МІЖНАРОДНЕ ПУБЛІЧНЕ ТА ПРИВАТНЕ ПРАВО

Данілова В.О.
студентка,
Кримський інститут права
Національного університету «Одеська юридична академія»

МІЖНАРОДНИЙ ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ ДЕРЖАВИ

Міжнародний тероризм належить до найбільш небезпечних і важко прогнозованих явищ, яке вирізняється особливим динамізмом і багатоплановістю, а також здатністю до адаптації й модернізації в умовах 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 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).

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 [1, с. 127].

Використання інформаційних технологій визначає структуру і якість озброєнь, необхідний рівень їх достатності, ефективність дій збройних сил держави. [2, с. 71].

Інформаційна безпеки держави – означає стан її захищеності, при якій 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].

Таким чином, інформаційна безпека стає невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки будь-якої держави.

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 обумовлено широким запровадженням інформаційно-телекомунікаційних систем у всіх сферах життєдіяльності суспільства [4, p. 98].

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 [5].

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 перенавантаження вузлів комунікації і т.п.)[6, с. 231].

Головним в 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. 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 [7].

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 в зашифрованому вигляді інструкції, карти, схеми, паролі та іншу важливу інформацію, розголошення якої може зашкодити національній безпеці держави [8, с. 165].

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 [9, с. 16].

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. В даний час для терористів легко уразливі практично всі комп'ютерні засоби обробки і зберігання інформації [10].

Підсумовуючи, варто сказати, що проблема протидії актам інформаційного тероризму – це комплексна проблема. Сьогодні нормативно-правові акти повинні відповідати вимогам сучасного розвитку. З цією метою будь-якій держави необхідно проводити цілеспрямовану роботу з гармонізації та вдосконалення законодавства у сфері інформаційної безпеки держави.

Список використаних джерел:

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. Информационньїй 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. 122134.

4. 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.

5. 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.

6. Бойченко О.В. Медіа-тероризм: особливості сучасних ознак інформаційній безпеці / О.В. Бойченко // Інтегровані інтелектуальні робототехнічні комплекси (ПРТК-2009): друга міжнародна наук.-практ. конф. (25-28 травня 2009 р.). – К.: НАУ, 2009. – С. 230-232.

7. Chambet P. Le cyber-terrorisme / P. Chambet // [Electronic source]. – Regime d'acces: http://www.chambet.com/publications/Cyberterrorisme.pdf.

8. Герасименко К.С. Сучасні ознаки загроз «інформаційного тероризму» / К.С. Герасименко // Форум права. – № 3. – С. 162-166.

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

10. Глазов О. В. Міжнародний інформаційний тероризм в контексті загроз національній безпеці України [Електронний ресурс]. – Режим доступу: http://lib.chdu.edu.ua/pdf/naukpraci/politics/2012/197-185-15.pdf