Інформаційна і національна безпека

УДК 343.96

МЕЛЬНИК Д.С., *кандидат юридичних наук,* старший дослідник,
провідний науковий співробітник НОЦ НА СБ України.
ORCID: https://orcid.org/0000-0002-1497-950X.
ЛЕОНОВ Б.Д., *доктор юридичних наук, професор,*
головний науковий співробітник МНДЦ при РНБО України.
ORCID: https://orcid.org/0000-0002-2488-7377.

ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ ІНФОРМАЦІЙНІЙ ІНФРАСТРУКТУРІ

DOI…

Анотація. *У статті відображені сучасні підходи до визначення змісту інформаційного тероризму та його соціальної і правової природи як загрози національній інформаційній інфраструктурі. Описані типові ознаки інформаційного тероризму. Розкриті основні форми (види) інформаційного тероризму, серед яких виділяється кібертероризм та медіа-тероризм. Проаналізовано національні та міжнародно-правові акти з питань боротьби з інформаційним тероризмом. Запропоновано шляхи удосконалення системи заходів протидії інформаційного тероризму.*

Ключові слова: *інформаційний тероризм, кібертероризм, медіа-тероризм, інформаційний простір, національна інформаційна інфраструктура, заходи протидії.*

Summary*. The article represents the modern approaches to determining the meaning of information terrorism and its social and legal nature as threat to the national information infrastructure. Typical signs of information terrorism are described. The main forms (types) of information terrorism are revealed, among which cyber terrorism and media terrorism stand out. National and international legal acts on combating information terrorism were analyzed. Ways to improve the system of measures to counter information terrorism were proposed.*

Keywords: *information terrorism, cyber terrorism, media terrorism, information space, countermeasures, national information infrastructure.*

Постановка проблеми. Стрімкий розвиток інформаційних технологій, масштаби застосування глобальних комунікаційних мереж та процес розбудови інформаційного суспільства зумовили появу нових загроз в інформаційній сфері, однією з яких наразі є використання нових можливостей в терористичній діяльності, що заподіює шкоду життєво важливим інтересам особи, суспільства і держави [1, с. 72].

Глобальний інфопростір упродовж останніх десятиліть став ареною боротьби між світовими державами-лідерами за отримання переваги у вирішенні проблем і конфліктів. Процеси глобалізації, інтернаціоналізації та прогрес у сфері інформаційних технологій породили нові терористичні та інформаційні загрози національній безпеці, зокрема, виникнення інформаційного тероризму, безпосередньо пов’язаного з рівнем комунікацій у сучасному суспільстві.

Загальна доступність інформаційних технологій значно підвищує ризики інформаційного тероризму, а розвиненість інформаційної інфраструктури суспільства сприяє створенню додаткових ризиків цього виду тероризму [2, с. 163], який в сучасних

© Мельник Д.С., Леонов Б.Д., 2024

умовах набуває надзвичайно деструктивного значення. Тому дослідження феномену інформаційного тероризму є важливим питанням забезпечення безпеки національної інформаційної інфраструктури в контексті інформаційної безпеки.

Результати аналізу наукових публікацій. Інформаційні аспекти тероризму досліджувалися багатьма вітчизняними дослідниками (Р. Банк [3], І. Білан, К. Беляков [4], О. Бойченко, К. Герасименко [2], С. Гнатюк [5], О. Дзьобань [6], Д. Дубов [7], О. Довгань [8], І. Короп [9], В. Кубальський, Л. Лабенко [10], Б. Леонов [1], О. Ончурова [11], А. Митко [12], В. Пилипчук [6], В. Хлань [8], Т. Яцик [13] та ін.), які спробували виокремити інформаційний тероризм в окремий вид та дослідити його зміст. Вагомий внесок у дослідження інформаційного тероризму зробили зарубіжні дослідники – М. Джеральд, В. Тафоя, Б. Хофман та ін. Однак в юридичній літературі та соціальній практиці наявні розбіжності в підходах щодо визначення форм і різновидів інформаційного тероризму. Також відсутній комплексний підхід до протидії інформаційному тероризму як загрозі національній інформаційній інфраструктурі.

