УДК 343.9
DOI https://doi.org/10.32782/2524-0374/2021-11/154

ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ І МАНІПУЛЮВАННЯ СВІДОМІСТЮ: ДЕТЕРМІНАЦІЯ ТА ЗАПОБІГАННЯ

INFORMATION TERRORISM AND CONSCIOUSNESS MANIPULATION: DETERMINATION AND PREVENTION

Пивоваров В.В., к.ю.н., доцент,
доцент кафедри кримінології та кримінально-виконавчого права
Національний юридичний університет імені Ярослава Мудрого

Пархоменко А.Ю., студентка ІІ курсу магістратури
господарсько-правового факультету
Національний юридичний університет імені Ярослава Мудрого

ХХІ століття характеризується стрімким розвитком інформаційних технологій, які поряд із тим, що полегшують доступ до інформації, також надають широкі можливості для маніпулювання цією інформацією. У статті автори аналізують поняття та види інформаційного тероризму, а також їх основні причини.

Нині інформація набуває все більшого значення, а отримати інформацію про ті чи інші події в різних сферах суспільного життя стає дедалі простіше. Однак занепокоєння викликає той факт, що не всі схильні критично оцінювати, перевіряти чи порівнювати інформацію, яку споживають. Зазначене надає широке поле для маніпулювання свідомістю пересічних громадян шляхом перекручування та спотворення інформації про ті чи інші події.

Розрізняють кібертероризм і медіаінформаційний тероризм. Чинний Кримінальний кодекс України не містить окремого складу злочину, який би стосувався інформаційного тероризму чи кібертероризму, унаслідок чого в осіб, які вчиняють такі діяння, може скластися оманливе враження щодо безкарності їхніх діянь, а тому випадків інформаційного тероризму стає дедалі більше. Унаслідок того, що кібертероризм належить до кіберзлочинів, він має високий ступінь латентності, оскільки особу злочинця встановити дуже складно.

Вищевказане підвищує суспільну небезпечність такого явища як інформаційний тероризм, його негативний вплив на суспільство й окрему особу, яка стала жертвою злочинного посягання.

Проаналізовані причини та передумови появи такого явища, як інформаційний тероризм, це, зокрема, стрімкий розвиток інформаційних технологій, відносна легкість скоєння, оскільки кіберзлочини не потребують фізичної присутності поруч із жертвою, планування в часі, можуть бути вчиненні миттєво, а також низький рівень культури споживання інформації. Однак є шляхи зменшення випадків і негативного впливу інформаційного тероризму, що свідчить про те, що суспільство може та має боротися із зазначеним явищем.

Ключові слова: інформація, маніпулювання свідомістю, інформаційний тероризм, кіберзлочинність.

The 21'st century is characterized by the rapid development of information technologies, which, on the one hand, facilitates access to information, but on the other hand, provides wide opportunities for manipulating such information. The authors analyze the concepts and types of information terrorism and its causes.

Currently, information is becoming increasingly important. Obtaining information about events in various spheres of public life is not a problem. However, it is a matter of concern that not everyone tends to critically evaluate, verify or compare the information they consume. This provides a wide field for manipulating of consciousness of ordinary citizens by distorting information about certain events.

There are two types of information terrorism cyberterrorism and media terrorism. The Criminal Code does not contain a separate corpus delicti related to information terrorism or cyberterrorism as a result, people who commit such acts may have a misleading impression of the impunity of their acts. Therefore the number of cases of information terrorism is increasing.

The abovementioned increases the social danger of such phenomenon as information terrorism, its negative impact on society and the individual who has become a victim of criminal encroachment.

The authors analyzes the causes and preconditions for the existence of such phenomenon as information terrorism. Such causes are the rapid development of information technologies, the relative ease of commission, as cybercrime does not require physical presence with the victim, time planning, can be committed instantly, and low consumption culture information. However, there are ways to reduce the incidence and negative impact of information terrorism, which indicates that society can and should combat this phenomenon.

