***УДК 343.3:341.4***

***Ілляшенко Алла Віталіївна –***
*к. держ. упр., ст. викладач кафедри судочинства та міжнародного права Сумського державного університету*

***Alla V. Illiashenko –***
*candidate of public administration, senior lecturer of the department of justice and international law, Sumy State University (2, Rymskoho-Korsakova Str., Sumy, Ukraine)*

***Кіяшко Юрій Михайлович –***
*студент Сумського державного університету*

***Yurii M. Kiiashko –***
*student of Sumy State University (2, Rymskoho-Korsakova Str., Sumy, Ukraine)*

# Інформаційний тероризм як злочинна діяльність міжнародного масштабу

*У статті розглядається інформаційний тероризм як міжнародне явище. Доведено, що ця злочинна діяльність має серйозну загрозу як для окремих груп людей, так і для національної безпеки держав. Надано характеристику змісту інформаційного тероризму, проаналізовано загрози, які створює ця діяльність. Розкрито сутність основних видів інформаційного тероризму: медіа- та кібертероризму. Наголошено на необхідності активної міжнародної співпраці для боротьби із інформаційним тероризмом.*

***Ключові слова**: інформаційний тероризм, кібертероризм, медіа-тероризм, інформаційна атака, маніпулювання свідомістю.*

*В статье рассматривается информационный терроризм как международное явление. Доказано, что эта преступная деятельность имеет серьезную угрозу как для отдельных групп людей, так и для национальной безопасности государств. Охарактеризованы содержания информационного терроризма, проанализированы угрозы, которые создает эта деятельность. Раскрыта сущность основных видов информационного терроризма: медиа и кибертерроризма. Отмечена необходимость активной международного сотрудничества для борьбы с информационным терроризмом.*

***Ключевые слова**: информационный терроризм, кибертерроризм, медиа-терроризм, информационная атака, манипулирование сознанием.*

***A.V. Illiashenko, Yu.M. Kiiashko Information Terrorism as an International Criminal Activity***

*The article deals with information terrorism as an international phenomenon which is a combination of physical violence and criminal use of information systems. Terror activities in information sphere aim at intimidation of population, creating an atmosphere of fear and panic, forming a feeling of a threat, causing a public resonance and consequences which are threatening to life and health of people etc. The article proves that this criminal activity has a serious threat to both a certain group of people and the national security of the states. The content of information terrorism has been defined. Threats which are caused by these activities have been analyzed. It has been determined that information terrorism is presented by computer economic crimes as well as dissemination of secret information. Attributes of acts of terrorism in informational sphere have been analyzed. Information terrorism has a covered preparation and execution, is characterized by a large range and synchronicity of attacks, remoteness and internationality. The essence of the main types of information terrorism such as media- and cyberterrorism have been investigated. Under media-terrorism the authors understand a*

*focused, planned, systematical use of mass media opportunities to create and distribute the feelings fear and its dissemination in information space to manipulate a public opinion. Media-terrorism can be public and covert. The main areas of media terrorism have been separated out. They are psychological and ideological influence on public opinion, search for resources and investments, collection and posting of information, coordination of activities and planning of acts of terror attacks. Cyber terrorism is an illegal attack or a threat of terror to the computers, networks or information in order to make authorities assist terrorists to achieve political and social goals. Two types of cyberterrorism have been dealt with. They are commission of terror actions through computers and computer networks and the use of cyberspace by terror groups for organizational and communication goals. Attention has been drawn to active international cooperation to fight against information terrorism.*

***Keywords:*** *information terrorism, cyberterrorism, media-terrorism, information attack, manipulation of consciousness.*

**Постановка проблеми.** Невід'ємним атрибутом сучасної глобалізаційної політики у сфері міжнародних інформаційних відносин є використання інформаційно-комунікативних технологій, що підвищує залежність учасників міжнародного спілкування, кожного конкретного індивіда від надійності функціонування всіх елементів інформаційної інфраструктури. При цьому існує ймовірність загрози використання таких технологій у деструктивних іноді протиправних цілях, а усталена тенденція динамічного розвитку технологічних інновацій та запізніла реакція міжнародних та національних законотворчих інститутів тільки розширюють спектр можливостей її вчинення. Однією з таких загроз є інформаційний тероризм, який, в епоху глобалізації, є одним із найнебезпечніших, постійно еволюціонуючих явищ.