Метою статті є внесення пропозицій з удосконалення системи заходів протидії інформаційному тероризму на основі аналізу вироблених зарубіжними і вітчизняними вченими підходів до визначення цього небезпечного явища.

Виклад основного матеріалу. Сучасні високотехнологічні інформаційні терористичні акти здатні викликати системну кризу на місцевому, регіональному і світовому рівнях. Реальна можливість застосування терористами новітніх інформаційних технологій створює передумови до масштабних аварій на виробництві, блокування роботи транспорту, дезорганізації системи державного управління, фінансів, роботи наукових та медичних центрів. В умовах дедалі більшого проникнення інформаційних технологій в системи управління державою та керування технологічними процесами національної інформаційної інфраструктури вони стають дедалі більш вразливими для інформаційних загроз.

Таким чином, політично вмотивована діяльність у кіберпросторі у формі атак на урядові та приватні веб-сайти стає більш поширеною. Дедалі частіше об’єктами атак стають національні інформаційні ресурси фінансових установ, підприємств енергетики і транспорту, органів безпеки й оборони держави, захисту від надзвичайних ситуацій.

Резолюцією Генасамблеї ООН № 53/70 щодо кіберзлочинності, прийнятою у грудні 1998 року, передбачено обов’язок держав-членів ООН інформувати Генерального секретаря ООН про свої погляди і оцінки щодо проблем інформаційної безпеки, визначення основних понять, пов’язаних з інформаційною безпекою і розвитком міжнародних принципів, що поліпшують глобальний інформаційний простір і телекомунікації та допомагають боротися з інформаційним тероризмом [14, с. 16].

Цей обов’язок зобов’язує державу у частині всебічного наукового дослідження соціального феномену інформаційного тероризму.

Однак наразі єдиного тлумачення інформаційного тероризму в науці інформаційного права не існує.

Аналіз зарубіжних джерел свідчить про те, що більшість іноземних дослідників є прихильниками точки зору, відповідно до якої інформаційний тероризм є різновидом терористичної діяльності, пов’язаної з новітніми досягненнями у сфері інформаційних технологій. Так, американський дослідник Тафойа під інформаційним тероризмом пропонує розуміти залякування суспільства шляхом використання новітніх технологій для досягнення політичних, релігійних чи ідеологічних цілей, а також дії, які призводять до відключення, виведення з ладу об’єктів критичної інфраструктури або знищення інформації [15].

Серед вітчизняних дослідників підходи до визначення поняття інформаційного тероризму варіюють від форми деструктивного інформаційно-психологічного впливу на особистість, суспільство і державу [1, с. 78] або використання різних форм і методів тимчасового або незворотного виведення з ладу інформаційної інфраструктури держави або її елементів [16, с. 6] до множини інформаційних війн та інформаційних спецоперацій, пов'язаних із національними або транснаціональними кримінальними структурами та спецслужбами іноземних держав [13, с. 57; 17].

У соціальній практиці домінує підхід, згідно з яким інформаційний тероризм – це прямий свідомий вплив на психіку та свідомість з метою формування необхідних думок і суджень, що певним чином визначають напрям поведінки людей [18].

В найбільш узагальненому розумінні інформаційний тероризм являє собою 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 інформаційного простору, пов'язаного з використанням інформації, інформаційних технологій [3; 19; 20, с. 250].

Залежно від злочинної мети та використання інструментів (засобів) її досягнення інформаційний тероризм поділяють на два види: медіа-тероризм та кібертероризм [20, с. 250].

Медіа-тероризм – зловживання інформаційними системами, мережами, та їхніми компонентами для здійснення терористичної діяльності (пропаганда та поширення ідеології тероризму, створення атмосфери страху в суспільстві, сприяння вчиненню теракту) [20, с. 250]. Засобами здійснення медіа-тероризму є інформаційні агентства, а також друковані медіа, мережі ефірних й кабельних мас-медіа, Інтернет, електронна пошта, спам тощо [3, с. 114].