Key words: information, manipulation of consciousness, information terrorism, cybercrime.

Постановка проблеми. ХХІ ст. позначилося стрімким розвитком інформаційних технологій, який із кожним днем набирає обертів. Нині злочини в галузі інформаційних технологій є дуже поширеними, а їх розкриття є досить складним процесом та потребує зусиль правоохоронних органів. Україна, як і всі країни світу, час від часу стикається з такими кримінальними викликами, як кібератаки на приватні і державні установи, банківські установи, реєстри виборців і системи голосування, захищені мережі об'єктів критичної інфраструктури тощо.

Проте очевидно, що мережа Інтернет дозволяє маніпулювати інформацією, водночас ускладнює процес установлення особи злочинця, а також притягнення його до відповідальності. У світовій інформаційній та мережевій війні кібертероризм став критичною проблемою, оскільки такий тероризм не тільки завдає шкоди державним і комерційним інтересам, але й загрожує громадянам, які за певних обставин і через відсутність необхідних знань можуть стати жертвою інформаційного тероризму.

Аналіз останніх досліджень і публікацій. Темі кіберзлочинності в Україні і світі присвячено багато наукових праць сучасних зарубіжних і вітчизняних науковців, зокрема, у контексті нашого дослідження заслуговують на увагу наукові праці та дослідження В.А. Кротюка, О.С. Геращенка, І.І. Кольцової, А.М. Митка, Л.Р. Наливайко, В.В. Пивоварова, В.І. Рюміної, О.В. Саган, М.П. Стрельбицького, С.Л. Саржан, О.В. Таволжанського й інших науковців. Нині сфера технологій розвивається дуже швидко, однак пов'язана із цим проблема поширення впливу на свідомість значною мірою залишається поза увагою кримінологів, саме тому зазначена тема потребує подальшого опрацювання, дослідження і популяризації серед науковців та студентської молоді.

Метою статті є кримінологічний аналіз явища інформаційного тероризму, його основних проявів, тенденцій, детермінант, а також поширення протиправного інформаційного терористичного впливу на свідомість, розгляд заходів запобігання їм.

Виклад основного матеріалу. У XXI ст. в переліку загроз національній безпеці тероризм розглядається державами як найнебезпечніше явище, яке важко прогнозувати і з яким важко боротися через його особливості [1]. Інформаційний тероризм органічно пов'язаний з іншими явищами, які є породженням сучасного техногенного розвитку цивілізації. Так, у науковій літературі представлені різноманітні погляди на розуміння природи й особливостей інформаційного насильства, інформаційної безпеки, інформаційної війни, інформаційного тероризму, його відмінностей від «класичного» тероризму, визначення характерних рис і особливостей даного феномену в умовах гібридної війни [2].

Зокрема, В.І. Рюміна характеризує поняття та мету інформаційного тероризму, визначає його як форму негативного впливу на особистість, суспільство і державу всіма видами інформації. Метою інформаційного тероризму є ослаблення і розхитування конституційного ладу [3].

Інформаційний тероризм визначається як умисне зловживання цифровими інформаційними системами, мережами або іншими технологічними розробками. Мета такого зловживання – здійснення терористичних операцій або атак [4].

Інформаційний тероризм часто ототожнюють із кібертероризмом, хоча, звичайно ж, вони – дві частини одного явища. Інформаційний тероризм передбачає цілеспрямовані маніпуляції з інформацією або її підтасування, а іноді й подачу свідомо неправдивих фактів, унаслідок чого відбувається залякування населення, поширюється паніка, настрої параноїдальних думок [5]. Уважаємо таке ототожнення недоцільним, оскільки сучасна наукова доктрина виокремлює два види інформаційного тероризму: кібертероризм і медіаінформаційний тероризм.

В.В. Пивоваров визначає кіберзлочинність як сукупність злочинів, учинених у кіберпросторі за допомогою або з опосередкованим використанням комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору, у межах комп'ютерних систем або мереж, а також проти комп'ютерних систем або мереж і комп'ютерних даних [6].