**Аналіз останніх досліджень і публікацій.** Окремі аспекти проблеми правового регулювання інформаційного тероризму були предметом дослідження у працях таких вчених як А. Фороса, В. Ліпкана, К. Герасименка, О. Бойченка, О. Глазова, О. Грицун, Т. Яцик та інших дослідників.

**Невирішені раніше проблеми.** Відсутність чіткої межі між використанням інформаційних технологій у воєнних чи кримінальних цілях та інформаційним тероризмом як злочинним діянням, а також відсутність нормативно-правового закріплення поняття «інформаційний тероризм» у міжнародних та національних нормативно-правових актах призводять до неможливості боротьби із такою злочинною діяльністю правовими засобами.

**Мета.** Метою статті є загальна характеристика та розкриття сутності і видів інформаційного тероризму як злочинної діяльності міжнародного масштабу.

**Виклад основного матеріалу.** Протягом останнього десятиліття інформаційний тероризм розглядається як відносно нове багатоаспектне політико-правове явище, що постійно еволюціонує, чим зумовлена відсутність законодавчо закріпленого поняття в міжнародних чи національних актах. У наукових колах під дефініцією «інформаційного тероризму» розуміється 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 [1, с. 98].

Основні труднощі у визначенні та нормативному закріпленні єдиної дефініції «інформаційного тероризму» полягає у подвійній ролі інформаційно-комунікаційних технологій. З одного боку такі технології та системи можуть розглядатися в якості об'єкта нападу, з іншого – як знаряддя для здійснення терористичних атак. Тому, як зазначає О. Грицун, виникає складність у встановленні чіткої межі між інформаційним тероризмом і використанням інформаційних технологій у воєнних чи кримінальних цілях. Основними відмінностями інформаційного тероризму від інших протиправних діянь в інформаційній сфері є його цілі, що притаманні й терористичним актам в загальному їх розумінні. До таких цілей відносять:

- залякування населення;
- створення атмосфери страху та паніки;
- формування відчуття загрози повторення

теракту;

- виклик великого суспільного резонансу;
- наслідки, небезпечні для життя та здоров'я людей;
- поширення інформації про теракт для широкої аудиторії [2, с. 312].

Ґенеза інформаційного тероризму, першочергово, зумовлена створенням нових й модифікацією існуючих видів інформаційно-комунікативних технологій, внаслідок чого, нерідко, розширюється арсенал знарядь та способів для здійснення терористичних атак. Не менш важливу роль у питанні розвитку даного явища відіграє утвердження та реалізація демократичних принципів (свободи слова, інформації тощо) й активна глобалізація інформаційних відносин, яка на сучасному етапі розвитку суспільства й світового господарства має вагомий вплив на всі сфери життєдіяльності.

На думку вітчизняних дослідників проблем тероризму інформаційний тероризм проявляється у формах комп'ютерних економічних злочинів, а також розголошення таємної інформації. Першу форму інформаційного тероризму складають:

- махінації та маніпулювання системами обробки даних (несанкціонований переказ грошей та їх використання);
- шпигунство (проникнення на конфіденційні канали зв'язку державних органів для здобуття інформації, шпигунство для здобуття закритих технологій);
- диверсія (завдання шкоди технічному та програмному забезпеченню вірусами, що порушує функціонування державних органів та інших установ);
- незаконне користування комп'ютерними послугами.

Розголошення таємниці нерозривно пов'язані з першим видом. Це отримання комерційної та конфіденційної інформації, яка на законних підставах зберігається власником у режимі таємності. Таке розголошення включає в себе:

- несанкціоноване здобування інформації для нецільового її використання особами, які не мають відповідного доступу;
- незаконний збір та переховування інформації;
- порушення правил користування конфіденційною інформацією [3, с. 258].

Характерними рисами терористичних актів в інформаційній сфері науковці визначають:

- прихований характер підготовки та реалізації таких діянь – відсутність проявів та слідів проникнення;
- масштабність атак – нанесення удару по великій кількості об'єктів;
- синхронність атак – вони можуть бути здійснені одночасно по багатьом об'єктам;
- віддаленість – джерело атаки може знаходитись за межами країни, в якій здійснюється напад;
- інтернаціональність – шкода може поширюватись на території кількох держав [4, с. 287-288].

Такий перелік ознак не є вичерпним та свідчить про особливу складність у питанні виявлення ключового джерела небезпеки, яке може знаходитися майже в будь-якій точці світу, при цьому здійснювати інформаційні атаки на один чи декілька об'єктів. Здійснюючи такі напади терористи завдають шкоди міжнародним, національним чи регіональним системам безпеки тієї чи іншої держави.

