УДК 32.019.51:323.28:323.2(477)

БАНК Р.О., *кандидат юридичних наук,*
старший викладач кафедри загальноправових дисциплін
Київського національного торговельно-економічного університету

ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ: ТЕОРЕТИКО-ПРАВОВИЙ АСПЕКТ

Анотація. *Стаття присвячена проблемі інформаційного тероризму в контексті загрози національній безпеці України. Визначено нормативно-правове закріплення інформаційного тероризму та окреслено суттєві прогалини в законодавстві України в регулюванні цього явища. Проведено аналіз та класифікацію видів інформаційного тероризму в сучасному глобальному кіберпросторі. Запропоновані деякі шляхи протидії інформаційному тероризму як фактору дестабілізації національної безпеки України.*

Ключові слова: *інформаційний тероризм, загрози, національна безпека, медіа-тероризм, кібертероризм, правове регулювання, нормативно-правове закріплення.*

Аннотация. *Статья посвящена проблеме информационного терроризма в контексте угрозы национальной безопасности Украины. Определено нормативно-правовое закрепление информационного терроризма и отмечены значительные пробелы в законодательстве Украины в регулировании этого явления. Проведен анализ и классификация видов информационного терроризма в современном глобальном киберпространстве. Предложены некоторые пути противодействия информационному терроризму как фактору дестабилизации национальной безопасности Украины.*

Ключевые слова: *информационный терроризм, угрозы, национальная безопасность, медиа-терроризм, кибертерроризм, правовое регулирование, нормативно-правовое закрепление.*

Summary. *The article is devoted to the problem of information terrorism in the context of threat to the national security of Ukraine. Author defines regulatory consolidation of information terrorism and outlines the significant gaps in the legislation of Ukraine in regulating this phenomenon. The article offers analysis and classification of information terrorism in today's global cyberspace. Author proposes some ways to counteract information terrorism as a factor of destabilization of Ukraine's national security.*

Keywords: *information terrorism, threats, national security, media terrorism, cyberterrorism, legal regulation, regulatory and legal consolidation.*

Постановка проблеми. В умовах швидкого поширення глобалізаційних процесів в макроекономічному просторі зростають можливості інформаційного впливу на особу, суспільство та державу. Безперервне широкомасштабне поширення інформації сприяє її розповсюдженню на великі території в найкоротші терміни. Хоч це і вважається одним з важливих досягнень людства, та все ж має свої недоліки, оскільки глобалізована інформатизація збільшує можливості виникнення інформаційних загроз. Інформаційна епоха розширила сферу поширення інформаційно-комунікативних воєн, що призвело до появи інформаційного тероризму, як засобу ведення інформаційної війни, що поєднав у собі біфуркаційні процеси фізичного тероризму, скорельованого в інформаційних системах та умисним зловживанням кіберпростором, мережами або їх компонентами з метою сприяння здійсненню терористичних операцій. Інформаційний тероризм набув нових загрозливих форм, а його швидке поширення стало наслідком зомбіювання соціуму та активізації сепаратистського руху, що в кінцевому результаті може стати причиною втрати суверенітету, незалежності та територіальної цілісності окремої держави.

Феномену інформаційного тероризму присвячено праці як зарубіжних, так і вітчизняних науковців. Серед теоретиків та практиків, які займалися дослідженням інформаційного тероризму як засобу ведення інформаційної війни в умовах транскордонних глобалізованих процесів та розвитку інформаційного кіберпростору, слід зазначити Д. Белла, Ж. Бодрійара, Е. Гіденса, М. Кастельса, Е. Тоффлера, Ф. Фукуяму, С. Хантінгтона, Б. Хофмана, А. Шміда та ін.

Дослідженню окремих проблем тероризму та його похідної – інформаційного тероризму, розробки та застосування заходів протидії цьому негативному явищу приділялася увага в роботах таких українських фахівців, як В. Ліпкан, Г. Почепцов, І. Рижов, Ю. Максименко, М. Зубок, А. Форос. Однак, необхідно зауважити, що комплексний аналіз цього феномену потребує подальших наукових досліджень в контексті його нормативно-правового закріплення.