Зарубіжні вчені надають таке визначення кібертероризму, який є різновидом інформаційного тероризму. Кібертероризм – це особливий вид тероризму, де «місцем» або «засобом» його здійснення є кіберпростір, водночас кіберпростором є глобальна взаємопов'язана мережа цифрових інформаційних та комунікаційних інфраструктур, під якою зазвичай розуміють інтернет і комп'ютерні мережі. Поняття кібертероризму є дуже широким і може описувати різні дії, зокрема просте поширення пропаганди в інтернеті або зміну/знищення інформації, навіть проведення терористичних атак за допомогою комп'ютерних мереж [7].

Отже, під кібертероризмом варто розуміти сукупність дій, які полягають в інформаційній атаці на комп'ютерну інформацію, обчислювальні системи, пристрої передачі даних, інші складники інформаційної інфраструктури. Зазначені дії можуть здійснюватися як злочинними угрупованнями, так і окремими особами.

Чинний Кримінальний кодекс України не містить окремого складу злочину, який би стосувався інформаційного тероризму чи кібертероризму. Однак національну правову базу щодо врегулювання кіберправовідносин становлять деталізовані нормативні акти: Конституція України, яка гарантує захист інформації, Кримінальний кодекс України, Конвенція Ради Європи «Про кіберзлочинність», закони України «Про телекомунікації», «Про Національну поліцію», «Про основи національної безпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», укази Президента України, інші нормативно-правові акти [8].

Варто звернути увагу на особливу спрямованість кібертероризму, яка полягає у проникненні в інформаційно-телекомунікаційну систему, перехопленні управління, пригніченні засобів мережевого інформаційного обміну тощо. Заслуговує на увагу позиція Дороті Денінга, експерта американського Центру досліджень тероризму, яка визначила кібертероризм як елемент класифікації терористичної діяльності в мережі Інтернет, визначає його як комп'ютерні атаки, сплановані з метою завдання максимальних збитків життєво важливим об'єктам інформаційної інфраструктури [9]. Небезпека такого виду інформаційного тероризму полягає в тому, що він не має національних меж (терористичні акції можуть здійснюватися з будь-якої точки світу), у проблематичності виявлення терориста в інформаційному просторі, адже хакери здійснюють терористичну діяльність зазвичай не з особистих комп'ютерів, що ускладнює ідентифікацію злочинця та його місцезнаходження.

Під медіаінформаційним тероризмом розуміють діяльність груп або цілих структур терористичного спрямування, які мають політичний характер. Така діяльність націлена на те, щоб знищити чи послабити інфраструктуру суспільства, зруйнувати соціальні системи чи політичні режими. Нині, в умовах зростання як внутрішніх, так і зовнішніх загроз, необхідно спрямувати зусилля на розроблення політики протидії інформаційному тероризму в Україні. Така політика має ґрунтуватися на таких аспектах, як: посилення комунікативного складника антитерористичної діяльності структур сектору безпеки; удосконалення інформаційної політики держави з урахуванням специфіки гібридної війни; удосконалення нормативно-правової бази; виховання інформаційної культури в молоді; інкорпорування потенціалу громадянського суспільства і суспільного телебачення в систему протидії медіаінформаційному тероризму; розвиток міжнародного співробітництва [1].

Медіатероризм має наслідком такий негативний вплив, коли кожен окремий індивід стає нездатним самостійно зорієнтуватися в інформаційному просторі, який фактично нині є необмеженим. Масмедіа мають практично необмежені інструменти для того, щоб будувати недостовірну інформаційну реальність, наповнену фейковими новинами. Завдання такої недостовірної реальності – перекручування істини, її приховування. Отже, натепер кількість інформації, безумовно, не свідчить про якість такої інформації, а тому будь-яка новина вимагає критичного її осмислення індивідом [10].

