УДК 343.326:32.019.51:323.28
DOI https://doi.org/10.32782/2524-0374/2022-10/143

ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ ТА СПОСІБ ІНФОРМАЦІЙНОЇ ВІЙНИ

INFORMATION TERRORISM AS A THREAT TO NATIONAL SECURITY AND A METHOD OF INFORMATION WARFARE

Лисько Т.Д., к.ю.н.,
доцент кафедри кримінального права та процесу
Національний авіаційний університет

Клімук О.О., студентка IV курсу юридичного факультету
Національний авіаційний університет

Лисянська Д.В., студентка IV курсу юридичного факультету
Національний авіаційний університет, м. Київ

Наукова стаття присвячена дослідженню актуального питання інформаційного тероризму, що набуває характеру всесвітньої проблеми, з якою зіткнулися більшість учасників міжнародних відносин. На початку XXI століття тероризм став одним з найнебезпечніших і важкопрогнозованих явищ, що набирає найрізноманітніших виглядів. Стрімкий розвиток інформаційних технологій породив такий вид тероризму як інформаційний. Здійснено аналіз та визначені проблеми законодавчого закріплення поняття інформаційного тероризму, вказано на суттєві колізії в законодавстві України в частині регулюванні цього питання. Охарактеризовано форми та класифікацію видів інформаційного тероризму в сучасному глобальному кіберпросторі. Вказано, що інформація відіграє ключову роль у формуванні громадських та державних інститутів.

Сучасну епоху тому й називають інформаційною ерою, адже це час створення нових інформаційних технологій та одночасно запеклої боротьби за розум і свідомість людей. Інформація стала виконувати не властиву їй функцію інструменту війни. Військові дії ведуться у свідомості людей, жодне рішення не проходить без так званої «інформаційної підтримки». Нав'язування агресивних новин спричиняє панічний стан у населення і це є зброєю в руках ворога. Інформаційна війна розглядає інформацію як окремий об'єкт або як потенційну зброю та вигідну ціль. Інформаційну війну можна розглядати як якісно новий вид бойових дій, активна протидія в інформаційному просторі. Інформаційна війна – це атака інформаційної функції, незалежно від засобів, які застосовуються. У науковій статті проаналізовані деякі можливі тенденції розвитку та вдосконалення протидії інформаційному тероризму як фактору, що підриває національну безпеку України, національну свідомість суспільства. З огляду на грандіозні наслідки цього процесу для всієї земної цивілізації особливого значення повинен набути контроль за його розвитком з боку громадянського суспільства та держави.

Ключові слова: інформаційний тероризм, загроза, національна безпека, інформаційна війна, кіберпростір.

This article is devoted to the rather actual topic of information terrorism, which is becoming a global problem that most participants in international relations have faced. At the beginning of the 21st century, terrorism has become one of the most dangerous and difficult-to-predict phenomena, which takes on a wide variety of forms. The rapid development of information technologies has given rise to such a type of terrorism as information terrorism. The analysis was carried out and the legislative consolidation of information terrorism was determined, as well as significant conflicts in the legislation of Ukraine in the regulation of this issue. The forms and classification of information terrorism in modern global cyberspace are characterized. Information plays a key role in the formation of public and state institutions.

Therefore the modern era is called the information era, because it is the time of the creation of new information technologies and at the same time a fierce struggle for the mind and consciousness of people. Information began to perform an uncharacteristic function of a tool of war. Military actions are conducted in the minds of people, no decision is made without the so-called "informational support". The imposition of aggressive news causes panic in the population, and this is a weapon in the hands of the enemy. Information warfare considers information as a separate object or as a potential weapon and profitable target. Information war can be considered as a qualitatively new type of combat, active countermeasures in the information space. Information warfare is an attack on the information function, regardless of the means used. In this way, some possible trends of development and improvement of combating information terrorism as a factor undermining the national security of Ukraine and the national consciousness of society are proposed. In view of the grandiose consequences of this process for the entire earthly civilization, "the control of its development by civil society must acquire special importance."

Key words: information terrorism, threat, national security, information war, cyberspace.

Постановка проблеми. Інформація є одним з основних чинників існування та розвитку соціально-політичної системи кожної країни. У сучасному світі вона стала одним із способів маніпуляції. Це спричинили підвищення можливості інформаційного впливу на особу, суспільство та державу в цілому. Постійне масштабне розповсюдження інформації сприяє її максимально швидкій появі на великих територіях. Однозначно, це одне із найзначніших та найважливіших досягнень нашого суспільства, проте як і кожна річ у цьому світі, має свої недоліки, які можуть привести до непоправних наслідків. Наприклад, це значно збільшує можливості виникнення інформаційних загроз. Інформаційна епоха розширила сферу інформаційно-комунікативних воєн, що призвело до появи інформаційного тероризму як засобу ведення інформаційної війни, що полягає у зловживанні кіберпростором, мережами або їх компонентами з метою сприяння здійсненню терористичних операцій. Інформаційний тероризм набуває обертів у вигляді нових загрозливих форм, а його стрімке розповсюдження може стати причиною втрати суверенітету, незалежності та територіальної цілісності окремої держави.

