УДК 323.28:[351.746:007]:316.658/.774

АНДРУСИШИН Юлія Іванівна
БАРАННІК Валерія Валеріївна

ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ ЯК СУЧАСНА ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ЛЮДИНИ, СУСПІЛЬСТВА, ДЕРЖАВИ

Постановка проблеми. В умовах розвитку інформаційного суспільства під впливом агресивно-деструктивної пропаганди з боку Російської Федерації актуалізуються нові, невідомі раніше загрози національній та міжнародній безпеці, однією з яких є інформаційний тероризм, прояви якого не завжди пов'язані із вчиненням насильницьких дій. Інформація при цьому розглядається як стратегічний ресурс, а цілеспрямоване маніпулювання громадською думкою та вчинення з цією метою терористичних дій стає одним із найважливіших і найнебезпечніших проявів гібридного протиборства на сучасній міжнародній арені.

Аналіз останніх досліджень і публікацій. Проблематиці інформаційного тероризму як одному із способів ведення інформаційної війни присвячена значна кількість праць як зарубіжних, так і вітчизняних дослідників. Зокрема, науковому обґрунтуванню актуальних шляхів забезпечення інформаційної безпеки сприяли праці М. Баглая, А. Даллеса, М. Кастельса, А. Крутських, І. Сафронова, Е. Тоффлера, Б. Хофмана, В. Шапіро, А. Шміда й ін. Інформаційний тероризм в умовах глобалізації, розвитку медіа- та кіберпростору став предметом досліджень сучасних науковців: О. Жайворонка, М. Матули, А. Митка, О. Саган, С. Саржана, О. Свентицької, Т. Яцика тощо. Розробленням заходів протидії терористичній діяльності в інформаційній сфері займалися такі фахівці, як В. Ліпкан, Г. Почепцов, І. Рижов, Ю. Максименко, М. Зубок, А. Форос та ін.

Наукові праці цих учених є основою для дослідження та розкриття змісту й особливостей інформаційного тероризму як актуальної загрози національній та міжнародній безпеці в сучасних умовах, що і є **метою** цієї статті.

Виклад основного матеріалу. На сьогодні ще немає загальноприйнятого визначення понять «інформаційний тероризм» і «кібертероризм». Їх визначення ускладнюється через неможливість чіткого розмежування із звичайними комп'ютерними злочинами чи побутовим маніпулюванням у ЗМІ. І в доробках науковців, і в міжнародно-правових документах наявна велика кількість різних тлумачень. Тільки С. Гнатюк у своєму дослідженні [5] наводить 25 визначень поняття

кібертероризму. Водночас в українському законодавстві (п. 13 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України») кібертероризм визначено досить формально як «терористичну діяльність, що здійснюється у кіберпросторі або з його використанням» [7].

Відповідно до етимологічного значення поняття «інформаційний тероризм» визначають як:

– здійснення або погрозу здійснення за допомогою інформаційних технологій і/або інформаційної зброї загальнонебезпечних 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 [9];

– безпосередній вплив на психіку й свідомість людей з метою формування потрібних думок і суджень, що певним чином спрямовують поведінку людей [11];

– політично мотивовану діяльність груп, структур терористичного спрямування, яка націлена на руйнування знаково-символьної інфраструктури людини і суспільства з метою деструкції соціальних систем і політичних режимів [14];

– 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 [8];

– форму негативного впливу на особистість, суспільство і державу всіма видами інформації [6];

– використання інформації та інформаційної інфраструктури задля насильства над свідомістю людей, маніпулювання їх поведінкою за допомогою певних методів і способів впливу, що дає змогу суб'єктам впливу чинити тиск на прийняття вигідних для них рішень з боку держав, груп людей або окремих осіб шляхом створення умов для хаосу, панічних настроїв тощо [12];

– небезпечні діяння з інформаційного впливу на соціальні групи осіб, державні органи влади і управління, пов'язані із розповсюдженням інформації, яка містить погрози переслідуванням, розправою, вбивствами, а також викривлення об'єктивної інформації, що спричиняє виникнення кризових ситуацій в державі, залякування населення, впровадження параноїдальних думок, нагнітання страху і напруги у суспільстві [16];

– 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 [2; 17].

Зазначений перелік можна продовжувати, однак з урахуванням багатогранності поняття інформаційного тероризму науковці [4; 16] пропонують розглядати його як у широкому, так і у вузькому розумінні.

