УДК 354:340.133:340.134

**ОЗЕРЧУК І.М.**, провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0001-7011-0772.

# ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ КІБЕПРОСТОРУ ВІД ДІЯЛЬНОСТІ ТЕРОРИСТИЧНИХ ОРГАНІЗАЦІЙ

***Анотація.*** *Досліджено проблеми забезпечення захисту кібепростору від діяльності терористичних організацій. Розглядаються існуючі у юридичній літературі визначення тероризму у кіберпросторі. Міститься аналіз законодавчих актів у сфері боротьби з тероризмом, серед яких виділяється Стратегія кібербезпеки України, а також Концепція боротьби з тероризмом. Висвітлюються основні тенденції розвитку діяльності міжнародних терористичних організацій з використанням інформаційних технологій, основні завдання яких зводяться до: пропаганди тероризму, у тому числі з використанням мережі Інтернет; вербування та навчання нових членів; отримання інформації про об'єкти можливих терористичних посягань; забезпечення терористичної діяльності; поширення інструктивних матеріалів виготовлення вибухових пристроїв. На підставі аналізу новацій антитерористичного законодавства країн ЄС запропоновані шляхи удосконалення протидії діяльності терористичних організацій у кіберпросторі.*

***Ключові слова:*** *тероризм, терористичні організацій, кіберпростір, кібератака, антитерористичне законодавство.*

***Summary.*** *The problems of ensuring the protection of cyberspace from the activities of terrorist organizations have been studied. The existing definitions of terrorism in cyberspace in the legal literature are considered. There is an analysis of legislative acts in the field of counter-terrorism, among which the Cyber Security Strategy of Ukraine and the Concept of Counter-Terrorism stand out. The article covers main tendencies of development of activity of the international terrorist organizations with use of information technologies, main tasks of which are reduced to: propaganda of terrorism, including with use of the Internet; recruiting and training new members; obtaining information about the objects of possible terrorist attacks; ensuring terrorist activities; distribution of instructional materials for the manufacture of explosive devices. On the basis of the analysis of innovations of the anti-terrorist legislation of the EU countries the ways of improvement of counteraction of activity of the terrorist organizations in cyberspace are offered.*

***Keywords:*** *terrorism, terrorist organizations, cyberspace, cyber attack, antiterrorist legislation.*

***Аннотация.*** *Исследованы проблемы обеспечения защиты киберпространства от деятельности террористических организаций. Рассматриваются существующие в юридической литературе определения терроризма в киберпространстве. Содержится анализ законодательных актов в сфере борьбы с терроризмом, среди которых выделяется Стратегия кибербезопасности Украины, а также Концепция борьбы с терроризмом. Освещаются основные тенденции развития деятельности международных террористических организаций с использованием информационных технологий, основные задачи которых сводятся к: пропаганде терроризма, в том числе с использованием сети Интернет; вербовки и обучения новых членов; получение информации об объектах возможных террористических посягательств; обеспечения террористической деятельности; распространение инструктивных материалов изготовления взрывных устройств. На основании анализа новаций антитеррористического законодательства стран ЕС предложены пути совершенствования противодействия деятельности террористических организаций в киберпространстве.*

***Ключевые слова:*** *терроризм, террористические организации, киберпространство, кибератака, антитеррористическое законодательство.*

**Постановка проблеми**. У Стратегії кібербезпеки України (далі – Стратегія), затвердженій Указом Президента України від 26.08.21 р. № 447, відзначається, що використання кіберпростору терористичними організаціями набуває глобального масштабу. Пріоритетними цілями кібертероризму є об'єкти атомної енергетики, електро- та водопостачання, сфери електронних комунікацій, фінансової та банківської сфери, авіа- та залізничного транспорту, сховищ стратегічних видів сировини, хімічні й біологічні об'єкти тощо. Саме тому використання терористичними організаціями кіберпростору для вчинення актів кібертероризму, фінансової та іншої підтримки терористичної діяльності визначено однією із загроз кібербезпеки України [1].