Метою статті є визначення агрегативних взаємозв’язків варіабельності щодо поняття “інформаційний тероризм” та його аксіоматичне закріплення у нормах права.

Виклад основного матеріалу. Закріплення в Конституції України (ст. 17) пріоритетності інформаційної безпеки, як основної функції держави демонструє рівень значущості інформаційних процесів та важливості протидії інформаційним загрозам [1].

Законом України “Про основи національної безпеки” (ст. 7) визначається, що захист від намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації є одним з базових завдань в боротьбі з інформаційними загрозами. До інших загроз віднесено: прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп’ютерна злочинність та комп’ютерний тероризм; розголошення інформації, яка становить державну таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави [2].

В Указі Президента України “Про Доктрину інформаційної безпеки України” від 8 липня 2009 р. № 514, що втратив чинність, було виділено наступні загрози інформаційній безпеці країни: поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України; зовнішні деструктивні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет; деструктивні інформаційні впливи, які спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності і недоторканності України; прояви сепаратизму в засобах масової інформації, а також у мережі Інтернет, за етнічною, мовною, релігійною та іншими ознаками.

Розроблений і підготовлений Державним комітетом телебачення і радіомовлення України новий проект Указу Президента України “Про Доктрину інформаційної безпеки України”, “Стратегія національної безпеки України” затверджена Указом Президента України від 26 травня 2015 р. № 287, Рішення Ради національної безпеки і оборони України “Про невідкладні заходи із забезпечення державної безпеки”, що введено в дію Указом Президента від 14 листопада 2014 р. № 880 та значна кількість інших нормативно-правових актів містять основоположні фундаментальні засадничі принципи боротьби з інформаційними загрозами, які в сукупності дають цілісну картину векторного впливу на інформаційне середовище. Однак в жодному з вище згаданих нормативно-правових актів не визначено поняття інформаційного тероризму, як загрози національної безпеки України.

Частково, на нормативному рівні, детермінанта інформаційного тероризму випливає через аналіз положень Закону України “Про боротьбу з тероризмом”, а саме через його корелятивний зв’язок з поняттям технологічного тероризму, що вчиняється з терористичною метою із застосуванням 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, або створюють умови для аварій і катастроф техногенного характеру [3]. Проте означена дефініція технологічного тероризму, в жодному випадку, не може рівноцінно замінити терміносполуки “інформаційний тероризм” на найвищому законодавчому рівні.

Якщо говорити про міжнародно-правові акти в цій сфері, головним документом, в якому йде мова про боротьбу з інформаційними загрозами, є Конвенція “Про кіберзлочинність” від 23 листопада 2001 р., ратифікована Верховною Радою України 07 вересня 2005 р. Цей документ націлено на здійснення загальної політики з питань кримінального права, метою якої є захист суспільства від кібертероризму. Однак, в цьому документі нічого не зазначено про поняття “інформаційний тероризм”, тільки ретельний аналіз Конвенції дає підстави стверджувати, що кібертероризм є частиною, або, за твердженням деяких науковців, ідентичним поняттям щодо інформаційного тероризму. Важливість означеного міжнародно-правового документу обумовлена процесом правової регламентації та імплементації у чинне законодавство поняття інформаційного тероризму.

Семантика нормативно-правових актів дає підстави стверджувати, що поняття інформаційного тероризму не знайшло свого відображення в чинному законодавстві України, однак на доктринальному рівні означене поняття досліджувалось як юристами, так і фахівцями з державного управління, безпекознавства та політології.

Так, В.О. Коршунов вказує, що інформаційний тероризм – це 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 [4, с. 6].

Т.П. Яцик вважає, що сучасний інформаційний тероризм характеризується як множина інформаційних війн та спецоперацій, пов’язаних із національними або транснаціональними кримінальними структурами та спецслужбами іноземних держав. Доступність інформаційних технологій значно підвищує ризики інформаційного тероризму [5, с. 57].

Міжнародні фахівці у сфері боротьби та протидії інформаційним загрозам, зазначають, що інформаційний тероризм – 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 [6, с. 98].

