

Інформаційна і національна безпека

УДК 32.019.51:323.28:323.2(477)

ЛЕОНОВ Б.Д., доктор юридичних наук, старший науковий співробітник, головний науковий співробітник (наукової установи) Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: <https://orcid.org/0000-0002-2488-7377>.

ТЕРОРИЗМ: ІНФОРМАЦІЙНО-ПРАВОВИЙ ВИМІР

Анотація. У статті висвітлені теоретико-правові аспекти інформаційного тероризму. Наведено класифікацію видів інформаційного тероризму в інформаційному просторі. Міститься аналіз нормативних актів України у сфері інформаційної безпеки. Запропоновано визначення інформаційного тероризму.

Ключові слова: тероризм, інформаційний тероризм, інформаційні технології, інформаційне насильство, кібертероризм.

Summary. The article highlights the theoretical and legal aspects of information terrorism. The classification of types of information terrorism in the information space is given. The analysis of regulatory acts of Ukraine in the field of information security is provided. The definition of information terrorism is offered.

Keywords: terrorism, information terrorism, information technologies, information violence, cyberterrorism.

Аннотация. В статье освещены теоретико-правовые аспекты информационного терроризма. Приведена классификация видов информационного терроризма в информационном пространстве. Содержится анализ нормативно-правовых актов в области информационной безопасности. Предложено определение информационного терроризма.

Ключевые слова: терроризм, информационный терроризм, информационные технологии, информационное насилие, кибертерроризм.

Постановка проблеми. Стрімкий розвиток інформаційних технологій, масштаб застосування глобальних телекомунікаційних мереж та процес побудови інформаційного суспільства обумовили виникнення нових загроз в інформаційній сфері, однією з яких на часі є використання виникаючих можливостей в терористичній діяльності, що заподіює шкоду життєво важливим інтересам особи, суспільства і держави. Рівень загрози інформаційного тероризму стрімко зростає в сучасних умовах глобалізації та набуває надзвичайно деструктивного значення. Особливу загрозу світовим інформаційним системам складає поєднання технологічного та наукового потенціалу провідних країн світу. Високотехнологічні терористичні акції здатні продукувати системну кризу для всієї світової спільноти. Україна, перебуваючи у стані гібридної війни, зазнає негативного інформаційного впливу, наслідки якого сьогодні гостро відчуються у суспільстві.

Результати аналізу наукових публікацій. Теоретичні аспекти протидії інформаційному тероризму досліджували Лабенко Л.В. [1], Бураєва Л.А. [2], Банк Р.О. [3], Пилипчук В.Г., Дзьобань О.П. [4] та ін. Особливості інформаційного тероризму як одного із засобів інформаційної війни, а також види та застосування інформаційної

зброї висвітлені у працях Почепцова Г.Г. [5], Брижка В.М. [6], Коршунова В.О. [7], Ришова І.М. [8], Яцик Т.П. [9] та ін. Серед зарубіжних теоретиків і практиків, які займалися дослідженням інформаційного тероризму як засобу введення інформаційної війни в умовах глобалізації та розвитку кіберпростору, слід зазначити Д. Белла [10], Ж. Бодрійара [11], Е. Тоффлера [12], Б. Хофмана [13], А. Шміда [14] та ін. Міжнародно-правові та кримінально-правові аспекти протидії інформаційному тероризму висвітлені в працях Ковлагіна Д.А. [15], Настюка В.Я., Трофімова С.А. [16], Молчанова М.А., Матевосової Є.К. [16].

Водночас, серед науковців відсутні єдині підходи до визначення поняття “інформаційний тероризм”. Існують також розбіжності поглядів щодо форм і різновидів інформаційного тероризму.

Метою статті є удосконалення визначення інформаційного тероризму з урахуванням підходів, вироблених вітчизняними і зарубіжними вченими.