Найбільш поширеними проявами сучасного інформаційного тероризму, на думку вчених є:

- інформаційно-психологічний тероризм (медіа-тероризм) – контроль над ЗМІ з метою поширення дезінформації, чуток, демонстрації могутності терористичних організацій;
- інформаційно-технічний тероризм (кібертероризм) – завдання збитків окремим елементам і всьому інформаційному середовищу супротивника в цілому: руйнування елементної бази, активне придушення ліній зв'язку, штучне перезавантаження вузлів комунікації тощо [5, с. 231].

Медіа-тероризм є однією з найбільш поширених форм інформаційного тероризму, розвиток якого пов'язаний зі стрімким розвитком інформаційних технологій, у тому числі й зі зростанням ролі медіа (мас-медіа), створюючи можливості використання таких технологій зацікавленими особами чи організаціями для реалізації власних ідей, зокрема для умисного здійснення діяльності терористичного змісту. Під медіа-тероризмом розуміють цілеспрямоване, планомірне, систематичне використання можливостей засобів масової

інформації для створення й тиражування почуттів страху (жаху, занепокоєння, тривоги) і розповсюдження їх в інформаційному просторі з метою маніпулювання суспільною свідомістю [6, с. 32].

Сучасні ЗМІ, які мають можливість здійснювати необхідну маніпуляцію шляхом трансформації інформаційних даних, є ключовим знаряддям для впливу на свідомість суспільства незалежно від їх місця знаходження. Необхідно зауважити, що з метою посилення ефективності здійснення такого різновиду терористичних актів часто використовуються найсучасніші наукові досягнення, що посилює резонуючий вплив на громадську думку, одночасно реалізуючи власні цілі зацікавлених сторін. Використання новітніх інформаційно-комунікативних технологій для здійснення медіа-терористичних атак, з одного боку, створює додаткові гарантії реалізації необхідної цілі, а з іншого – створює нові виклики перед світовою спільнотою у виробленні та законодавчому закріпленні механізмів його протидії.

Медіа-тероризм, як відзначає В. Циганов, здійснюється у відкритій (пропаганда, реклама, агітація, інформаційні повідомлення) і прихованій (аудіо- і відео- сугестія, тобто звукове та візуальне навіювання, нейролінгвістичне програмування та інші психотехнології) формах. Основою і одночасно спільною рисою цих форм медіа-терористичного маніпулювання індивідуальної і суспільної психіки виступає дезінформація як формування та масове поширення на інформаційних каналах недостовірної, спотвореної або тенденційно підібраною інформації для впливу на оцінки, наміри і орієнтацію населення, політичних лідерів і керівників [6, с. 25].

На сучасному етапі до основних напрямів постійної медіа-терористичної діяльності належать такі методи, як:

1. Психологічний та ідеологічний вплив на свідомість мас. Виокремлюють кілька форм (типів) психологічних терористичних атак: дезінформація, страх і паніка, суспільний шок, демонстрація своїх дій, увага мас-медіа. При цьому використовуються, як правило, три основні прийоми: 1) посилання на безвихідь, що веде до такого типу боротьби (імперативність терору); 2) демонстрація насилля як протидія насиллю могутніших країн (наприклад, замість відомого імідж-виразу «Бен Ладен – терорист № 1» з'явився зворотний «Буш – терорист № 1», що добре сприймається широким колом навіть не прихильників терору); 3) використання гасел ненасилля, спрямованих до жалю, та інших свідомих методів порушення правил доведення чи спростування, що відомі з теорії аргументації чи логіки.

2. Пошук ресурсів, засобів, інвестицій, резервів та прибічників, а саме сайтів, що змушують добровільно віддавати та вкладати фінансові ресурси (як номінальні банкноти, так і «мережеві» гроші й інші цінності):

- благодійних релігійних та інших сайтів-посередників;
- виявлення користувачів сайтів для майбутньої з ними співпраці;
- сайтів з вербовки;
- збору інформації та даних;
- оперативної інформації, що може призводити до масових протестів у всьому світі релігійно налаштованих громадян;
- організації масових заворушень.

3. Збір та розміщення інформації здійснюються через пошук та аналіз мап, схем, планів, місць особливо небезпечних об'єктів, отруйних та інших речовин, боєприпасів тощо. Проводиться інструктаж прихильників («Посібник терориста», «Поварна книга терориста, анархіста» тощо).