Іншим визначенням інформаційного тероризму є діяльність, що виражається в залякуванні населення й органів влади з метою досягнення злочинних намірів [7, с. 14].

Визначення інформаційного тероризму можна віднайти в інших дослідженнях фахівців з цієї проблематики. Однією з характерних рис визначень інформаційного тероризму є те, що в переважній більшості з них згадується тільки один аспект інформаційної безпеки, а саме пов’язаний із засобами обробки інформації, що, на наш погляд, звужує поняття інформаційного тероризму, тим самим обмежуючи сферу

правового регулювання, що не сприяє ефективній співпраці держав у процесі боротьби з інформаційним тероризмом.

Необхідно відзначити, що для України, де інформатизація суспільства перебуває на етапі становлення, а інформаційні ресурси контролюються, в переважній частині, приватними суб’єктами підприємницької діяльності, головними загрозами у сфері інформаційного тероризму є зовнішні, а не внутрішні. Їх переважно створюють іноземні держави, міжнародні терористичні та інші злочинні угрупування й організації, які користуються слабкою координацією та цілеспрямованістю діяльності органів публічної адміністрації у боротьбі з цим небезпечним явищем.

Неспроможність налагодження з боку органів публічної адміністрації ефективного механізму протидії інформаційним загрозам створила передумови для зростання великої кількості різновидів інформаційного тероризму.

Аналіз нормативно-правової бази та наукової літератури дає нам підстави провести структурну класифікацію видів інформаційного тероризму, яку умовно можна розділити на інтелектуальну та матеріальну. Так, а) дискредитація, дезінформація, поширення чуток, неповної, неточної, недостовірної інформації, маніпуляція свідомістю, зомбіювання населення є частиною інформаційно-психологічного тероризму; б) завдання збитків окремим елементам і всьому інформаційному середовищу супротивника в цілому, руйнування елементної бази, активне придушення ліній зв’язку, штучне перезавантаження вузлів комунікації є частиною інформаційно-технічного тероризму.

Необхідно відзначити, що специфічним різновидом інформаційно-психологічного тероризму (інтелектуального) є медіа-тероризм. У випадку медіа-тероризму йдеться про різновид інформаційного тероризму, що є зловживанням інформаційними системами, мережами, та їхніми компонентами для здійснення терористичних дій та акцій. Засобами здійснення медіа-тероризму є друковані ЗМІ, мережі ефірних й кабельних мас-медіа, Інтернет, електронна пошта, спам тощо. Медіа-тероризм представляє собою особливий вид терористичної діяльності, що виділений за критерієм використання інструментів (засобів) досягнення терористами власних цілей.

К.С. Герасименко стверджує, що його сутність полягає у спробах шляхом організації спеціальних медіа-кампаній дестабілізувати суспільство, створити у ньому атмосферу громадянської непокори, недовіри суспільства до дій та намірів влади й особливо – її силових структур, покликаних захищати суспільний порядок [8, с.163].

Найефективнішими з інструментаріїв медіа-тероризму вважаються ЗМІ та мережа Інтернет, що у корелятивному взаємозв’язку формують інформаційний ресурс, який здатний за абстрактною реальністю приховувати достовірну, точну та повну інформацію. Яскравим прикладом використання терористами ЗМІ та мережі Інтернет є маніпулювання громадською думкою, поширення дезінформуючого впливу на суспільство, дискредитація офіційних органів публічної адміністрації з метою психологічного зомбіювання соціуму та поширення одновекторної інформації, що в результаті формує ідеологію прийнятну для терористів.

Важливо зауважити, що на сучасному етапі інформаційний тероризм широко використовує різноманітні новітні засоби комунікації для полегшення процесу планування операцій, проведення зборів, встановлення зв’язку, отримання та передачі оперативної інформації тощо. Наприклад, під час громадянської війни в Сирійській Арабській Республіці у 2011 – 2014 роках сирійські бойовики широко використовували мультимедійні смартфони Iphone, що пізніше стало причиною їхньої заборони урядом країни [9].