Виклад основного матеріалу. Законодавство України не містить визначення інформаційного тероризму. Закон України “Про боротьбу з тероризмом” згадує поняття “технологічний тероризм”, під яким слід розуміти кримінальні правопорушення, що вчиняються з терористичною метою із застосуванням ядерної, хімічної, бактеріологічної (біологічної) та іншої зброї масового ураження або її компонентів, інших шкідливих для здоров'я людей речовин, засобів електромагнітної дії, комп'ютерних систем та комунікаційних мереж, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру (ст. 1) [18]. Наведене визначення не збігається з дефініцією інформаційного тероризму, яке є ширшим за змістом.

Закон України “Про основні засади забезпечення кібербезпеки України” містить визначення “кібертероризму” [19], який можна визнати лише одним з різновидів інформаційного тероризму, про що мова буде іти далі.

Доктрина інформаційної безпеки [20] визначає лише актуальні загрози та пріоритети державної політики в інформаційній сфері. З-поміж загроз згадуються спеціальні інформаційні операції, інформаційна експансія, інформаційне домінування, зміст яких лише частково охоплює поняття інформаційного тероризму.

Стратегія національної безпеки України [21] основним завданням розвитку системи кібербезпеки визначає гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації (п. 52), а серед пріоритетних завдань правоохоронних, спеціальних, розвідувальних та інших державних органів виділяється активна та ефективна протидія розвідувально-підривній діяльності, спеціальним інформаційним операціям та кібератакам. У Стратегії згадується “інформаційна зброя”, яку застосовує Російська Федерація для зміцнення своїх позицій у Європі, а також поширення міжнародного тероризму у кіберпросторі як загроза національній безпеці України.

Очевидно, що визначення інформаційного тероризму має знайти відображення у Стратегії інформаційної безпеки України, розробка якої впливає з положень Стратегії національної безпеки України (п. 66).

Зауважимо, що визначення інформаційного тероризму не містять й міжнародні правові акти, серед яких виділяються Конвенція Ради Європи про запобігання тероризму (2005 р.), Конвенція про кіберзлочинність (2001 р.) Аналіз зазначених актів дає підстави для висновку, що кібертероризм є частиною або, за твердженням деяких науковців, ідентичним поняттям щодо інформаційного тероризму [3, с. 112].

Таким чином, аналіз нормативно-правових актів у сфері боротьби з тероризмом свідчить про те, що поняття інформаційного тероризму не знайшло відображення у чинному законодавстві України. Однак, як зазначалося раніше, на доктринальному рівні це поняття досліджувалося як вченими, так і практичними фахівцями у сфері інформаційних технологій. На думку більшості зарубіжних дослідників, інформаційний тероризм є різновидом терористичної діяльності, яка пов'язана з досягненнями у сфері інформаційних технологій.

На думку О. Ісакова, інформаційний тероризм – це сфера негативного впливу на особу, суспільство, державу за допомогою всіх видів інформації з метою послаблення або повалення конституційного ладу [22].

Схожої думки додержується І.М. Глотіна, на думку якої інформаційний тероризм як багатогранне, мінливе явище є формою негативного впливу на особу, суспільства, державу за допомогою використання інформаційно-комунікаційних технологій. Вільний доступ, анонімність користувачів, масовість аудиторії, обмежені можливості контролю, недосконалість законодавства є чинниками, які сприяють поширенню інформаційного тероризму [23, с. 134].

Окремі дослідники розглядають інформаційний тероризм в межах виключно інтелектуальної сфери. Так, А. Кота вважає інформаційний тероризм одним з найбільш перспективних видів тероризму, який діє в інтелектуальній сфері і породжує новий вид пов'язаного з кіберпростором насильства, яке може бути спрямоване проти будь-кого, а його успіх забезпечується не грубою силою, а нейронами [24, с. 56]. Дійсно, різного роду маніпуляції суспільною свідомістю негативно впливають на інтелектуальний розвиток людства, а інформаційний тероризм можна визнати різновидом деструктивного інформаційно-психологічного впливу на масову свідомість людей [25].