Аналіз останніх досліджень та публікацій. Сутність інформаційного тероризму активно досліджується в працях як зарубіжних, так і вітчизняних науковців. Питаннями вивченням тероризму в умовах глобалізації, розвитку інформаційно-комунікаційних технологій та зростання ролі засобів масової інформації в житті суспільства займалися Герасименко К. С., Коршунов В. О., Катренко А., Мельник С. В., Лихова С.Я., Леонов Б.Д. та інші.

Метою і завданням наукової статті є дослідження феномену інформаційного тероризму, його характерних рис та способів протидії цьому явищу.

Виклад основного змісту. Сьогодні немає одного підходу до визначення інформаційного тероризму, різні вчені трактують його інакше і їхні погляди є досить таки пере-

конливими. Інформаційний тероризм – це в першу чергу, одна із форм негативного впливу на особу, суспільство і державу усіма видами інформації. 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 [3, с. 6]. Це різного роду погрози, дії по залякуванню окремих осіб і суспільства в цілому, є злочином з ознаками тероризування. Інші вчені вважають, що інформаційний тероризм – це здійснення або погроза здійснення за допомогою інформаційних технологій і/або інформаційної зброї вибуху, підпалу чи інших загально небезпечних діянь, що можуть спричинити загибель людей або інші тяжкі наслідки й спрямовані на залякування населення з метою спонукання держави, міжнародної організації, фізичної чи юридичної особи або групи осіб до здійснення чи відмови від здійснення якої-небудь дії.

Держава як політичний інститут є носієм загальнонаціональних образів, а виважена державна політика має серйозний вплив на формування уявлень про державу в зовнішньому інформаційному просторі, просування, трансформацію цих іміджів. Не менш важливою ланкою у цьому контексті є просування локальних образів, як таких, що є частиною політичної системи та національного дискурсу держави.

Інформаційні кримінальні правопорушення суттєво впливають на інформаційну безпеку держави не тільки через те, що ними заподіюється значний економічний збиток, але насамперед через те, що наслідком вчинення зазначених кримінальних правопорушень є порушення нормальної роботи інформаційних і комунікаційних систем, а також поширюється інформація, що має протиправний характер [4].

У Конституції України (ст. 17) закріплюється пріоритетність інформаційної безпеки, як основної функції держави, що демонструє рівень значущості інформаційних процесів та важливості протидії інформаційним загрозам [2]. 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 [7].

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 масмедіа, 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 [1, с. 163].

Одним із найефективнішим інструментом медіа-тероризму є засоби масової інформації та мережа Інтернет, які у поєднанні виступають «цементом» для інформаційного ресурсу, що здатний за абстрактною реальністю приховувати достовірну, точну та повну інформацію. Яскравим прикладом використання терористами ЗМІ та мережі Інтернет є маніпулювання думкою громади, поширення впливу на суспільство, застосування дезінформації, дискредитація офіційних органів публічної адміністрації з метою психологічного вербування соціуму та поширення однотипної інформації, що в кінцевому підсумку формує ідеологію, прийнятну для терористів.

Безперечно, головною зброєю у боротьбі з інформаційним тероризмом залишається законодавство. Протидія інформаційному тероризму як складовій терористичної діяльності ґрунтується на засадах, визначених Законом України «Про боротьбу з тероризмом» [6]: 1) законності та неухильного додержання прав і свобод людини і громадянина; 2) комплексного використання з цією метою правових, політичних, соціально-економічних, інформаційно-пропагандистських та інших можливостей; 3) пріоритетності попереджувальних заходів; 4) невідворотності покарання за участь у терористичній діяльності; 5) пріоритетності захисту життя і прав осіб, які наражаються на небезпеку внаслідок терористичної діяльності; 6) поєднання гласних і негласних методів боротьби з тероризмом; 7) нерозголошення відомостей про технічні прийоми і тактику проведення антитерористичних операцій, а також про склад їх учасників; 8) єдиноначальності в керівництві силами і засобами, що залучаються для проведення антитерористичних операцій; 9) співробітництва у сфері боротьби з тероризмом з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з тероризмом.

Протидія інформаційному тероризму правоохоронними органами України здійснюється шляхом оперативно-розшукової діяльності щодо виявлення, розкриття, профілактики окремих видів кіберзлочинів; інформаційно-аналітичної розвідки в комп'ютерній мережі, електронної телекомунікації; кримінально-процесуальної і криміналістичної діяльності щодо розкриття, розслідування злочинів і притягнення винних до відповідальності; спеціально кримінологічних заходів [5, с. 44]. 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 [8, с.114]. 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 має змогу загрожувати інформаційним системам, розташованим практично в будь-якій точці земної кулі [9]. За інформацією спеціалістів контррозвідувальних управлінь, кібертерористи за допомогою електронної пошти передають в зашифрованому вигляді інструкції, карти, схеми, паролі

та іншу важливу інформацію, розголошення якої може зашкодити національній безпеці держави.