Під впливом медіа-тероризму індивід не здатен самостійно орієнтуватися в необмеженому інформаційному просторі доступних даних, тому що мас-медіа представлена сьогодні у вигляді інструментів для конструювання недостовірної реальності. Завданням цієї реальності є не відтворення та поширення достовірної інформації, а підкорення особистості невластивим їй судженням. Таким чином, сьогодні не можна говорити про перехід кількості інформації в її якість. Особливо це стосується ЗМІ та мережі Інтернет, так як вони виступають об’єктом політичного впливу, який має на меті викривити реальний стан речей.

Специфічним різновидом інформаційно-технічного (матеріального) тероризму є кібертероризм. Під ним розуміють сукупність дій, що включають інформаційну атаку на комп’ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші складові інформаційної інфраструктури, яка здійснюється злочинними угрупуваннями або окремими особами. Кібертероризм спрямований на проникнення в інформаційно-телекомунікаційну систему, перехоплення управління, пригнічення засобів мережевого інформаційного обміну та здійснення інших деструктивних дій. Небезпека такого виду інформаційного тероризму полягає в тому, що він не має національних меж (терористичні акції можуть здійснюватися з будь-якої точки світу) та в проблематичності виявлення терориста в інформаційному просторі, адже хакери здійснюють терористичну діяльність через декілька підставних комп’ютерів, що ускладнює його ідентифікацію та визначення місцезнаходження [10, с. 230-231].

Кібертероризм за швидкого глобального інформаційного поширення набув нових загрозливих тенденцій та здатний завдати величезної шкоди на місцевому, національному та міжнародному рівнях. Здійснення кібертерористичних атак з фінансової точки зору стало прибутковою справою для терористів, що змушує уряди багатьох країн світу виділяти значні кошти для протидії та нейтралізації цього явища. До того ж, кібертерористи розширили свій діапазон дій у зв’язку з тотальним та масштабним застосуванням Інтернету, що призвело до зростання кількості злочинів пропорційно числу користувачів комп’ютерних мереж.

Кібертероризм є серйозною соціально-небезпечною 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. Досвід, що є у світової спільноти у цій сфері, зі всією очевидністю 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 [11].

За твердженням фахівців контррозвідувальних управлінь, “терористи” за допомогою електронної пошти передають в зашифрованому вигляді інструкції, карти, схеми, паролі та іншу важливу інформацію, розголошення якої може зашкодити національній безпеці держави [8, с. 165].

У зв’язку з цим Генеральна Асамблея ООН прийняла в грудні 1998 року резолюцію по кіберзлочинності, що стосується кібертероризму та кібервійни. Резолюція 53/70 закликає держави-члени 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 і що допомагають боротися з інформаційним тероризмом і злочинністю [12, с. 16].

Кібертероризм став новим видом загрози національній безпеці держави, який за стрімкого розвитку інформаційних технологій та глобального поширення мережі

Інтернет набув новітніх форм та здатний нанести значної шкоди як в мікросередовищі, так і в макропросторі.

Проаналізувавши вищезазначене, необхідно зауважити, що проблеми інформаційного тероризму в контексті національної безпеки держави, викликають необхідність аналізу його структури та нормотворчого закріплення.

Висновки та пропозиції.

Нормотворчо-правовий базис повинен слугувати надійним бар’єром захисту від інформаційних загроз, які виникають у ході функціонування держави, як структурної одиниці в глобальному середовищі. З метою забезпечення конституційних прав та свобод громадян, повинні вводитися в дію механізми протистояння джерелам інформаційного тероризму. Дані механізми утворюються сукупністю законодавчих актів, які передбачають справедливі покарання за порушення системи суспільних інтересів.

Незважаючи на наявність низки вагомих нормативно-правових актів, українське інформаційне законодавство не виявляє себе ефективною системою захисту національних інтересів. Особливо це відчувається в умовах перебігу збройного конфлікту та проведення антитерористичної операції. Поширення неправдивих відомостей, нав’язування ідей та поглядів, які суперечать демократичним цінностям громадян, вплив на суспільну свідомість, неповне відображення статистичних даних – всі ці та багато інших дій спрямовуються на дискредитацію нашої країни в міжнародному політичному та культурно-ідеологічному просторі. Відсутність профілактичних заходів та нейтральна позиція державних лідерів щодо даної проблематики лиш загострює інформаційне протистояння та сприяє формуванню негативного іміджу держави на міжнародній арені.