З точки зору американського професора У. Тафойа, інформаційним тероризмом є залякування суспільства шляхом використання високих 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 [26].

Слід зазначити, що визначення інформаційного тероризму висвітлюються і в дослідженнях вітчизняних вчених.

В.О. Коршунов під інформаційним тероризмом пропонує розуміти новий вид терористичної діяльності, орієнтований на використання різних форм і методів тимчасового або незворотного виведення з ладу інформаційної інфраструктури держави або її елементів, а також за допомогою протиправного використання інформаційної структури для створення умов, що тягнуть за собою тяжкі наслідки для різних сторін життєдіяльності особистості, суспільства і держави [7, с. 6].

Т.П. Яцик вважає, що сучасний інформаційний тероризм характеризується як множина інформаційних війн та спецоперацій, пов'язаних з національними або транснаціональними кримінальними структурами та спецслужбами іноземних держав [9, с. 57].

На кримінально-правові аспекти інформаційного тероризму звертає увагу Р.О. Банк, який вважає за доцільне передбачити у законодавстві відповідальність за інформаційний терористичний акт. Під таким актом пропонується розуміти дії інформаційно-психологічного та інформаційно-технічного впливу, спрямовані на розв'язання суспільно-політичних, ідеологічних, національних, територіальних конфліктних ситуацій з метою маніпуляції та зомбіювання свідомості особи чи

широкого кола осіб шляхом реалізації способів і методів інформаційного насильства, застосування інформаційної зброї [3, с. 115].

Аналіз національного законодавства та наукової літератури з порушеного питання дає підстави для висновку, що інформаційний тероризм – доктринальне поняття теорії інформаційної безпеки, під яким розуміють: 1) різновид форми суспільно небезпечного діяння, яким є “тероризм”; 2) форму деструктивного інформаційно-психологічного впливу на особистість, суспільство і державу; 3) небезпечні діяння з інформаційного впливу на соціальні групи осіб, державні органи влади і управління, пов’язані із розповсюдженням інформації, яка містить погрози переслідуванням, розправою, вбивствами, а також викривлення об’єктивної інформації, що спричиняє виникнення кризових ситуацій в державі, нагнітання страху і напруги у суспільстві [1]; 4) певний насильницький пропагандистський вплив на психіку людини, який не дає йому можливості критично оцінювати отриману інформацію [2]; 5) новий вид терористичної діяльності, орієнтований на використання різних форм і методів тимчасового або незворотного виведення з ладу інформаційної інфраструктури держави або її елементів, а також за допомогою протиправного використання інформаційної структури для створення умов, що тягнуть за собою тяжкі наслідки для різних сторін життєдіяльності особистості, суспільства і держави [7]; 6) множину інформаційних війн та інформаційних спецоперацій, пов’язаних із національними або транснаціональними кримінальними структурами та спецслужбами іноземних держав [9]; 7) злиття фізичного насильства зі злочинним використанням інформаційних систем, а також умисне зловживання цифровими інформаційними системами, мережами або їх компонентами з метою сприяння здійсненню терористичних операцій або акцій [27]; 8) ідеологічно обґрунтовану практику впливу, направленою на залякування населення, на прийняття рішення або вчинення дії (бездіяльності) органом влади, органом місцевого самоврядування, міжнародною організацією, соціальною групою, юридичною особою або фізичною особою в межах інформаційного простору, пов’язаного з використанням інформації, інформаційних технологій і (або) інформаційного ресурсу [15].

Основою інформаційного тероризму є інформаційне насильство, з-поміж властивостей якого виділяється: несиловий, ідеальний характер, вихід за межі фізичних закономірностей; нелінійність; порушення закону збереження речовини й енергії, кумулятивний характер, можливість бурхливого зростання інформації; широке розповсюдження; можливість ідеального клонування; нелокалізованість у часі; опосередкований характер і прихованість впливу; віртуальний характер впливу; можливість фіксування; селективність; легкість доступу, злому інформаційних систем [28].

