УДК [323.28+327]:351.746.1(477)

Глазов О. В.

МІЖНАРОДНИЙ ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ У КОНТЕКСТІ ЗАГРОЗ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

Статтю присвячено проблемі міжнародного інформаційного тероризму та участі механізмів державного апарату у боротьбі з даним різновидом злочинної діяльності, котрий несе загрозу національній безпеці держави. Проведено аналіз сучасного стану та рівня загроз «інформаційного тероризму» національним та міжнародним інтересам суспільства. Визначено суттєві перешкоди здійсненню ефективної протидії правоохоронними органами терористичним проявам та актам.

Ключові слова: *національна безпека, тероризм міжнародний, тероризм інформаційний, кібертероризм, інформаційна війна.*

Статья посвящена проблеме международного информационного терроризма и участия механизмов государственного аппарата в борьбе с данным видом преступной деятельности, который несет угрозу национальной безопасности государства. Проведен анализ современного состояния и уровня угроз «информационного терроризма» национальным и международным интересам общества. Определены существенные препятствия осуществлению эффективного противодействия правоохранительными органами террористическим проявлениям и актам.

Ключевые слова: *национальная безопасность, терроризм международный, терроризм информационный, кибертерроризм, информационная война.*

The article is devoted to the problem of prevention of international information terrorism and participation of mechanisms of the state machinery in the fight against this kind of criminal activity that threatens national security. Drawn an analysis of current condition and level of threats of «information terrorism» over national and international public interests. Detected significant obstruction of effective counteraction by law machinery to terrorism demonstrations and terrorism acts.

Key words: *national security, international terrorism, information terrorism, cyberterrorism, information war.*

Міжнародний тероризм належить до найбільш небезпечних і важко прогнозованих явищ, вирізняється особливим динамізмом і багатоплановістю, а також здатністю до адаптації й модернізації в умовах основних цивілізаційних тенденцій сучасності – глобалізації та інформатизації. Так, одним із загрозливих проявів міжнародного тероризму стає інформаційний тероризм, в основі якого – маніпуляція свідомістю мас, розповсюдження інформаційно-емоційного ефекту, на який розраховано більшість терористичних актів, залучення прихильників серед членів суспільства, вплив на владні структури, які приймають політичні рішення. Осмислення в цьому відношенні феномену інформаційного тероризму є передумовою формування більш чітких уявлень щодо сутності сучасного міжнародного тероризму, запобігання загроз, здатних зруйнувати державні інститути, основи державної стабільності, як і основи національної безпеки демократичних країн взагалі.

Зазначимо, що проблеми міжнародного тероризму, і зокрема такого його прояву як інформаційний тероризм знаходять відображення в значному доробку сучасних політологів. Йдеться про аналіз кримінально-правових та політологічних вимірів сучасного міжнародного тероризму [8, 11], концепції інформаційного тероризму, ознак та основних тенденцій його еволюції [2, 12, 14], проявів інформаційного складника політичного тероризму [9, 10, 13], концептуальних засад у сфері інформаційної безпеки держави [1, 3], проблем забезпечення інформаційної безпеки України [4, 5, 16], особливостей міжнародних стандартів інформаційної безпеки [15] і т. і.

Втім, незважаючи на велику кількість праць з даної проблематики, дане питання потребує подальшої наукової розробки, а також розгляду проблеми взаємовпливу сучасного тероризму як невід'ємної частини інформаційної структури та засобів масової інформації (ЗМІ). На порядку денного й узагальнення підходів щодо сутності, ознак, концепції та еволюції інформаційного тероризму; виявлення основних соціокультурних та інформаційних передумов розвитку тероризму в контексті розвитку глобалізаційних

процесів сучасності; з'ясування основних причин використання терористичними угрупованнями інформаційно-комунікативних технологій; визначення загальних політико-правових та морально-етичних засад обмеження діяльності засобів масової інформації у контексті боротьби з терористичними проявами; аналіз дієвості апарату державних установ та громадських організацій у сфері запобігання терористичним та екстримістським проявам в Україні та світі, в плані міжнародного співробітництва з даного питання.