Під кібертероризмом слід розуміти суспільно небезпечну діяльність, яка полягає у вчиненні за допомогою комп'ютерних та електронних комунікаційних засобів навмисних, політично мотивованих атак на комп'ютерні системи/мережі, на інформацію, що обробляється (циркулює) в них, якщо вони викликають порушення роботи критичної інфраструктури держави та створюють (можуть створювати) небезпеку для життя й здоров'я людей, завдали чи можуть завдати значної шкоди матеріальним об'єктам, або спричинили інші тяжкі наслідки, й були вчинені з метою привернення максимально можливої уваги до політичних вимог терористів або використання кіберпростору для інших цілей терористичної діяльності, безпосередньо не пов'язаних зі здійсненням терактів [21, с. 153].

На жаль, вироблені вітчизняними і зарубіжними вченими підходи до визначення інформаційного тероризму, його ознак та видів не були враховані українським законодавцем під час формування законодавчої бази у сфері боротьби з тероризмом. Наразі вітчизняне законодавство не містить визначення інформаційного тероризму та похідних від нього понять. Закон України "Про основні засади забезпечення кібербезпеки України" у п/п. 13 ст. 1 містить визначення лише одного з різновидів інформаційного тероризму – кібертероризму як терористичної діяльності, що відбувається у кіберпросторі або здійснюється з його використанням [22].

Концепція боротьби з тероризмом в Україні, затверджена Указом Президента України від 05.03.19 р. № 53/2019, взагалі не використовує термін "інформаційний тероризм" та відповідно не передбачає заходів з протидії йому.

Варто звернути увагу, що визначення інформаційного тероризму не містять й міжнародні правові акти, серед яких варто виділити Конвенцію Ради Європи про запобігання тероризму (2005 р.), Конвенцію про кіберзлочинність (2001 р.), Стратегією Ради Європи щодо боротьби з тероризмом на 2023 – 2027 роки (2023 р.).

Водночас, у листопаді 2016 року Європарламент ухвалив резолюцію "Стратегічні комунікації ЄС як протидія пропаганді третіх сторін", в якій йдеться про те, що пропаганда є частиною "гібридної війни", що спрямована на "спотворення правди, сіяння сумнівів й ворожнечі між країнами Союзу". Серед джерел пропаганди, яким, згідно з резолюцією, має протистояти ЄС, названі терористичні організації "Аль-Каїда" та "Ісламська держава" [23].

На переконання експертів з міжнародної безпеки, напад терористичної групи "ХАМАС" на Ізраїль 07 жовтня 2023 р., з одного боку, є очевидним актом агресії, а з іншого боку – ця атака містила всі елементи гібридного інструментарію, який активно використовує Росія у війні проти України. Таким чином "ХАМАС" і його ключовий союзник Іран долучилися до поширення гібридної агресії на Близькому Сході [24] .

У свою чергу, Резолюція Генасамблеї ООН від 26 червня 2018 року A/RES/72/284 відзначила факти широкого використання в умовах глобалізованого суспільства терористами та їх пособниками новітніх інформаційно-комунікаційних технологій (Інтернет, соціальні мережі тощо) для вчинення терактів, вербування виконавців, планування та/або фінансування терактів чи підбурювання до них, пошуку однодумців та підтримки співчуваючих.

Зростання зловживань новітніми інформаційними технологіями (електронні комунікації, соцмережі, медіа-платформи, цифрові фінансові інструменти, засоби анонімізації тощо) для терористичних цілей відзначає й Стратегія Ради Європи щодо боротьби з тероризмом на 2023 – 2027 роки [25].

Найбільш небезпечними визнаються прояви кібертероризму. Такі прояви фахівці поділяють на такі групи: 1) реалізація терористичних актів у кіберпросторі, компоненти якого фактично стають інструментом вчинення протиправних дій; 2) використання компонентів кіберпростору як предмету злочинних посягань; 3) використання кіберпростору для досягнення суміжних або проміжних цілей терористичної діяльності [5, с. 122].