Російська Федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України [1]. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій.

За таких умов дослідження проблеми забезпечення захисту кібепростору від діяльності терористичних організацій є вкрай необхідним. Зазначене завдання є надзвичайно актуальним в контексті зростання нових викликів і загроз національній безпеці України, пов'язаних зокрема із застосуванням інформаційних технологій.

**Результати аналізу наукових публікацій**. Останнім часом питання протидії кібертероризму досліджували Б.Д. Леонов [2], Серьогін В.С. [3], Нізовцев Ю.Ю. [4], Корченко О.Г. [5], Бутузов В.М. [6], Погорецький М.А. [7], Пилипчук В.Г. та Дзьобань О.П. [8]. Питанню визначення кібербезпеки стосувалася робота Баранова О.А. [9], забезпечення кібербезпеки стало предметом праць Гнатюка С.О. [10], Лук'янчука Р.В. [11], Ткачука Н.А. [12] та ін. Водночас, проблемні питання забезпечення захисту кібепростору від діяльності терористичних організацій залишаються недостатньо дослідженими.

**Метою статті** є удосконалення протидії діяльності терористичних організацій у кіберпросторі з урахуванням антитерористичного законодавства та зарубіжного досвіду боротьби з тероризмом.

**Виклад основного матеріалу.** У юридичній літературі тероризм розглядається як складне, багатовимірне та багаторівневе явище реальної дійсності, яке розглядається в сучасній правовій науці у двох аспектах: 1) як негативне явище дійсності, що становить певну соціальну систему, детермінована взаємодією негативних факторів суспільного життя та відповідних рис особистості терориста; 2) як правову оцінку та відображення цього явища в чинному законодавстві [13, с. 672]. Іноді тероризм визначають як специфічну форму ведення війни, метою якої є не матеріальний Інтернет-ресурс, і не геополітичний інтерес (сфера впливу та ринки збуту), а інтерес інформаційний – механізм соціального управління в суспільстві [14, с. 6]. Останнім часом з'явився новий термін "інформаційний тероризм", під яким пропонується розуміти антисоціальне явище, для якого характерним є умисне застосування інформаційно-психологічного та інформаційно-технічного впливів, спрямованих на маніпуляцію чи залякування населення або заподіяння шкоди інформаційному суспільству чи окремим особам з метою примусити публічну владу, міжнародну організацію, юридичну чи фізичну особу (групу осіб) вчинити якусь дію (або утриматися від її вчинення) в межах інформаціного

простору, пов'язаного з використанням Інтернету, інформаційних технологій і(або) інформаційних ресурсів [15, с. 250].

Окремим різновидом інформаційного тероризму є кібертероризм, який Закон України "Про основні засади забезпечення кібербезпеки України" визначає як терористичну діяльність, що здійснюється в кіберпросторі або з його використанням. Відповідно до ч. 5 ст. 5 цього Закону суб'єкти забезпечення кібербезпеки у межах своєї компетенції здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях [16].

Сучасний тероризм набув суттєвого поширення за допомогою мережі Інтернет. У Концепції боротьби з тероризмом, затвердженій Указом Президента України від 05.03.19 р. № 53, фіксується положення про те, що терористичні загрози, котрі постали перед Україною, вимагають удосконалення функціонування загальнодержавної системи боротьби з тероризмом, яке має здійснюватися з використанням досвіду та найкращих світових практик у сфері боротьби з тероризмом, у тому числі на основі поетапного впровадження положень Глобальної контртерористичної стратегії ООН [17]. Відповідні зусилля повинні спрямовуватися на впровадження дієвих механізмів усунення (локалізації) терористичних ризиків для об'єктів можливих терористичних посягань, що органічно поєднуватимуть політичні, правові, організаційні, інформаційні, соціальні, контррозвідувальні, розвідувальні, оперативно-розшукові, режимні, фінансові й інші заходи [17].