Як відзначають науковці, основною формою кібертероризму є інформаційна атака на комп'ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші складові інформаційної інфраструктури, яка здійснюється злочинними угрупуваннями або окремими особами. Наслідком такої атаки є проникнення в інформаційно-телекомунікаційну мережу або комунікаційну інфраструктуру, перехоплення управління, пригнічення засобів мережевого інформаційного обміну та здійснення інших деструктивних дій.

Форми та прояви інформаційного тероризму варто враховувати при визначенні стану загроз інформаційного тероризму, перелік яких чинне законодавство України, на жаль, не містить [11, с. 173].

Варто зазначити, що у зв'язку з набуттям інформаційними тероризмом глобальних масштабів та його інтернаціональним характером, виникла необхідність у правовому регулюванні цього явища на міжнародному рівні. Заходи боротьби з інформаційним тероризмом повинні ґрунтуватися на єдиних законах, вироблених міжнародним співтовариством. У зв'язку з цим в грудні 1998 року Генеральна Асамблея ООН прийняла 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. Окремої уваги заслуговує Конвенція про кіберзлочинність [10], у якій акцентовано увагу на необхідності вироблення державами-учасницями спільної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності шляхом створення відповідного законодавства і налагодження міжнародного співробітництва для налагодження більшого, швидкого і ефективно функціонуючого міжнародного співробітництва у кримінальних питаннях ефективної боротьби з кіберзлочинністю.

Висновки. Підсумовуючи вищесказане, варто зазначити, що боротьба та протидія актам інформаційного тероризму – це комплексна та актуальна проблема. Наші закони повинні мати певний рівень та відповідати сучасним вимогам. Для цього, уряд та верхівка нашої держави має спланувати та проводити цілеспрямовану роботу з гармонізації та вдосконалення законодавства у сфері інформаційної безпеки держави. Україні насамперед потрібна розроблена та координована ефективна інформаційна політика, яка буде спрямована на інформування населення та забезпечення його розуміння того, в чому базуються основні причини тероризму – підвищення медіа-грамотності (вміння протистояти спробам маніпулювання собою за допомогою інформаційних потоків) та довіри до держави та інші складові, які допоможуть вибудувати систему захисту кожної людини від негативного впливу інформаційного тероризму.

Також доволі важливим фактором, який впливатиме на зменшення рівня інформаційного тероризму є створення та формування системи ціннісно-якісних рис людини за допомогою спеціальних програм, розроблених спільно із засобами масової інформації, які б стали агітацією відповідного нормалізованого способу життя, тактовного ставлення та поваги один до одного, а також соціально-культурний розвиток свідомості громадянського суспільства.

ЛІТЕРАТУРА

1. Герасименко К. С. Сучасні ознаки загроз «інформаційного тероризму». *Форум права.* 2009. № 3. С. 162-166.
2. Конституція України : Закон України від 28.06.96 р. № 254к/96-ВР. *Відомості Верховної Ради України* (ВВР). 1996. № 30. Ст. 141.
3. Коршунов В. О. Політичний тероризм: інформаційні методи боротьби : автореф. дис. …канд. політ. наук : спец. 23.00.02 «Політична інститути та процеси». Дніпропетровськ, 2008. – 18 с.
4. Кубишкін О. В. Міжнародно-правові проблеми забезпечення інформаційної безпеки держави. URL: http://pravolib.pp.ua/mejdunarodnopravovyie-problemyi-obespecheniya.html. (дата звернення 29.09.2022).
5. Мельник С.В., Тихомиров О.О., Лєнков О.С. До проблеми формування понятійно-термінологічного апарату кібербезпеки. *Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка*. ВІКНУ, 2011. С. 165-171.
6. Про боротьбу з тероризмом : Закон України від 20.03.2003 р. № 638-IV : станом на 12 черв. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/638-15#Text (дата звернення: 23.10.2022).
7. Про основи національної безпеки України : Закон України від 19.06.2003 р. № 964-IV : станом на 8 лип. 2018 р. URL: https://zakon.rada.gov.ua/laws/show/964-15#Text (дата звернення: 13.10.2022).
8. Bank R.O. Informacijnyj teroryzm jak zagroza nacional'nij bezpeci Ukrai'ny: teoretykopravovyj aspekt. Informacija i pravo. 2016. № 1(16). S. 110-116.
9. Chambet P. Le cyber-terrorisme. URL: http://www.chambet.com/publications/Cyberterrorisme.pdf. (дата звернення 20.10.2022).
10. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 р. : станом на 7 верес. 2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 13.10.2022).
11. Леонов Б., Лихова С. Інформаційний тероризм як загроза національній безпеці україни. *Scientific works of National Aviation University. Series: Law Journal «Air and Space Law»*. 2021. Т. 2, № 59. С. 170–176.