Водночас найбільш оптимальним видається групування, яке дозволяє виділити дві основні найбільш небезпечні форми кібертероризму [26, с. 78-80]:

1) вчинення терактів організаціями, групами й окремими особами за допомогою комп'ютерів чи комп'ютерних мереж або шляхом впливу на інформацію, яка в них обробляється (циркулює), – виведення з ладу інформаційно-комунікаційних систем (далі – ІКС) управління державою, об'єктів критичної інфраструктури (далі – ОКІ), спричинення інших надзвичайних подій шляхом втручання в роботу програмного забезпечення ІКС зазначених об'єктів, у т.ч. з використанням комп'ютерних вірусів. Ця форма кібертероризму полягає у використанні комп'ютерних мережевих інструментів для несанкціонованого впливу на припинення роботи національних критичних інфраструктур (енергетика, логістичні перевезення, фінансові платежі, урядові операції тощо) та/або примушування чи залякування урядів або цивільного населення;

2) використання можливостей кіберпростору терористичними організаціями, групами й окремими терористами для інших цілей, не пов'язаних з безпосереднім вчиненням терактів, однак спрямованих на забезпечення терористичної діяльності (координація й планування протиправної діяльності; збір необхідної інформації;

використання як засобу зв'язку зі своїми членами та однодумцями; збирання коштів для фінансування терористичних рухів; вербування нових членів тощо).

Передумовою для існування й подальшого розвитку явища кібертероризму є зростаюча залежність національної інформаційної інфраструктури від автоматизованих систем (далі – АС) управління ОКІ. Новітні інформаційно-комунікаційні технології широко застосовуються терористами для порушення штатних режимів роботи АС управління технологічними процесами на ОКІ поряд з традиційними способами вчинення терактів.

Такий стан справ знижує ефективність виконання уповноваженими суб'єктами безпекових завдань, перешкоджає забезпеченню ефективного захисту ОКІ, що суттєво підвищує небезпечність відповідних загроз національній інформаційній інфраструктурі.

Для вчинення актів кібертертероризму можуть бути використані різні способи протиправної діяльності у кіберпросторі [21, с. 151]:

- отримання несанкціонованого доступу до відомостей, що становлять державну, військову або банківську таємницю, персональні дані тощо;
- завдання збитків окремим елементам інформаційної інфраструктури ОКІ – руйнування мереж зв'язку та енергоживлення, блокування їх роботи, використання шкідливих програм для руйнування програмно-апаратних засобів тощо;
- викрадення або знищення інформації, програмного забезпечення і ресурсів шляхом подолання захисту, впровадження шкідливих програм;
- шкідливий вплив на роботу програмного забезпечення та інформацію, що обробляється (циркулює);
- оприлюднення та погроза опублікувати інформацію з обмеженим доступом;
- захоплення медіа-каналів з метою поширення дезінформації та чуток, демонстрації потужності терористичної організації та оголошення вимог;
- знищення або активне придушення систем і мереж зв'язку, перевантаження комунікаційних вузлів, невірна адресація;
- здійснення інформаційно-психологічних акцій і операцій тощо.

Сучасні терористи переважно завдають асиметричних ударів, коли стратегічні цілі досягаються звичайними засобами, без використання високотехнологічної зброї. Однак їх технічні можливості постійно підвищуються: вони використовують все більш доступні для широкого загалу супутниковий зв'язок, сучасні засоби підробки документів, новітні інформаційні технології, нарощують свою присутність та активність у кіберпросторі для вербування нових членів, підтримання комунікації з осередками (у т.ч. через "Darknet" та з використанням новітніх методів шифрування), надання послідовникам інструкцій з підготовки та вчинення терористичних атак, іншої протиправної діяльності у кіберпросторі [27, с. 6].

Бажаючи звернути увагу керівників нашої держави на зростання загрози кібертероризму, науковці справедливо відзначають, що терористів можуть зацікавити об'єкти національної інформаційної інфраструктури, де використовуються інформаційно-комунікаційні технології: АС управління та Data-центри урядових установ, військові та медичні центри управління, АС управління реакторами АЕС, сховищ радіоактивних матеріалів, нафто- й газопроводів, систем водопостачання й розподілу електроенергії, космічні супутники, транспортні вузли, оборонні та хімічні заводи і бактеріологічні лабораторії [28, с. 319-320]. У разі реалізації цих злочинних намірів терористи можуть завдати значної шкоди національній безпеці України.