Слід відзначити, що нові тенденції у розвитку тероризму створюють додаткові виклики для національної і міжнародної безпеки і потребують належного реагування. З огляду на це, заходи з удосконалення антитерористичної політики як на національному, так і на міжнародному рівнях мають носити перманентний характер навіть за умов низького рівня відповідної загрози. На даний час, зусилля багатьох країн спрямовані на посилення захисту від терористичної загрози [18].

У червні 2021 року Європол опублікував щорічний звіт про ситуацію з тероризмом та його основні тенденції в країнах Європейського союзу. Автори звіту звернули увагу на той факт, що протягом останніх років кількість здійснених терористичних атак в Європі залишається приблизно на одному рівні. У 2020 році таких атак було зафіксовано 57 в країнах ЄС, 62 – у Великобританії і 2 – в Швейцарії (всього 121). У 2019 р. зафіксовано 119, а у 2018 р. – 129 атак. За останній рік від рук терористів в країнах ЄС загинула 21 людина. При цьому практично всі жертви були обрані випадково [19]. Фіксується також тенденція зниження кількості заарештованих терористів.

Згідно з оприлюдненим Європолом інформаційним звітом усі терористичні атаки були поділені на три основні групи за ідеологічною мотивацією їх виконавців: джихадисти, ультраправі і ультраліві радикали. Відзначається тенденція розширення присутності терористичних та екстремістських груп у віртуальному Інтернет-просторі (у першу чергу в соціальних мережах).

З огляду на активне використання терористичними організаціями Інтернету та соціальних мереж для пропаганди та вербування нових послідовників, планується створення Європейського центру боротьби з тероризмом та радикалізацією в Інтернеті. Він має стати елементом існуючого при Європолі довідкового бюро в мережі Інтернет. При МВС Чехії нещодавно утворено Центр боротьби з тероризмом і гібридними загрозами, діяльність якого зосереджена на аналізі Інтернет контенту і відповідному реагуванні [18].

Інтернет надав додаткові можливості оперативно і скоординовано керувати діями членів терористичних організацій, спілкуватися між собою, поширювати інформацію в режимі реального часу, стимулюючи саморадикалізацію серед потенційних членів радикальних організацій з перспективою їх вербування до терористичних груп [20, с. 76].

Слід погодитися з Леоновим Б.Д., що використання терористами досягнень науково-технічного прогресу, активне використання сучасних інформаційно-комунікаційних технологій, мережі Інтернет з терористичною метою є основною тенденцією поширення терористичної злочинності [20, с. 85].

З використанням сучасних інформаційних технологій, у тому числі мережі Інтернет, міжнародні терористичні організації виконують завдання: 1) пропаганди тероризму (за допомогою великої кількості Інтернет-форумів, онлайн "AQAP", журналу "Inspire" тощо); 2) вербування та навчання нових членів; 3) отримання інформації про об'єкти можливих терористичних посягань; 4) забезпечення терористичної діяльності (планування, зв'язок, збір грошей тощо); 5) демонстрації звітів про результати терористичних актів; 6) поширення інструктивних матеріалів виготовлення вибухових пристроїв [20, с. 76].

Останнім часом спостерігається тенденція зрощування соціальних мереж із ресурсами мобільного зв'язку, що дозволяє розміщати інформацію в соціальних мережах і відслідковувати повідомлення інших абонентів. Це, наприклад, активно використовувалося для загострення протестних акцій у низці арабських країн шляхом поширення дезінформації, провокаційних фото- та відеоматеріалів. Терористичні структури активно використовують медіа-сферу як для звернення до широкої аудиторії, так і для впливу на цільові групи користувачів, тим самим створюючи "свій бренд" і "піар-акції" перед світовою спільнотою [21, с. 43]. Крім цього, слід відзначити, що глобальна електронна мережа сприяла появі багатьох незалежних одна від одної децентралізованих терористичних мереж. На даний час терористичні організації практикують тактику "некерованого супротиву", суть якої зводиться до того, що відповідальність за планування та здійснення терористичної діяльності лягає виключно на децентралізованого виконавця. Тоді як діяльність самої терористичної організації концентрується на складанні інструктивних матеріалів аудіо- та відеозакликів в мережі Інтернет, які допомагають децентралізованим групам не виходити за межі терористичної стратегії, яку виробляють ідеологи та лідери терористичних організацій [21, с. 43].

