina.com/display.aspx?id=8558&lib=tax&SearchKeyword=&SearchCKeyword=&EncodingName=big5>

29. African Union. African Union Convention on Cyber Security and Personal Data Protection. Malabo, 27.VI.2014. URL: <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>

30. Organization of American States. Comprehensive Inter-American Cybersecurity Strategy. OEA/Ser.G CP/doc.4419/04. 2004. URL: <https://ccdcoe.org/uploads/2018/10/OAS-040608-InterAmericanCyber Security Strategy.pdf>

31. Asean Cybersecurity Cooperation Strategy (2021 – 2025). URL: [https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025\\_final-23-0122.pdf](https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf)

32. Goodman M. Future Crimes: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It. New York: Doubleday, 2015. 464 p.

33. Rid T., Buchanan, B. Attributing Cyber Attacks. Journal of Strategic Studies. 2015. Vol. 38, № 1-2. P. 4-37. URL: <https://ridt.co/d/rid-buchanan-attributing-cyber-attacks.pdf>

34. Svantesson D. J. B. Solving the Internet Jurisdiction Puzzle. Oxford: Oxford University Press, 2017. URL: <https://doi.org/10.1093/oso/9780198795674.001.0001>

35. Polonetsky J., Tene, O. Privacy and Big Data: Making Ends Meet. Stanford Law Review Online. 2013. Vol. 66. P. 25-31. URL: <https://www.stanfordlawreview.org/online/privacy-and-big-data-privacy-and-big-data>

**Oleh Onyshchenko**

*postgraduate student of the Department of International and European Law  
Faculty of Law and International Relations  
State Non-Commercial Company  
«State University «Kyiv Aviation Institute»»*

#### **EVOLUTION OF INTERNATIONAL LEGAL REGULATION OF THE FIGHT AGAINST CYBERTERRORISM**

The article examines the evolution of international legal mechanisms for countering cyberterrorism from the first attempts at conceptual understanding in the 1990s to the current stage of digital transformation of society. The author emphasizes that the development of information and communication technologies, on the one hand, has opened up new opportunities for global cooperation, and on the other hand, has created the conditions for the emergence of new forms of terrorist activity carried out in cyberspace.

In this context, cyberterrorism is considered one of the most dangerous forms of transnational crime, capable of disrupting the functioning of critical state infrastructure, causing large-scale socio-economic consequences, and undermining international security. The paper traces the formation of the conceptual apparatus and legal approaches to defining the phenomenon of cyberterrorism in international law. It notes that the lack of a single official definition of this phenomenon complicates effective law enforcement and creates difficulties in qualifying relevant acts.

Key international documents that laid the foundations for legal regulation in the field of

combating cybercrime and cyberterrorism were analyzed, in particular the 2001 Council of Europe Convention on Cybercrime (Budapest Convention), resolutions and reports of the UN General Assembly and Security Council, as well as regional initiatives of the European Union, NATO, and the Commonwealth of Independent States. It is shown that it is thanks to these documents that an international legal framework is gradually being formed, aimed at ensuring collective cybersecurity and preventing the use of information technologies for terrorist purposes.

Particular attention is paid to the issues of unifying terminology and distinguishing between the concepts of “cybercrime” and “cyberterrorism.” It is emphasized that despite the close connection between these phenomena, they have different legal characteristics, objects of infringement, and levels of public danger. The lack of clear definitions at the international level creates conditions for conflicts in national legislation and complicates international cooperation.

The article also analyzes issues of jurisdiction in cyberspace, where the territorial boundaries of states are effectively losing their significance. The author examines modern mechanisms of intergovernmental cooperation, in particular within the framework of the Budapest Convention, the activities of specialized

units of Interpol and Europol, as well as the creation of national and international cyber incident response centers (CERT/CSIRT). The importance of the rapid exchange of information between states, joint investigation of cyber incidents, coordination of extradition procedures, and proving crimes committed in the digital environment is emphasized.

It is concluded that the current system of international legal regulation of the fight against cyberterrorism is in the process of active development and needs further improvement. A necessary condition for effectively countering this phenomenon is the development of universal security standards, the harmonization of national legislation, the creation of joint information and analytical platforms, and the development of partnerships between government agencies, the private sector, and international organizations. It is the consolidation of the efforts of all members of the international community that will make it possible to form a comprehensive system of prevention, response, and accountability in the fight against cyberterrorism that meets the current challenges of global security.

**Keywords:** cyberterrorism; international law; cybercrime; Budapest Convention; international cooperation; cybersecurity; jurisdiction; United Nations; regional initiatives; Interpol; Europol; digital space.