Глобальна контртерористична стратегія ООН 2006 року передбачає, що держави-члени співпрацюють у сфері боротьби з тероризмом у всіх його формах і проявах у мережі Інтернет, у т.ч. шляхом використання можливостей глобальної мережі як інструмента боротьби з поширенням тероризму [29]. Стратегія відзначає зростаючу небезпеку інформаційного тероризму на міжнародному і регіональному рівнях.

Україна ратифікувала цю стратегію і тривалий час здійснює взаємодію з міжнародними контртерористичними інституціями у сфері боротьби з інформаційним та іншими формами тероризму, що дає змогу враховувати досвід законодавчого та організаційного забезпечення й функціонування зарубіжних систем протидії інформаційному тероризму.

В ЄС найефективнішим у довгостроковій перспективі заходом протидії інформаційному тероризму експерти вважають боротьбу з пропагандою радикального ісламу. Насамперед, мається на увазі блокування акаунтів пропагандистів тероризму в соцмережах, введення кримінальної відповідальності за пропаганду тероризму в мережі Інтернет, посилення контролю за діяльністю мечетей (насамперед салафітських) і спроби виведення їх із-під контролю Саудівської Аравії, а також посилення Інтернет-контролю за діяльністю ісламських організацій [30, с. 93].

Висновки.

Враховуючи викладене, закономірним є висновок про те, що явище інформаційного тероризму в сучасних умовах є реальною загрозою національній безпеці багатьох держав світу. Зокрема, інформаційний тероризм загрожує непередбачуваними наслідками з точки зору руйнування ОКІ – систем управління й життєзабезпечення сучасних держави і суспільства. Такий висновок узгоджується з положеннями Стратегії національної безпеки України (Указ Президента України від 14.09.20 р. № 392), Стратегії кібербезпеки України (Указ Президента України від 26.08.21 р. № 447) та Стратегії забезпечення державної безпеки (Указ Президента України від 16.02.22 р. № 56).

Комплексний характер загроз національній безпеці, пов’язаних з явищем інформаційного тероризму, потребує визначення інноваційних підходів до формування системи кібербезпеки ОКІ та подальшого розвитку інформаційного простору в умовах глобалізації й вільного обігу інформації.

Однак наразі ані в Україні, ані в світі досі немає комплексного акта з питань боротьби з інформаційним тероризмом, спрямованого на запобігання і припинення використання інформаційних та електронних комунікаційних технологій терористами.

Тому для покращення протидії інформаційному тероризму вважається за доцільне вжити на державному рівні таких заходів [21, с. 154-155; 31, с. 114]:

1) ***законодавчих:***

– необхідно спираючись на міжнародний досвід уніфікувати вітчизняне законодавство у сфері боротьби з інформаційним тероризмом та внести зміни до профільного закону, визначивши поняття інформаційного тероризму у ст. 1 Закону України “Про боротьбу з тероризмом”;

– внести зміни до розділу XVI Особливої частини КК України в частині його доповнення новою нормою про відповідальність за кібертероризм;

– вдосконалити нормативно-правове регулювання порядку залучення правоохоронних органів до діяльності із запобігання, виявлення і припинення актів інформаційного тероризму;

2) ***організаційних*** – спрямованих на удосконалення національної системи протидії тероризму в інформаційній сфері:

– запровадити єдину державну систему протидії інформаційному тероризмому, визначивши чіткі завдання для уповноважених на це державних органів (за умови координації з боку АТЦ Служби безпеки України).