Активізувалася та перейшла на новий рівень Інтернет-ресурсна база низки терористичних і екстремістських організацій, зокрема "Руху Талібан", "Союзу ісламського джихаду" (СІД), "стамбульські сайти" (//www.sehadetzamani.com; www.sehadetvakti.com). Пропаганда стала більш організованою, активною і агресивнішою, використовуються сучасні методи "промивки мізків" та дезінформація [20, с. 76].

З приводу останнього слід звернути увагу ще на один принциповий момент. Не завжди злочини вчиняються під впливом спілкування у групі. Іноді рішення про вчинення злочину та способи його здійснення навіяні впливом книг, ЗМІ, у тому числі мережі Інтернет.

Потужним інструментом психологічного впливу на прибічників і потенційних терористів-одинаків є публікація терористичними угрупованнями власних електронних журналів, у яких містяться релігійне обґрунтування, рекомендації з підготовки, або прямі заклики до вчинення терактів чи інших насильницьких дій проти конкретних осіб або об'єктів [20, с. 43].

Це нас виводить на проблему терориста-одинака, діяльність якого не пов'язана з міжнародними терористичними організаціями. Тип терориста-одинака, для якого характерна підвищена активність в Інтернеті й відсутність зв'язків з терористичними

організаціями, є відносно новим соціальним феноменом, який дедалі більше привертає увагу правоохоронних органів. Цей тип терористів діє, як правило, під впливом гніву та відчаю, зумовлених пропагандою ідей тероризму, закликів до вчинення певних терористичних дій, висвітлених у друкованих виданнях або в Інтернеті. Особи цієї категорії нерідко є емігрантами або вихідцями з емігрантських родин, які незадоволені політикою країни, де вони перебувають. Зазвичай це спокійні та непомітні люди, які скоюють терористичний акт для того, щоб привернути увагу громадськості до певної події (наприклад, війни в Афганістані) [20, с. 285]. Яскравим прикладом таких актів є напад, який вчинив Андрес Брейвік у Норвегії у липні 2011 року, в результаті якого було вбито 77 людей.

С. Атран, на підставі широких досліджень визначає соціальні характеристики "джихадистів", у тому числі терористів-смертників. Здебільшого це – добре освічена людина, ідеалістично налаштована, політично активна й водночас позбавлена культурного коріння, переважно це молодь із мусульманських і європейських країн. Ці молоди люди, як правило, новоявлені апологети вчення, яке сповідують "радикальні ісламісти". Їхні переконання формуються під впливом історій, у яких демонструється повсюдна соціальна несправедливість та політичні репресії проти мусульман, що поширюються каналами супутникового телебачення та в мережі Інтернет [22, с. 127]. Учений акцентує увагу, що радикалізація молоді відбувається в соціальних мережах: безпосередньо у невеликих групах із числа друзів або в процесі спілкування у віртуальних Інтернет-спільнотах [22, с. 130]. З потенційним смертником ведуть розмову про почесну смерть шляхом знищення "невірних" під час якої навіюється думка про пов'язані з нею надії всього клану, у зв'язку з чим створюється мікросередовище майбутнього смертника. Кінцева мета подібної обробки – добровільне бажання йти на смерть [21, с. 37]. Прояви індивідуального тероризму потребують постійного моніторингу з боку правоохоронних органів.

Використання терористами новітніх інформаційних технологій для вербування нових членів та поширення в мережі Інтернет терористичної ідеології вимагає впровадження нових методів і засобів боротьби з тероризмом. Це зумовлює оновлення антитерористичного законодавства, зміни до якого нещодавно внесені законодавцем низки країн ЄС.