Медіаінформаційний тероризм нині є характерним не тільки для ЗМІ, а спостерігається й у соціальних мережах. Науковці підкреслюють, що один із найважливіших аспектів проблеми – стан правопорядку, нормативно-правового забезпечення заходів боротьби із протизаконним впливом негативного контенту в соціальних мережах [11].

Отже, інформаційний тероризм є великою загрозою, оскільки впливає на суспільну свідомість і здатен впливати на суспільну думку. Пересічні громадяни не завжди критично оцінюють інформацію, яку отримують із різноманітних джерел, а тому інформаційний тероризм має вкрай негативні наслідки для суспільства та держави.

До характерних рис сучасного інформаційного тероризму варто віднести такі:

– публічність, оскільки здійснюється зазвичай із застосуванням масмедіа, інтернет-медіа. Технологічний прогрес і розвиток засобів масової комунікації вимагають переосмислення значення ролі ЗМІ в суспільстві, усвідомлення значущості характеру, форм і методів подачі інформації в управлінні суспільною свідомістю;

– пов'язаність із технологічним прогресом та розвитком нових технологій;

– здійснення суто шляхом застосування інформаційних та цифрових технологій.

Окремо науковці М.П. Стрельбицький та С.Л. Саржан виділяють такі специфічні риси інформаційного тероризму:

– високий ступінь латентності вчиненого діяння, легка конспірація замовників, джерел фінансування та виконавців;

– швидка ескалація, завдяки якій забезпечується миттєве досягнення запланованої мети;

– реальність загрози органам державної влади, державі, державному устрою, законності, суспільству, спричинення нестабільності та хаосу в суспільстві;

– легка контрольованість із боку замовника чи виконавця, оскільки через те, що зазначені злочини вчиняються віддалено, можна оперативно вносити корективи ззовні;

– такі дії є дешевими за вартістю, не потребують значних вкладень, однак масштабні за охопленням і відчутні за наслідками;

– можуть безпосередньо вплинути на ухвалення політичних і управлінських рішень;

– групують і об'єднують населення навколо певних ідей та лідерів або проти них [2].

Нагальні детермінанти інформаційного тероризму, на нашу думку, полягають у площині світових кризових явищ, що нині поглиблюються. Суспільство втрачає важелі регулювання складних соціально-політичних процесів, політичні ідеали та моральні цінності змінюються, широкі верстви населення все частіше залучаються до активного політичного життя, не маючи водночас належних знань і обґрунтованих уявлень щодо справжніх витоків і причин тих чи інших подій політичного життя. А тому об'єктивно зростає прагнення мати важелі впливу на суспільну думку, дієві можливості швидкого групування мас населення навколо певних ідей або проти них. Розглядаючи численні умови інформаційного тероризму, обов'язково варто підкреслити: зазначені діяння відносно легко вчинити, скоординувати чи змінити план дій у разі виникнення якихось непередбачуваних ситуацій. Розвиток інформаційних технологій та технологічний прогрес відкрили фактично необмежені можливості для маніпулювання інформацією навколо різноманітних сфер суспільного чи політичного життя. Звичайно, за задумом, розвиток технологій мав працювати лише на благо суспільства, однак, на жаль, нині може бути використаний і проти суспільства, конкретної особи, держави чи навіть низки держав.

Інформаційний тероризм має негативні наслідки для держави та суспільства, проблема загострюється внаслідок нездатності чи не напрацювання навичок критичного мислення у значної частини населення, яке масово і некритично споживає різноманітний інформаційний контент, а тому поширення, наприклад, фейкових новин у суспільстві нині є надто легким процесом.