Так, за умов глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнень і боротьби різновекторних національних інтересів держав стає інформаційний простір. Сучасні інформаційні технології дають змогу державам реалізувати власні інтереси без застосування воєнної сили, послабити або завдати значної шкоди безпеці конкурентної держави, яка не має дієвої системи захисту від негативних інформаційних впливів.

За сучасних умов інформаційна складова набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки. Інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та інформаційні технології значною мірою впливають на рівень і темпи соціально-економічного, науково-технічного і культурного розвитку [1, с. 127].

Від обсягу, швидкості та якості обробки інформації значною мірою залежить ефективність управлінських рішень, зростає значення методів управління з використанням інформаційних технологій соціальними та економічними процесами, фінансовими і товарними потоками, аналізу та прогнозування розвитку внутрішнього і зовнішніх ринків. Використання інформаційних технологій визначає структуру і якість озброєнь, необхідний рівень їх достатності, ефективність дій збройних сил. Спроможність ідентифікувати науково-технічні та екологічні проблеми, здійснювати моніторинг їх розвитку і прогнозування наслідків безпосередньо залежать від ефективності використовуваної інформаційної інфраструктури [2, с. 71].

Таким чином, інформаційна безпека стає невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки.

Основне поняття інформаційної безпеки держави – означає стан її захищеності, за якої спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив, котрий завдає суттєвої шкоди національним інтересам [3, с. 122].

Відповідно до законодавства України поняття «інформаційна безпека» має наступне визначення: «стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання, порушення цілісності, конфіденційності та доступності інформації» [4, с. 80].

Виокремлюють три рівня забезпечення інформаційної безпеки [5, с. 318]: 1) *рівень особи* (формування раціонального, критичного мислення на основі принципів свободи вибору); 2) *суспільний рівень* (формування якісного інформаційно-аналітичного простору, плюралізм, багатоканальність отримання інформації, незалежні потужні ЗМІ, які належать вітчизняним власникам); 3) *державний рівень* (інформаційно-аналітичне забезпечення діяльності державних органів, інформаційне забезпечення внутрішньої і зовнішньої політики на міждержавному рівні, система захисту інформації з обмеженим доступом, протидія правопорушенням в інформаційній сфері, комп'ютерним злочинам).

Згідно із Законом України «Про основи національної безпеки» однією з основних загроз інформаційній безпеці є «намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації». До інших загроз віднесено [6]: 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.

У Доктрині інформаційної безпеки України, підписаній Президентом у липні 2009 р., виділено наступні загрози інформаційній безпеці країни [7]: 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 спрямовано 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.

Визнаємо, терористична діяльність як складне, багатоаспектне негативне соціально-політичне явище давно переросла рамки національних меж і перетворилася на масштабну загрозу для безпеки всього людства. Проблема тероризму ускладнюється тим, що тероризм, будучи по суті своїй складним соціально-політичним явищем, акумулює в собі соціальні суперечності, що досягли в сучасному суспільстві рівня багатобічного конфлікту [8, с. 29].

Інформаційна епоха розширила сферу діяльності тероризму, що призвело до появи «інформаційного тероризму», який визначається як 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.

Особливу небезпеку сучасності становить відносно новий вид терористичної діяльності – інформаційний тероризм, розгортання якого зумовлено широким запровадженням інформаційно-телекомунікаційних систем у всіх сферах життєдіяльності суспільства [9, p. 98].

Для України, де інформаційна діяльність поки що не набула належного розвитку, головні загрози у сфері інформаційного тероризму є не внутрішніми, а зовнішніми. Їх переважно створюють іноземні держави, міжнародні терористичні та інші злочинні угруповання й організації, які користуються нерозвиненістю й слабкістю відповідних державних структур.

Визначаючи стан сучасних загроз інформаційного тероризму, слід зазначити, що інформаційний тероризм – це, насамперед, форма негативного впливу на особистість, суспільство і державу усіма видами інформації.