У широкому розумінні *інформаційний тероризм* являє собою маніпулювання суспільною свідомістю шляхом масового поширення неправдивої і сфабрикованої інформації з метою створення напруженості в суспільстві, нестабільності, хаосу, спрямованих на реалізацію політичних чи економічних цілей в інтересах терористів. У вузькому розумінні – це кібератаки на інформаційні системи, що працюють у контурах управління державними та соціально важливими технологічними об'єктами і системами (атомними чи гідроелектростанціями, банками, хімічним виробництвом, авіацією та іншими видами транспорту тощо), з метою виведення їх із ладу, спричинення економічних, екологічних та інших катастроф тощо.

Найзагальнішими ознаками інформаційного тероризму є [9]: організована форма насильства; здійснення психологічного впливу на широке коло цільової аудиторії, залякування і деморалізація людей, психологічне тероризування певних осіб чи окремих груп суспільства задля досягнення результату; привернення уваги до певної проблеми, вчинення навколо неї галасу; демонстративний характер дій. Водночас терористичні акти в інформаційній сфері характеризуються низкою притаманних лише їм специфічних ознак, зокрема [3]: прихованість – відсутність проявів та слідів проникнення; масштабність – нанесення удару по великій кількості об'єктів; синхронність – атаки можуть бути здійснені одночасно по багатьом об'єктам; віддаленість – джерело атаки може знаходитись за межами країни, в якій здійснюється напад; інтернаціональність – шкода може завдаватися на території кількох держав; публічність – засобами найчастіше виступають друковані ЗМІ, мережі ефірних і кабельних масмедіа, інтернет, електронна пошта тощо.

Інформаційний тероризм у медіапросторі базується на реалізації та масштабуванні інформаційно-емоційного ефекту, зокрема й через залучення прихильників із представників суспільства, із метою впливу на державні інституції, прерогативою яких є прийняття геополітичних і державно важливих рішень. Таким терористичним актам зазвичай притаманне здійснення психологічного насильства над людьми шляхом втручання в їхнє особисте життя, маніпулювання свідомістю, використовуючи з цією метою цілий комплекс методів – від пропаганди (наприклад, представлення альтернативного погляду на події), агітації (приміром, заклики до підтримки ідей і цілей різних рухів) і реклами (наприклад, альтернативного способу життя духовної людини, як це робить медіаармія ісламської держави ІДІЛ) до залякування населення та владних структур шляхом демонстрації терористичних актів на ресурсах світових цифрових платформ [14]. Тобто, зазначені методи орієнтовані не стільки на фізичне насильство й заподіяння матеріальної шкоди, скільки на широкомасштабний вплив на свідомість людей і нав'язування суспільству та державним інституціям своєї волі через використання [13]:

– дезінформування – обман чи введення в оману щодо справжніх намірів для спонукання людини до запрограмованих дій шляхом надання неповної або непотрібної інформації або спотворення частини інформації чи контексту;

– пропаганди – нав'язування людям або групі осіб певних переконань за принципом «мета виправдовує засоби»;

– диверсифікації громадської думки – розпорошення уваги на різні

– маніпулювання – приховане впровадження у психіку особистості цілей, бажань, намірів, установок, які не збігаються з наявними в неї;

– залякування – передача інформації, що має на меті порушення рівноваги та формування тривожних або панічних настроїв стосовно певних викликів або загроз.

Науковці й практики поділяють інформаційний тероризм на (див. рис. 1): інформаційно-психологічний – контроль над ЗМІ з метою

Рисунок 1 – Основні види інформаційного тероризму

штучно резоновані проблеми й відволікання цим від вирішення першочергових завдань;

– психологічного тиску – вплив на психіку людини шляхом залякування, погроз із метою її спонукання до бажаної поведінки;

– чуток – розповсюдження переважно неправдивої інформації здебільшого неофіційними каналами з метою дезорганізації окремих груп населення, суспільства в цілому, установ чи організацій;

поширення дезінформації, чуток, демонстрації могутності терористичних організацій, що здійснюється, насамперед, у духовній сфері, де наявна боротьба ідей, та охоплює політичні, філософські, правові, естетичні, релігійні й інші погляди [9]; інформаційно-технічний – завдання шкоди окремим фізичним елементам інформаційного середовища держави шляхом створення перешкод, використання спеціальних програм, що стимулюють руйнування систем управ-

ління [1]. Відповідно, перший різновид представлений медіатероризмом, а другий – кібертероризмом. Розглянемо детальніше характерні особливості кожного з них.