4. Координація дій та планування терактів. Використання досягнень ІТ для спрощення, здешевлення та ефективності завуальованої координації шляхів, використання відео- та аудіо- можливостей засобів масової комунікації [7].

Наступним, найбільш поширеним проявом інформаційного тероризму, є кібертероризм, який характеризують як протиправну атаку або загрозу атаки на комп'ютери, мережі або інформацію, що знаходиться в них, здійсненою з метою примусити органи влади до сприяння в досягненні політичних чи соціальних цілей [8, с. 48]. На основі наведеної дефініції Є. Роговский виділяє два види кібертероризму:

- безпосереднє вчинення терористичних дій за допомогою комп'ютерів та комп'ютерних мереж;
- використання кіберпростору терористичними групами в організаційно-комунікаційних цілях і з метою шантажу, але не

для безпосереднього здійснення терактів [9].

Перший характеризує поєднання понять «кіберпростір» і «тероризм» тахарактеризується як умисна атака на електронні обчислювальні машини, комп'ютерні програми, мережі чи оброблювані ними інформаційні дані,створюючи небезпеку смерті населення, заподіяння майнової шкоди чи настання інших суспільно небезпечних наслідків.

Другий вид кібертероризму – використання інформаційного простору терористичними групами в організаційно-комунікаційних цілях (але не для безпосереднього здійснення терактів), проведення теоретичного, військового, теологічного навчання та пропаганди, а також рекрутування нових членів і забезпечення зв'язку між окремими осередками. При цьому, як зазначає дослідник, існує кілька способів, за допомогою яких терористичні групи використовують Інтернет у своїх цілях:

- збір інформації, необхідної для планування терактів;
- збір коштів для підтримки терористичних рухів (в тому числі, шляхом вимагання і шантажу);
- поширення агітаційно-пропагандистської інформації про терористичні рухи, їхні цілі і завдання, намічені дії, форми протесту, звернення до масової аудиторії з повідомленнями про визнання своєї відповідальності за скоєні терористичні акти і т. п.;
- інформаційно-психологічний вплив на населення з метою шантажу, створення паніки, поширення дезінформації і тривожних чуток;
- організаційна діяльність: наприклад, розміщення у відкритому доступі і розсилка відкритих і зашифрованих інструкцій (інформації про вибухові речовини і вибухові пристрої, отрути, отруйні гази, а також інструкцій щодо їх самостійного виготовлення), повідомлень про час зустрічей зацікавлених людей та ін.;
- анонімне залучення до терористичної діяльності співучасників, наприклад хакерів і представників бізнесу, які надають різні інформаційні послуги на комерційній основі і не віддають собі звіту в тому, хто і чому ці послуги оплачує;
- зростаючі технологічні можливості застосування комунікаційних технологій для планування та координації своїх дій, що створює основу для переходу до менш чітким організаційним структурам, розширення потенціалу малих терористичних груп, навмисних здійснювати свої операції децентралізовано [9].

Небезпека даного різновиду інформаційного тероризму також полягає у відсутності державних меж (такі акти можуть бути здійснені з різних точок земної поверхні). Також виникає складність у виявленні терориста, адже нерідко він вчиняє акти через один або декілька «підставних»комп'ютерів, що суттєво ускладнює як його ідентифікацію так і встановлення місця перебування.

Потенційно у майбутньому кібертероризм може перерости в одну із найбільших загроз людства,що безпосередньо пов'язано з активним впровадженням інформаційно-комунікативних технологій у всі сфери життєдіяльності суспільства. Унаслідок вчинення кібер-атак можуть виникати негативні з політичної чи економічної точки зору, наслідки як на локальному чи державному, так і міжнародному рівнях. Зовнішні кібер-атаки можуть переслідувати різні за значенням для світової чи національної безпеки цілі, а об'єктами таких атак можуть бути як інформація з обмеженим широкому загалу доступом, так і необхідне технічне устаткування для контролю над воєнними комплексами, електростанціями та іншими об'єктами стратегічно важливого значення.

**Висновки.** Інформаційний тероризм, залишаючись малодослідженим явищем, є однією з найбільших загроз сучасності. Основна небезпека такого прояву терористичної діяльності пов'язана зі стрімким розвитком інформаційно-комунікативних технологій та відсутністю необхідної нормативної бази, що створює складність при відмежуванні такого явища від інших до нього подібних. Найбільш поширеними проявами інформаційного тероризм є медіа-тероризм та кібертероризм кожен з яких несе загрозу не тільки державній, а й міжнародній безпеці.