Іншим визначенням інформаційного тероризму є діяльність, що виражається в залякуванні населення й органів влади з метою досягнення злочинних намірів [10, p. 14].

У мирний час прямими виконавцями акцій інформаційного тероризму є іноземні спецслужби й організації, закордонні і значна частина українських ЗМІ, організації сектантів і церковників, різного роду місіонерські організації, окремі екстремістські елементи і групи. Активно використовують інформаційні канали і безпосередньо терористи, подаючи свої плани через офіційні канали інформації. Дестабілізація суспільства чи то у внутрішній політиці країни, між ворогуючими публічними особистостями, чи то у зовнішньополітичних стосунках через інформаційний тероризм стає дедалі популярнішою. Адже вдало оформленою інформацією можна знищити все, і зброя стане неактуальною [11].

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. Розвиненість інформаційної інфраструктури суспільства сприяє створенню додаткових ризиків інформаційного тероризму.

У свою чергу, інформаційний тероризм розділяється на інформаційно-психологічний тероризм (контроль над ЗМІ з метою поширення дезінформації, чуток, демонстрації могутності терористичних організацій) та інформаційно-технічний тероризм (завдання збитків окремим елементам і всьому інформаційному середовищу супротивника в цілому: руйнування елементної бази, активне придушення ліній зв'язку, штучне перезавантаження вузлів комунікації і т. п.). У цьому плані теоретично та практично виправданим представляється використання терміна тероризм [12, с. 231].

Досить типовим прикладом для розуміння сутності медіа-терору, механізмів його викликання, стимулювання й поширення може служити такий специфічний засіб масової інформації, як листівка. У ній головну роль відіграє не інформація, як така, а пропаганда, контрпропаганда, агітація, реклама. Тому головним завданням такого засобу інформаційного тероризму є не інформування, а маніпулювання.

Головним у тактиці інформаційного тероризму є наявність небезпечних наслідків терористичного акту з широтою розголошення відомостей та великим суспільним резонансом.

Поряд із зазначеним, інформаційний тероризм, або «кібертероризм», за формами дії на кіберпростір має всі властиві ознаки політичного тероризму взагалі.

Останнім часом поняття кібертероризму перетнуло межі фантастичного і широко обговорюється в засобах масової інформації. Загроза тероризму в Інтернеті виявилася більших, ніж очікувалося, масштабів, а функції кібертероризму неймовірно розширилися через тотальне поширення Інтернету. Кібертероризм є серйозною соціально-небезпечною загрозою для людства, порівняно, 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 в рівній мірі загрожувати інформаційним системам, розташованим практично в будь-якій точці земної кулі [13].

Стрімке зростання кількості злочинів, що здійснюються в кіберпросторі, пропорційно числу користувачів комп'ютерних мереж (за оцінками Інтерполу, темпи зростання злочинності в глобальній мережі Інтернет, є найшвидшими на планеті) ще раз підкреслює стан небезпеки з боку інформаційного тероризму.

За твердженням фахівців контррозвідувальних управлінь, «терористи» за допомогою електронної пошти передають у зашифрованому вигляді інструкції, карти, схеми, паролі та іншу важливу інформацію, розголошення якої може зашкодити національній безпеці держави [14, с. 165].

У зв'язку з цим Генеральна Асамблея ООН прийняла в грудні 1998 року резолюцію по кіберзлочинності, що стосується кібер-тероризму 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.

Отже, можна констатувати, що загроза кібертероризму в даний час є доволі складною і актуальною проблемою, причому вона буде ускладнюватись по мірі розвитку і розповсюдження інформаційних технологій [15, с. 16].

Це привертає увагу до механізму інформаційної безпеки в контексті національної безпеки держави, викликає необхідність аналізу його структури, рівня дієвості, напрямів вдосконалення з урахуванням потреб часу.