Залежно від спрямованості умовно можна виділити два види інформаційного тероризму: 1) “психологічний” (пропаганда тероризму, створення атмосфери страху і паніки в суспільстві і т.д.); 2) “технічний” (контролювання або блокування каналів передачі масової інформації, порушення функціонування об’єктів інформаційної інфраструктури та ін.) [17].

Залежно від злочинної мети та використання інструментів (засобів) її досягнення інформаційний тероризм теж поділяється на два види: медіа-тероризм та кібертероризм.

Медіа-тероризм – зловживання інформаційними системами, мережами, та їхніми компонентами для здійснення терористичної діяльності (пропаганда та поширення ідеології тероризму, сприяння вчиненню теракту). Засобами здійснення медіа-тероризму є друковані ЗМІ, мережі ефірних й кабельних мас-медіа, Інтернет, електронна пошта, спам тощо. [3, с. 114].

Кібертероризм – навмисна, політично вмотивована атака на об'єкти інформаційного простору, що створює небезпеку для життя та/або здоров'я людей або настання інших тяжких наслідків, якщо такі дії були здійсненні з метою порушення державної чи громадської безпеки, залякування населення, провокації військового конфлікту чи загроза вчинення таких дій [4]. Закон України “Про основні засади забезпечення кібербезпеки України” визначає кібертероризм як терористичну діяльність, що здійснюється в кіберпросторі або з його використанням (ст. 1) [19]. Кібертероризм є серйозною суспільно-політичною загрозою для людства, у порівнянні навіть з ядерною, бактеріологічною і хімічною зброєю, причому ступінь цієї загрози через свою новизну, не до кінця ще усвідомлений і вивчений. Світовий досвід свідчить про безперечну уразливість будь-якої держави, тим більше, що кібертероризм не має державних кордонів; кібертерорист здатний рівною мірою загрожувати інформаційним системам, розташованим практично в будь-якій точці земної кулі шляхом використання спеціального програмного забезпечення, призначеного для несанкціонованого проникнення в комп'ютерні мережі та організації віддаленої кібератаки на інформаційні ресурси жертви [29, с. 42-43].

Також небезпечними проявами інформаційного тероризму є релігійні, псевдорелігійні, сектантські організації, в середовищі яких зароджуються ідеї тероризму, а масовий інформаційний вплив на людей забезпечує поширення ідеології прихильників таких організацій [25, с. 7].

Викладене свідчить про необхідність визначення на законодавчому рівні поняття “інформаційний тероризм”, а також формування системи запобігання тероризму з урахуванням його інформаційних різновидів. У ст. 3 Закону України “Про боротьбу з тероризмом” передбачено принцип пріоритетності попереджувальних заходів. Кінцевим підсумком реалізації державної політики у сфері запобігання тероризму має стати усунення причин і умов, що сприяють виникненню цього негативного явища. Курс на пріоритетність запобігання тероризму обумовлюється такими чинниками: 1) доктринальним визначенням стратегії запобіжної діяльності; 2) прогнозуванням змін і тенденцій тероризму та його проявів; 3) визначенням порядку, методики, форм і засобів запобіжної діяльності; 4) інформаційним забезпеченням реалізації визначених завдань; 5) розробкою програм, планів запобігання тероризму; 6) координацією запобіжної діяльності суб'єктів боротьби з тероризмом; 7) здійсненням контролю за виконанням; 8) матеріальним та іншим ресурсним забезпеченням [30].

Завдання, основні принципи та напрями вдосконалення загальнодержавної системи боротьби з тероризмом з огляду на сучасні терористичні загрози національній безпеці України та прогноз їх розвитку визначені Концепцією боротьби з тероризмом в Україні, напрями реалізації якої передбачають: визначення та аналіз причин і умов, що призводять до поширення тероризму; удосконалення правових та організаційних основ боротьби з тероризмом; удосконалення існуючих, розроблення та впровадження нових методів боротьби з тероризмом; оптимізація шляхів та способів захисту життя і безпеки, прав і свобод людини і громадянина, захисту інтересів суспільства та держави від терористичних посягань; поліпшення інформаційного, наукового, кадрового та матеріально-технічного забезпечення суб'єктів боротьби з тероризмом [31].