– гарантувати кіберстійкість та кібербезпеку національної інформаційної інфраструктури в умовах цифрової трансформації України;

– впровадити універсальну систему індикаторів кіберзагроз, засновану на міжнародних стандартах з питань кібербезпеки та кіберзахисту;

– упровадити ризик-орієнтований підхід щодо забезпечення інформаційної та кібербезпеки ОКІ, розробити методику ідентифікації та оцінки кіберризиків для національної інформаційної інфраструктури держави;

– поглибити державно-приватну взаємодію у запобіганні кібератакам та кіберінцидентам на ОКІ, реагуванні на них, усуненні їх наслідків в умовах кризових ситуацій, надзвичайного і воєнного стану;

3) ***режимних, контррозвідувальних та оперативно-розшукових***, спрямованих на зниження інформаційних загроз терористичного характеру:

– посилити моніторинг контенту мережі Інтернет (соціальні мережі, блоги, форуми та сервіси) та упровадити у практику новітні технологічні рішення, що надають доступ до інформації, що циркулює в мережі;

– удосконалити наявну систему контррозвідувального забезпечення інформаційної безпеки держави, насамперед в частині протидії інформаційному тероризму;

– забезпечувати постійне виявлення, запобігання і припинення актів інформаційного тероризму, усунення їх причин і умов;

– запровадити загальнодержавну систему виявлення й нейтралізації кібератак, протидії проявам інформаційного тероризму на ОКІ;

– упровадити в систему оперативних пошукових заходів можливостей використання штучного інтелекту, нейромереж, Інтернету речей для ідентифікації й відстеження осіб, технічних засобів, причетних до вчинення протиправних дій, покращення розкриття терористичних актів або підготовки до них [24];

– нарощувати спроможності уповноважених органів у проведенні негласних перевірок стану готовності ОКІ до кібератак/кіберінцидентів;

– покращувати взаємодію уповноважених державних органів (СБУ, НПУ, Держспецзв'язку) між собою та з відповідними компетентними органами іноземних держав, співпрацю з міжнародними організаціями, що протидіють тероризму в усіх його проявах (насамперед, з Інтерполом та Європолом);

4) ***контрпропаганда і стратегічні комунікації з суспільством.*** Необхідно запровадити практику публічного роз'яснення громадськості загроз і небезпек, які несе в собі інформаційний тероризм, а також основних заходів протидії цьому негативному явищу (обов'язково із зазначенням позитивних результатів), залучення на добровільній основі до таких заходів представників громадськості та медіа-середовища.

Поширення кіберзагроз на усі сфери національної інформаційної інфраструктури та постійне вдосконалення інструментів їх реалізації зумовлюють необхідність зміни підходів у протидії інформаційному тероризму під час повномасштабної військової агресії РФ проти України.

Використана література

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

2. Герасименко К. С. Сучасні ознаки загроз "інформаційного тероризму". *Форум права.* 2009. № 3. С. 162-166. URL: http://www.nbuv.gov.ua/e-journals/FP/2009-3/09gkczit.pdf (дата звернення: 04.08.2024).

3. Банк Р.О. Інформаційний тероризм як загроза національній безпеці України: теоретико-правовий аспект. *Інформація і право.* № 1(16)/2016. С. 110-116.

4. Беляков К.І, Цимбалюк В.С. Інформаційні технології як чинник терористичного акту. *Боротьба з організованою злочинністю і корупцією (теорія і практика).*2003. № 8. С. 90-97.

5. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Ukrainian Scientific Journal of Information Security.* 2013. № 2 (19). С. 118-129.

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

7. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва: монографія. Київ: НІСД, 2014. 328 с.

8. Довгань О.Д., Хлань В.Г. Кібертероризм як загроза інформаційному суверенітету держави. *Інформаційна безпека людини, суспільства, держави*. 2011. № 3 (7). С. 49-53.

9. Короп І.В. Інформаційний тероризм. *Альманах міжнародного права.* 2017. Вип. 18. С. 96-102.

10. Лабенко Л. В. Інформаційний тероризм: поняття та ознаки. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/3439/%D0%9B%D0%B0%D0%B1%D0%B5%D0%BD%D0%BA%D0%BE.pdf?sequence=1&isAllowed=y (дата звернення: 04.08.2024).

11. Бойченко О.В., Ончурова О.О. Кібертероризм у складі сучасних проблем національної безпеки. *Форум права*. 2010. № 2. С. 57-62.

12. Митко А.М., Кольцова І.І. Інформаційний тероризм як інструмент впливу на інформаційний конформізм в глобальному середовищі. *Політичне життя*. *Східноєвропейський національний університет імені Лесі Українки*. 2018. № 2. С. 135-139.