Так, державна система забезпечення інформаційної безпеки країни являє собою організаційне об'єднання державних органів, а також сил та засобів інформаційної безпеки, що виконують свої функції на основі

закону під контролем і захистом судової влади. Державна система складає найважливішу ланку системи інформаційної безпеки особистості, суспільства і держави в правовій державі. Основними завданнями такої системи є: виявлення і прогнозування дестабілізуючих факторів і інформаційних загроз життєво важливим інтересам особистості, суспільства та держави; здійснення комплексу оперативних і довготривалих заходів з їхнього попередження і усунення; створення і підтримання в готовності сил та засобів забезпечення інформаційної безпеки.

Органи (служби) інформаційної безпеки можуть створюватися (на законодавчих засадах) і в недержавних структурах для захисту своїх потреб у забезпеченні необхідною інформацією. Дані органи на основі укладення відповідних угод можуть бути приєднані до єдиної державної системи інформаційної безпеки [16, с. 23].

Згідно із Законом України «Про основи національної безпеки України» визначаються основні напрями державної політики з питань національної безпеки в інформаційній сфері [17]: забезпечення національного суверенітету України; вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій в даній сфері, наповнення внутрішнього та світового інформаційного простору достовірної інформації про Україну; активне залучення ЗМІ до боротьби з корупцією, зловживанням службовим становищем, іншими явищами, які загрожують національній безпеці України; вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери.

Неможна стверджувати однозначно, що існуючий в Україні апарат забезпечення інформаційної безпеки, дійсно готовий витримати сучасні виклики та загрози як внутрішнього так і зовнішнього характеру. Необхідність у постійному вдосконаленні, налагодженні усіх механізмів взаємодії – основна мета, досягнення якої зможе вирішити усі поставлені завдання перед апаратом забезпечення національної безпеки.

Охарактеризувавши проблему, постає необхідність у визначенні основних векторів (пріоритетів) у сфері забезпечення інформаційної безпеки України. Згідно із Законом України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», вирішення проблеми забезпечення інформаційної безпеки держави має здійснюватись у наступних напрямках [18]: створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів; підвищення рівня координації діяльності державних органів щодо виявлення, оцінки та прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань; вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері; розгортання та розвиток Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Так, з урахуванням вищевикладеного матеріалу, необхідно зазначити наступне: інформаційний тероризм як сучасне соціально-політичне явище становить серйозну загрозу безпеці та життєво важливим інтересам як особистості, так суспільства і держави. Очевидно, що застосування терористами новітніх досягнень науки і техніки сильно розширює їх руйнівні можливості, дозволяє залучати до себе загальну увагу і тримати людей в постійному страху. На сьогодні для терористів легко уразливі практично всі комп'ютерні засоби обробки і зберігання інформації.

Підсумовуючи, варто сказати, що проблема протидії актам інформаційного тероризму – це комплексна проблема. Сьогодні закони повинні відповідати вимогам сучасного розвитку. З цією метою урядові нашої держави необхідно проводити цілеспрямовану роботу з гармонізації та вдосконалення законодавства у сфері інформаційної безпеки держави. Державна політика забезпечення інформаційної безпеки України повинна бути складовою політики національної безпеки та повинна передбачати системну привентивну діяльність органів влади по наданню гарантій інформаційної безпеки особі, соціальним групам та суспільству в цілому. Одним з пріоритетних напрямків має бути організація взаємодії та координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх належним фінансуванням та необхідною сучасною матеріально-технічною базою. Також необхідно ставити акцент на активізації зусиль у формуванні належної міжнародної системи інформаційної безпеки. Виконання всіх цих вимог призведе до радикального зниження рівня інформаційної злочинності та тероризму, і як наслідок, призведе до підвищення інформаційної безпеки не тільки нашої держави, але й тих країн, з котрими вона співпрацюватиме.

Таким чином, властивості сучасного інформаційного тероризму є і можуть бути предметом подаль-шої наукової уваги дослідників даного складного соціально-політичного явища, котре потребує детальнішого розгляду як одна зі складових цивілізаційного процесу, а відповідну зкооперовану антитерористичну діяльність як підсистему національної та міжнародної систем безпеки.