Так, німецьким законодавцем у 2016 р. внесено зміни до Закону "Про Федеральну розвідувальну службу" (BND), якими розширюються повноваження цієї служби. Зокрема, передбачено надання права щодо зняття інформації з телекомунікаційних каналів на території ФРН, у т.ч. й прослуховування громадян країни (до цього BND не мала повноважень здійснювати такі заходи на території країни), зберігати інформацію про користувачів Інтернету та передавати її до партнерських спецслужб [18]. Серед інших додаткових заходів, спрямованих на протидію тероризму в Німеччині, також можна виокремити: надання Відомству із захисту конституції необмеженого доступу до баз даних та архівів організацій зв'язку та обміну інформацією, у т.ч. до клієнтської бази за умови отримання відповідного дозволу від комісії, що забезпечує виконання вимог конституції про таємницю листування, пошти та телефонного спілкування; підвищення спроможностей спецслужб з виявлення та припинення протиправної діяльності у кіберпросторі [18], особлива увага приділятиметься "Даркнету", який активно використовується терористичними угрупованнями.

У 2016 році Парламентом Франції до Кримінального кодексу внесено зміни, якими передбачено встановлення відповідальності за нові види злочинів, зокрема, створення сайтів терористичної спрямованості за межами Франції [18]. Також посилено боротьбу з

відмиванням грошей і фінансуванням тероризму, зокрема, введено заборону на поповнення або використання банківських карт, які не можуть бути пов'язані з ідентифікованим користувачем [18].

7 червня 2016 парламент Угорщини вніс зміни до Конституції та низки законів, що стосуються реагування на терористичні загрози. Конституція відтепер містить положення про можливість оголошення урядом стану терористичної загрози (потребує затвердження парламентом протягом наступних 15 днів). Серед заходів, що можуть запроваджуватись урядом виділяється більш строгий контроль Інтернету і поштового зв'язку. При МВС Угорщини створено Інформаційно-аналітичний центр по боротьбі з тероризмом та злочинністю, основним завданням якого є моніторинг та аналіз даних про загрози національній безпеці [18].

Україна також не стоїть осторонь проблеми забезпечення захисту кіберпростору від діяльності терористичних організацій. Так, у Стратегії одним з важливих пріоритетів забезпечення кібербезпеки України визначено забезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства. Стратегією передбачено, що за допомогою розгалуженої системи індикаторів буде визначатися стан досягнення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Серед цілей Стратегії виділяється посилення спроможності національної системи кібербезпеки для мінімізації загроз кіберзлочинності та кібертероризму (стримування) [1].

Ціль С.2 Стратегії сформульована так: "Ефективна протидія розвідувально-підривній діяльності у кіберпросторі та кібертероризму – Україна забезпечить безперервне здійснення контррозвідувальних заходів з виявлення, попередження та припинення розвідувально-підривної діяльності іноземних держав, актів кібершпигунства та кібертероризму, усунення умов, що їм сприяють, та причин їх виникнення для убезпечення інтересів держави, суспільства і окремих громадян". Для досягнення цілі С.2 Україна забезпечить ефективну протидію розвідувально-підривній діяльності у кіберпросторі та кібертероризму, зокрема, шляхом створення відповідно до схвалених концептуальних засад загальнодержавної системи виявлення кібератак, протидії актам кібертероризму і кібершпигунства щодо об'єктів критичної інформаційної інфраструктури [1].

**Висновки.**

Одним з важливих напрямів антитерористичної діяльності є забезпечення захисту кіберпростору від діяльності терористичних організацій шляхом удосконалення системи виявлення кібератак та проявів кібертероризму.

Важливе значення для України має посилення взаємодії між правоохоронними органами України із відповідними органами та спеціальними службами інших країн з питань протидії кібертероризму.