Одним з визначених Концепцією пріоритетів боротьби з тероризмом є інформаційне, наукове та інше забезпечення боротьби з тероризмом. Відповідно до Концепції таке забезпечення має включати здійснення моніторингу стану і тенденцій поширення тероризму; проведення постійного системного аналізу і багатовимірною комплексного оцінювання причин та умов, що впливають на виникнення і поширення

тероризму, постійного і своєчасного обміну між суб'єктами боротьби з тероризмом інформацією про терористичні загрози; уніфікації програм навчання, підготовки та перепідготовки особового складу та працівників суб'єктів боротьби з тероризмом; застосування сучасних систем безпеки на об'єктах можливих терористичних посягань; забезпечення суб'єктів боротьби з тероризмом необхідною ресурсною базою [31].

Реалізація зазначених заходів безумовно сприятиме запобіганню різним проявам тероризму, у т.ч. інформаційного. Проте, на законодавчому рівні залишається невизначеним поняття “інформаційний тероризм”, його ознаки та види. Це, у свою чергу, ускладнює реалізацію антитерористичної політики держави.

Висновки.

Таким чином, як узагальнююче можна надати наступне визначення поняття “інформаційний тероризм”: *Інформаційний тероризм – антисоціальне явище, для якого характерним є умисне застосування інформаційно-психологічного та інформаційно-технічного впливу, спрямованого на маніпуляцію чи залякування населення або заподіяння шкоди 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 і (або) інформаційного простору.*

Закріплення такого поняття на законодавчому рівні сприятиме реалізації державної інформаційної політики в контексті протидії правопорушенням в інформаційній сфері, забезпеченню інформаційної безпеки як складової національної безпеки України.

Використана література

1. 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: 04.02.2021).
2. Бураева Л.А. Информационный терроризм как угроза национальной безопасности Российской Федерации. URL: <https://cyberleninka.ru/article/n/informatsionnyy-terrorizm-kak-ugroza-natsionalnoy-bezopasnosti-rossiyskoj-federatsii/viewer> (дата звернення: 04.02.2021).
3. Банк Р.О. Інформаційний тероризм як загроза національній безпеці України: теоретико-правовий аспект. *Інформація і право*. № 1(16)/2016. С. 110-116.
4. Пилипчук В.Г., Дзьобань О.П. Теоретичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації. *Стратегічні пріоритети*. 2011. № 4. С. 12-17.
5. Почепцов Г.Г. Информационные войны. – (Серия: Образовательная библиотека). Издательство: Рефл-бук, 2001. 576 с.
6. Брижко В.М. е-боротьба в інформаційних війнах та інформаційне право: монографія; за ред. члена-кореспондента АПрН України, д.е.н., професора М. Швеця. Київ: НДЦП АПрН України, 2007 р. 236 с.
7. Коршунов В.О. Політичний тероризм: інформаційні методи боротьби: автореф. дис. ...канд. політ. наук: спец. 23.00.02. Дніпропетровськ, 2008. 18 с.
8. Рижов І.М., Строгий В.І. Концептуальні засади соціально-інформаційних технологій упередження кризових явищ соціального характеру (на прикладі моніторингу тероризму). *Науковий вісник Львівського державного університету внутрішніх справ. Серія: “Юридичні науки”*. 2014. № 3. С. 219-228.
9. 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.
10. Livingstone М.Н. International terrorism in the contemporary World. Westport (Conn.). 1978.