ЛІТЕРАТУРА

1. Бондаренко В. О. Інформаційна безпека сучасної держави: концептуальні роздуми / В. О. Бондаренко, О. В. Литвиненко // Стратегічна панорама. – 1999. – № 1–2. – С. 127–133.
2. Баринов А. Информационный суверенитет или информационная безопасность? / А. Баринов // Національна безпека і оборона. – 2001. – № 1. – С. 70–76.

3. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи / В. Петрик // Юридичний журнал. – 2009. – № 5. – С. 122–134.
4. Горбулін В. П. Актуальні проблеми системного забезпечення інформаційної безпеки України / В. П. Горбулін, М. М. Биченок, П. М. Копка // Матеріали міжар. наук.-практ. конф. «Форми та методи забезпечення інформаційної безпеки держави». – К. : Нац. Акад. СБ України. – 2008. – С. 79–85.
5. Кузьменко А. М. Особливості проблем законодавчого забезпечення інформаційної безпеки держави, суспільства і громадянина в умовах інформаційно-психологічного протиборства / А. М. Кузьменко // Часопис Київського університету права. – 2010. – № 4. – С. 317–321.
6. Закон України «Про основи національної безпеки України» // Відомості Верховної Ради України. – 2003. – № 39. – Ст. – 351.
7. Указ Президента України «Про Доктрину інформаційної безпеки України» від 23 квітня 2008 року N 377 (377/2008) // [Електронний ресурс]. – Режим доступу : http://media-yuryst.com/pro_doktrynu_inform_bezpeky_ukrayiny.aspx.
8. Дурдинець В. В. Тероризм – загроза суспільству / В. В. Дурдинець // Надзвичайна ситуація. – 2001р. – № 9. – С. 29–31.
9. 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.
10. Thevenet C. Cyber-terrorisme, mythe ou réalité? / C. Thevenet // Série Mémoires et Thèse. – Université de Marne-La-Vallée. – 2005. – 57 p.
11. Надьон О. В. Правовий аналіз передумов виникнення загрози тероризму в Україні / О. В. Надьон // [Електронний ресурс]. – Режим доступу : http://pravoznavec.com.ua/period/chapter/2/24/849.
12. Бойченко О. В. Медіа-тероризм: особливості сучасних ознак інформаційній безпеці / О. В. Бойченко // Інтегровані інтелектуальні робототехнічні комплекси (ІРТК-2009): друга міжнародна наук.-практ. конф. (25-28 травня 2009 р.). – К. : НАУ, 2009. – С. 230-232.
13. Chambet P. Le cyber-terrorisme / P. Chambet // [Electronic source]. – Régime d'accès : http://www.chambet.com/publications/Cyberterrorisme.pdf.
14. Герасименко К. С. Сучасні ознаки загроз «інформаційного тероризму» / К. С. Герасименко // Форум права. – № 3. – С. 162–166.
15. Катренко А. Особливості інформаційної безпеки за міжнародними стандартами / А. Катренко // Альманах економічної безпеки. – 1999. – № 2. – С. 15–17.
16. Гуцалюк М. Інформаційна безпека України: нові загрози / М. Гуцалюк // Бизнес и безопасность. – 2003. – № 5. – С. 2–3.
17. Закон України «Про основи національної безпеки України» // Відомості Верховної Ради України. – 2003. – № 39. – Ст. – 351. Із змінами, внесеними згідно із Законом № 3200-IV (3200-15) від 15.12.2005. ВВР. – 2006. – № 14. – Ст. 116.
18. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» // Відомості Верховної Ради України (ВВР). – 2007. – № 12. – Ст. 102.

Рецензенти: ***Тригуб О. П.,*** д.і.н, професор;
Бронніков В. Д., к.і.н., доцент.

 Дата надходження статті до редколегії 14.09.2012 р.

ГЛАЗОВ Олексій Володимирович – аспірант Інституту всесвітньої історії Національної академії наук України, м. Київ, Україна.

Коло наукових інтересів: система знань про національну і міжнародну безпеку; теорія і практика боротьби з тероризмом та іншими формами екстремістської діяльності; міжнародні конфлікти.