13. Яцик Т.П. Особливості інформаційного тероризму як одного із способів інформаційної війни. *Науковий вісник Національного університету ДПС України (економіка, право).* 2014. № 2(65). С. 55-60.

14. Катренко А. Особливості інформаційної безпеки за міжнародними стандартами. *Альманах економічної безпеки*. 1999. № 2. С. 15-17.

15. Tafoya W.L. Cyber Terror. *FBI Law Enforcement Bulletin.* 2011. URL: http://www.fbi.gov/stats-services/publications/law-enforcementbulletin/november-2011/cyber-terror (дата звернення: 04.08.2024).

16. Коршунов В.О. Політичний тероризм: інформаційні методи боротьби: автореф. дис. …канд. політ. наук: спец. 23.00.02. Дніпропетровськ, 2008. 18 с.

17. Брижко В.М., Швець М.Я. е-боротьба в інформаційних війнах та інформаційне право: монографія ; за ред. М. Швеця. Київ: НДЦПІ АПрН України, 2007 р. 236 с.

18. Інформаційний тероризм. Центр протидії дезінформації при РНБО України. URL: https://web.archive.org/web/20220412094834/https://cpd.gov.ua/announcement (дата звернення: 27.08.2024).

19. Бєляков К. І. Антитерористичне законодавство України: інновації 2013. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2013. № (2)30. С. 117-125.

20. Леонов Б.Д. Інформаційний тероризм. Енциклопедія соціогуманітарної інформології / коорд. проекту та заг. ред. проф. К.І. Бєляков. Одеса: Видавничий дім "Гельветика", 2021. Т. 2. С. 249-252.

21. Мельник Д.С. Кібертероризм: поняття, форми прояву, перспективні заходи протидії. *Вісник Харківського національного університету внутрішніх справ.* Харків, 2023. № 3(102). С. 144-158.

22. 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

23. Європейський парламент ухвалив резолюцію щодо протидії російській пропаганді. – (23.11.2016р.). URL: http://glavcom.ua/news/jevropeyskiy-parlament-uhvaliv-rezolyuciyushchodo-protidiji-rosiyskiy-propagandi-384228.html (дата звернення: 04.08.2024).

24. Єрохіна Т. Ризик терористичних атак у Європі: як ескалація в Секторі Гази загрожує міжнародній безпеці. – (06.12.2023 р.). URL: https://www.rfi.fr/uk (дата звернення: 04.02.2024).

25. Council of Europe Counter-Terrorism Strategy (2023-2027). URL: https://search.coe.int/cм#{%22CoEIdentifier%22:[%220900001680a9ad67%22],%22sort%22:[%22CoEValidationDate%20Descending%22]} (дата звернення: 04.08.2024).

26. Тропина Т.Л. Киберпреступность и кибертерроризм. *Компьютерная преступность и кибертерроризм*. 2004. Вып. 1. С. 76-81.

27. Резнікова О.О., Місюра А.О., Войтовський К.Є. Міжнародний тероризм: загрози для України: аналітична записка. Київ: НІСД. 2018. 32с.

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

29. Глобальна контртерористична стратегія ООН. URL: https://www.un.org/counterterrorism/ctitf/ru/un-globalcounter-terrorism-strategy (дата звернення: 04.08.2024).

30. Жайворонок О.І. Міжнародний досвід протидії інформаційному тероризму та його імплементація в Україні. *Публічне управління та митне адміністрування*. 2020. № 1 (24). С. 91-96.

31. Мельник Д.С. Щодо актуальних потреб захисту національної критичної інформаційної інфраструктури України*:* матеріали IX Всеукр. наук.-практ. конф. *Актуальні проблеми управління інформаційною безпекою держави,* м. Київ, 30 берез. 2018 р. – (МОН України, Ін-т модерн. змісту освіти, М-во інформ. політики України, Нац. акад. СБУ, НДІ інформатики і права НАПрН України). Київ: Нац. акад. СБУ, 2018. С. 114-116.

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