**Список використаних джерел:**

1. Jerrold M. From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism / M. Jerrold // NATO Library Terrorism and Political Violence. – Summer 2000. – Vol. 12. – № 2. – Pp. 97-122.

2. Грицун О. Питання міжнародно-правового регулювання інформаційного тероризму [Електронний ресурс] / О. Грицун. – 2014. – Режим доступу : http://kul.kiev.ua/images/chasop/2014_4/CHAS14_4.pdf.

3. Форос А. Інформаційний тероризм, як загроза національній безпеці України [Електронний ресурс] / А. Форос. – 2010. – Режим доступу : http://liber.onu.edu.ua:8080/bitstream/123456789/6850/1/256-261ф.pdf.

4. Недильниченко В. Информационные угрозы в контексте противодействия терроризму [Електронний ресурс] / В. Недильниченко // Материалы третьей международной научной конференции по проблемам безопасности и противодействия терроризму. – 2008. – Режим доступу : http://www.iisi.msu.ru/UserFiles/File/publications/spconf07.pdf.

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

6. Цыганов В. Медиа-терроризм. Терроризм и средства массовой информации [Електронний ресурс] / В. Цыганов. – 2004. – Режим доступу : http://www.studmed.ru/view/cyganov-v-media-terrorizm-terrorizm-i-sredstva-massovoy-informacii_d398538de83.html.

7. Кіслов Д. Сучасні медіа та інформаційні війни / Д. Кіслов. – К. : Леся, 2012. – 239 с.

8. Denning D. Activism, Hacktivism, andCyberterrorism: the Internet as a Tool for Influencing Foreign Policy [Електронний ресурс]. – Режим доступу : http://www.nautilus.org/info-policy/workshop/papers/denning.html.

9. Роговской Е. Россия в борьбе с международным терроризмом: грани повышения позитивного образа страны [Електронний ресурс] / Е. Роговской. – 2007. – Режим доступу : http://www.rusus.ru/?act=read&id=66.

**References**

1. M. Jerrold, From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism / M. Jerrold // NATO Library Terrorism and Political Violence. – Summer 2000. – Vol. 12. – № 2. – Pp. 97-122.

2. O. Hrytsun, Pytannia mizhnarodno-pravovoho rehuliuvannia informatsiinoho teroryzmu [Elektronnyi resurs] / O. Hrytsun. – 2014. – Rezhym dostupu : http://kul.kiev.ua/images/chasop/2014_4/CHAS14_4.pdf.

3. A. Foros, Informatsiinyi teroryzm, yak zahroza natsionalnii bezpetsi Ukrainy [Elektronnyi resurs] / A. Foros. – 2010. – Rezhym dostupu : http://liber.onu.edu.ua:8080/bitstream/123456789/6850/1/256-261ф.pdf.

4. V. Nedilnichenko, Informatsionnie ugrozi v kontekste protivodeystviya terrorizmu [Elektronnyi resurs] / V. Nedilnichenko // Materiali tretey mezhdunarodnoy nauchnoy konferentsii po problemam bezopasnosti i protivodeystviya terrorizmy. – 2008. – Rezhym dostupu : http://www.iisi.msu.ru/UserFiles/File/publications/spconf07.pdf.

5. O. Boichenko, Media-teroryzm: osoblyvosti suchasnykh oznak informatsiinii bezpetsi / O. Boichenko // Intehrovani intelektualni roboto tekhnichni kompleksy (PRTK-2009) : druha mizhnarodna nauk.-prakt. konf. (25-28 travnia 2009 r.) – K. : NAU, 2009. – Pp. 230-232.

6. V. Tsyganov, Media-terrorizm. Terrorizm i sredstva massovoy informatsii [Elektronnyi resurs] / V. Tsyganov. – 2004. – Rezhym dostupu : http://www.studmed.ru/view/cyganov-v-media-terrorizm-terrorizm-i-sredstva-massovoy-informacii_d398538de83.html.

7. D. Kislov, Suchasni media ta informatsiini viiny / D. Kislov. – K. : Lesia, 2012. – 239 p.

8. D. Denning, Activism, Hacktivism, and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy [Elektronnyi resurs]. – Rezhym dostupu : http://www.nautilus.org/info-policy/workshop/papers/denning.html.

9. E. Rogovskiy, Rossiya v borbe s mezhdunarodnim terrorizmom: grani povisheniya pozitivnogo obraza strain [Elektronnyi resurs] / E. Rogovskiy. – 2007. – Rezhym dostupu : http://www.rusus.ru/?act=read&id=66.