Саме тому доречно було б більшу увагу приділити нормативно-правовому регулюванню наступних питань:

- визначення на законодавчому рівні поняття інформаційного тероризму;
- кодифікація інформаційного законодавства;
- застосування новітніх розробок в сфері інформаційних технологій з метою захисту персональних даних;
- закріплення на законодавчому рівні інтернет-відносин у ланцюгу держава-інтернет-споживач;
- захист інформації від несанкціонованого доступу;
- сприяння науково-технічному розвитку національних засобів масової комунікації;
- державне регулювання доступу до інформаційних ресурсів.

Також вбачається доцільним закріплення в законодавстві юридичної відповідальності за інформаційний тероризм, а саме криміналізація цього небезпечного діяння. Так, пропонуємо доповнити Кримінальний кодекс України ст. 258^{-6} “Інформаційний терористичний акт”. Редакція та структура цієї правової норми буде наступною:

Інформаційний терористичний акт, тобто, 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 – караються виправними роботами на строк до двох років або арештом на строк до шести місяців,

або обмеженням волі на строк до трьох років, або позбавленням волі на той самий строк з конфіскацією майна або без такої.

Вказані напрями діяльності держави щодо удосконалення механізмів протидії інформаційному тероризму дозволять здійснити перехід інформаційного законодавства України на новий якісний рівень та прискорити розвиток дієвих заходів боротьби з цим негативним явищем.

Використана література

1. Конституція України : Закон України від 28.06.96 р. № 254к/96-ВР // Відомості Верховної Ради України (ВВР). – 1996. – № 30. – Ст. 141.

2. Про основи національної безпеки України : Закон України від 19.06.03 р. № 964-IV // Офіційний вісник України. – 2003. – № 29. – Ст. 1433

3. Про боротьбу з тероризмом : Закон України від 20.03.03 р. // Відомості Верховної Ради України (ВВР). – 2003. – № 25. – Ст. 180

4. Коршунов В. О. Політичний тероризм: інформаційні методи боротьби : автореф. дис. на здобуття наук. ступеня канд. політ. наук : спец. 23.00.02 “Політична інститути та процеси” / В.О. Коршунов. – Дніпропетровськ, 2008. – 18 с.

5. 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.

6. Jerrold M. From Car Bombs to Logic Bombs : The Growing Threat from Information Terrorism / M. Jerrold // NATO Library at : Terrorism and political violence, vol. 12, no. 2, Summer 2000. – P. 97-122.

7. Thevenet C. Cyber-terrorisme, mythe ou réalité? / C. Thevenet // Série Mémoires et Thèse. – Université de Marne-La-Vallée. – 2005. – 57 p

8. Герасименко К. С. Сучасні ознаки загроз “інформаційного тероризму” // Форум права. – 2009. – № 3. – С. 162-166. – Режим доступу : file:///C:/Users/User/Downloads/FP_index.htm_2009_3_26%20(12).pdf

9. Ілія Куса. Інформаційний аспект тероризму та переговорний процес із терористами. 15.02.2014. – Режим доступу : http://mskod.com/informatsiyniy-aspekt-terorizmu-ta-peregovorniy-protses-iz-teroristami

10. Бойченко О.В. Медіа-тероризм : особливості сучасних ознак інформаційній безпеці : матеріали другої міжнародної наук.-практ. конф. [“Інтегровані інтелектуальні робототехнічні комплекси (ПРТК-2009)”], (Київ, 25 – 28 травня 2009 р.). – К. : НАУ, 2009. – С. 230-232.

11. Chambet P. Le cyber-terrorisme – Режим доступу : http://www.chambet.com/publications/Cyberterrorisme.pdf.

12. Катренко А. Особливості інформаційної безпеки за міжнародними стандартами // Альманах економічної безпеки. – 1999. – № 2. – С. 15-17.

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