Серед низки заходів ефективного протистояння і запобігання загрозам інформаційного тероризму вважаємо за необхідне виділити такі:

– варто уніфікувати та гармонізувати національне законодавство з міжнародними стандартами, а саме закріпити у Кримінальному кодексі України склади злочинів, які становитимуть інформаційний тероризм (кібертероризм та медіаінформаційний тероризм);

– продовжувати наукові комплексні кримінологічні дослідження та розробки методик і способів виявлення інформаційного тероризму, можливого оперативного припинення таких діянь;

– підвищувати ефективність роботи департаменту кіберполіції НП України й інших правоохоронних структур цього спрямування;

– удосконалювати і розвивати міжнародну організаційно-правову взаємодію, яка стосується різноманітних аспектів протидії кіберзлочинності й інформаційному тероризму, оскільки інформаційний тероризм часто має транснаціональний характер, як наслідок, негативний вплив на країни і континенти;

– підвищувати загальний рівень інформаційної культури і безпеки населення, рівень правової культури, а серед молоді – у закладах освіти стимулювати навички критичного мислення та культури споживання медіаконтенту.

Висновки. Інформаційний тероризм є складним явищем, його не можна прямо ототожнювати з кібертероризмом, оскільки останній є лише одним із його видів. Інформаційний тероризм є значно ширшим та включає в себе ще таке поняття, як «медіаінформаційний тероризм». Інформаційний тероризм є великою загрозою, оскільки впливає на суспільну свідомість і здатен впливати на суспільну думку. Через поширену некритичність мислення значних верств населення інформаційний тероризм становить серйозну загрозу для суспільства та національної безпеки.

Потребує розроблення ефективна система протидії та запобігання інформаційному тероризму. Її розроблення вимагає спільних зусиль державних інституцій, закладів освіти всіх рівнів та громадян, потребує об'єднання зусиль на міжнародному рівні через транснаціональний і корпоративний характер інформаційного тероризму.

ЛІТЕРАТУРА

1. Саган О.В. Протидія медіаінформаційному тероризму як питання національної безпеки України : дис.. … канд. політ. Наук : 21.01.01. Київ, 2021. 224 с.

2. Війни інформаційної епохи: міждисциплінарний дискурс : монографія / за ред. В.А. Кротюка. Харків : ФОП Федорко М.Ю., 2021. 558 с.

3. Рюміна В.І. Інформаційний тероризм як інструмент зовнішньої політики держави на сучасному етапі. *Україна в системі глобального інформаційного обміну: теоретико-методологічні аспекти дослідження і підготовки фахівців :* матеріали Всеукраїнської науково-практичної конференції, м. Львів, 27 травня 2011 р. Львів : Видавництво Львівської політехніки, 2011. С. 267–269.

4. Jerrold M. From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism. *Terrorism and Political Violence*. 2007. P. 97–122.

5. Стрельбицький М.П., Саржан С.Л. Соціальні передумови (юридичні факти) інформаційного тероризму та кіберзлочинів. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2014. № 2. С. 217–226.

6. Пивоваров В.В., Лисенко С.Ю. Кіберзлочинність: кримінологічний погляд на генезис явища та шляхи запобігання. *Право і суспільство*. 2016. № 3. С. 177–182.

7. Lux Mayer Laura. Defining cyberterrorism. *Revista chilena de derecho y tecnología*. 2017. № 2. URL: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842018000200005 (дата звернення: 20.11.2021).

8. Таволжанський О.В. Кримінологічні аспекти кіберзлочинності у сучасних умовах. *Журнал східноєвропейського права*. 2016. № 31. С. 80–86. URL: https://inlnk.ru/n065n (дата звернення: 20.11.2021).

9. Геращенко О.С. Кібертероризм як фактор загрози національній безпеці України: ґенеза поняття та шляхи протидії. *Південноукраїнський правничий часопис*. 2016. № 3. С. 39–42.

10. Митко А.М., Кольцова І.І. Інформаційний тероризм як інструмент впливу на інформаційний конформізм у глобальному середовищі. *Політичне життя*. 2018. № 2. С. 135–139. URL: https://jpl.donnu.edu.ua/article/view/5966 (дата звернення: 20.11.2021).

11. Пивоваров В.В. Деструктивний контент у соціальних мережах як фактор криміногенного впливу на суспільну свідомість. *Право і суспільство*. 2019. № 6. С. 131–137.