11. Жан Бодрийяр. Дух терроризма. Войны в заливе не было (сборник). Москва: “РИПОЛ классик”, 2016. 930 с.
12. Тоффлер Э., Тоффлер Х. Война и антивоенная: Что такое война и как с ней бороться. Как выжить на рассвете XXI века. Москва: АСТ: Транзиткнига, 2005. 412 с.
13. Хоффман Б. Терроризм – взгляд изнутри / пер. с англ. Е. Сажина. Москва: Ультра. Культура, 2003. 252 с.
14. Шмид А. Статистика терроризма: задачи определения тенденций в глобальном масштабе: *Форум по проблемам преступности и общества*. Т. 4. № 1, 2. Декабрь 2004 г. С. 51-71.
15. Ковлагина Д.А. Информационный терроризм: понятие, уголовно-правовые и иные меры противодействия: дис. ...канд. юрид. наук: спец. 12.00.08. ФГБОУ ВПО Саратовская государственная юридическая академия, 2016. 270 с.
16. Настюк В.Я. Трофімов С.А. Міжнародно-правовий режим протидії тероризму: монографія. Харків: Право, 2008. 350 с.
17. Молчанов Н.А., Матевосова Е.К. Информационный терроризм в международно-правовом контексте. *Вестник Университета имени О.Е. Кутафина (МГЮА)*. 2018. № (5). С. 94-103.
18. Про боротьбу з тероризмом: Закон України від 20.03.03 р. № 638-IV. *Відомості Верховної Ради України*. 2003. № 25. Ст. 180. URL: <https://zakon.rada.gov.ua/laws/show/638-15#Text> (дата звернення: 04.02.2021).
19. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. *Відомості Верховної Ради*. 2017. № 45. Ст. 403. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (дата звернення: 04.02.2021).
20. Доктрина інформаційної безпеки: Указ Президента України від 25.02.17 р. № 47. URL: <https://zakon.rada.gov.ua/laws/show/47/2017#Text> (дата звернення: 04.02.2021).
21. Стратегія національної безпеки України: Указ Президента України від 14.09.20 р. № 392. URL: <https://zakon.rada.gov.ua/laws/show/392/2020#Text> (дата звернення: 04.02.2021).
22. Исаков А.И. Информационный терроризм. *Обозреватель-Observer*. – (Научно-аналитический журнал). URL: http://observer.materik.ru/observer/N5-6_02/5-6_10.htm (дата звернення: 04.02.2021).
23. Глотина И.М. Информационный терроризм и его влияния на экономику. *Экономическая глобализация и проблемы национальной международной безопасности*. 2014. С. 132-134. URL: <file:///C:/Users/%D0%91%D0%BE%D1%80%D0%B8%D1%81/Downloads/informatsionnyu-terrorizm-i-ego-vliyanie-na-ekonomiku.pdf> (дата звернення: 04.02.2021).
24. Кога А. Эпоха терроризма. *Международный терроризм и право*. Москва, 2004. С. 56-60.
25. Арчаков В. О понимании проблемы информационного терроризма в глобальном и региональном масштабе. URL: https://beldumka.belta.by/isfiles/000167_885379.pdf (дата звернення: 04.02.2021).
26. 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: 04.02.2021).
27. Jerrold M. From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism. *NATO Library at: Terrorism and political violence*. Vol. 12, no. 2. Summer 2000. P. 97-122.
28. Дзьобань О.П. Насильство інформаційне. – (Енциклопедія соціогуманітарної інформології). Київ: Видавничий дім “Гельветика”, 2020. Т. 1. С. 151-155.
29. Мазуров В.А. Кибертерроризм: понятие, проблемы противодействия: доклады ТУСУРа, 2010. № 1(21). Ч. 1. С. 41-45.
30. Леонов Б.Д. Запобігання та протидія тероризму: теоретичні підходи. *Часопис Національного університету “Острозька академія”*. Серія: “Право”. 2012. № 2(6). URL: <http://lj.oa.edu.ua/articles/2012/n2/12lbdttp.pdf>
31. Концепція боротьби з тероризмом: Указ Президента України від 05.03.19 р. № 53. URL: <https://zakon.rada.gov.ua/laws/show/53/2019#Text> (дата звернення: 04.02.2021).