Оскільки розв'язання проблеми кібретероризму можливе лише на міжнародному рівні, потребує активізації міжнародне співробітництво з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в терористичних цілях.

## Використана література

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України": Указ Президента України від 26.08.21 р. № 447. URL: https://www.president.gov.ua/documents/4472021-40013

2. Леонов Б.Д. Тероризм: інформаційно-правовий вимір. *Інформація і право*. № 2(37)/2021. С. 72-79.

3. Леонов Б.Д., Серьогін В.С. Удосконалення методичного забезпечення експертних досліджень спеціальних програмних засобів у сфері протидії кіберзлочинності. *Інформація і право.* № 4(31)/2019. С. 98-106.

4. Нізовцев Ю.Ю. Судово-експертне дослідження ознак втручання в роботу інформаційно-телекомунікаційних систем шляхом віддалених атак на відмову в обслуговуванні: методичні рекомендації. Київ: Видавничий дім "АртЕк", 2016. 118 с.

5. Корченко О.Г. та ін. Ознаковий принцип формування класифікацій кібератак. *Вісник Східноукраїнського національного університету імені Володимира Даля*. 2010. № 4 (146). Ч. 1. С. 184-193.

6. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій: навч. посіб. / В.М. Бутузов, В.Д. Павловський, Л.П.Скалозуб та ін.; за ред. Б.В. Романюка, Є.Д. Скулиша. Київ, 2011. 404 с.

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

8. Пилипчук В.Г., Дзьобань О.П. Теоретичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації. *Стратегічні пріоритети*. 2011. № 4. С. 12-17.

9. Баранов О.А. Про тлумачення та визначення поняття "кібербезпека". *Правова інформатика.* № 2(42)/2014. С. 54-62.

10. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Безпека інформації*. 2013. Т. 19. № 2. С. 118-129.

11. Лук'янчук Р.В. Державне стратегічне планування у сфері забезпечення кібербезпеки: реалії сьогодення. *Вісник Національної академії державного управління при Президентові України*. *Сер.: Державне управління*. 2016. № 3. С. 131-137.

12. Ткачук Н. Стан та проблемні питання реалізації Стратегії кібербезпеки України. *Інформація і право*. № 1(28)/2019. С. 129-134.

13. Велика українська кримінологічна енциклопедія. У 2 т. Т. 2: М-Я / редкол.: В.В. Сокуренко (голова), О.М. Бандурка (співголова) та ін. ; наук. ред. О.М. Литвинов. Харків: Факт, 2021. 870 с.

14. Рижов І. М. Основи аналізу терогенності соціальних систем: монографія. Київ: Магістр – XXI сторіччя. 2008. 288 с.

15 Енциклопедія соціогуманітарної інформології / ред. проф. К.І. Бєляков. Одеса: Вид. дім "Гельветика", 2021. Т. 2. 432 с.

16. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163–19#Text

17 Концепція боротьби з тероризмом: Указ Президента України від 05.03.19 р. № 53. URL: https://zakon.rada.gov.ua/laws/show/53/2019#Text

18 Іноземний досвід протидії тероризму: висновки для України: аналітична записка. URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/inozemniy-dosvid-protidii-terorizmu-visnovki-dlya-ukraini

19 Новый отчет Европола о терроризме в странах ЕС: поводов для оптимизма по-прежнему нет. URL: https://vot-tak.tv/novosti/24-06-2021-otchet-evropola

20 Леонов Б.Д. Запобігання тероризму: кримінологічний аспект: монографія. Київ: Видавничий дім "АртЕк". 2020. 435 с.

21 Использование современных методов вовлечения лиц в террористическую деятельность: аналитический обзор / автор. кол.: Бондаренко А.Е. и др. ; под общей ред. А.П. Новикова. Москва: "Энциклопедия антитеррора", 2013. 57 с.

22. Aron, R. Paix et guerre entre les nations. Paris: Calmann-Levy, 1962. Pp. 15-19.

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