Так, ***медіатероризм,*** або ***медіакілерство,*** передбачає зловживання інформаційними системами, мережами та їхніми компонентами для здійснення терористичних дій та акцій. Його сутність полягає у спробах шляхом організації спеціальних медіакампаній дестабілізувати суспільство, створити в ньому атмосферу громадянської непокори, недовіри суспільства до дій і намірів влади й, особливо, її силових структур, покликаних захищати суспільний порядок. Засобами здійснення медіатероризму є друковані ЗМІ, мережі ефірних і кабельних масмедіа, інтернет, електронна пошта, різні електронні ігри тощо [3]. Під впливом медіатероризму індивід не здатен самостійно орієнтуватися в перенасиченому інформаційному просторі, чому сприяє зокрема й використання масмедіа інструментів для конструювання недостовірної реальності. Завдання останньої – приховувати та не транслювати правдиву інформацію, здійснюючи «м'який, неочевидний вплив» задля підкорення та контролю свідомості людей [10].

У межах реалізації медіакілерства використовується низка моделей комунікативного впливу, найпоширенішими з яких є такі [15]:

– *націоналістична*, тобто здійснення терористичних актів задля повалення існуючого економічного чи політичного режиму з їх подальшою інтерпретацією в медіа як таких, що спрямовані на благо держави; у такій моделі терористичні організації створюють собі образ «борців за державний суверенітет» (наприклад, висвітлення російськими ЗМІ та інтернет-сайтами подій, які відбуваються на сході України, як боротьби за права місцевого «русского населения» від утисків фашистської української влади);

– *релігійна*, що передбачає використання терористичними організаціями віри як методу виправдання своєї діяльності та реалізується через перекручування релігійних текстів і настанов задля нав'язування думки цивільному населенню про необхідність війни чи, навіть, смерті (наприклад, ісламський тероризм);

– *модель нагнітання*, що реалізується через масштабування та поширення в суспільстві відчуття страху та паніки, при цьому терористичні організації не намагаються виправдати себе, а їхні зусилля спрямовані на вплив на ЗМІ задля нагнітання серед цивільного населення відчуття безпорадності.

Кібертероризм пов'язаний із технічним прогресом, діджиталізацією суспільства та входженням віртуального простору в повсякденне життя людей. Його специфіка визначається тим, що кібертерористичні акти, на перший погляд, не пов'язані з відкритим насильством. Проте приклади його реалізації свідчать про значну загрозу життю та здоров'ю населення, що може настати внаслідок цих комп'ютерних атак.

Термін «кібертероризм» (як поєднання слів *кібер* і *тероризм*) уперше придумав та використав старший дослідник Інституту безпеки

і розвідки в Каліфорнії (США) Баррі Коллін (Barry C. Collin) [21] для пояснення терористичних дій у віртуальному просторі. Цей термін, на думку деяких науковців [20], поєднує два найбільших страхи сьогодення – тероризм і кіберпростір.

На основі аналізу тлумачень зазначених феноменів поняття «кібертероризм» розумітимемо як суспільно небезпечну діяльність із використанням комп'ютерів і телекомунікаційних мереж, що здійснюється із політичних, релігійних, ідеологічних мотивів із метою завдання шкоди чи здійснення дій (або погрози), що загрожують суспільству, спричиняють небезпеку життю і здоров'ю людей та призводять до інших тяжких наслідків.

Прикладами кібертероризму, що ілюструють методи та цілі діяльності кібертерористичних угруповань, є, зокрема, такі резонансні події:

1. У травні 2021 року здійснено кібератаку на американську трубопровідну систему ColonialPipeline (США), внаслідок якої робота всіх трубопроводів цієї системи була зупинена та в США оголошено надзвичайний стан. Злочинці вимагали викуп за зашифровані та викрадені (100 Гб інформації) дані. За наявною інформацією, група хакерів може бути пов'язана з Росією [18].

2. У квітні 2017 року відбулася масштабна атака вірусу NotPetya, що заблокувала роботу значної кількості вебсайтів та автоматизованих систем в Україні (міністерств, банків, ЗМІ, компаній, що постачають електроенергію). Зазначене шкідливе програмне забезпечення уразило інформаційні системи 64 країн світу. Водночас, вважається, що основною метою зловмисників було не вимагання коштів, а заподіяння максимальної шкоди інфраструктурі України [19].

3. У грудні 2015 року стосовно України зафіксовано першу у світі (а в грудні 2016 – другу) кібератаку на енергетичну систему, що призвела до виведення її з ладу та відключення від енергопостачання більше 200 тисяч користувачів: «Прикарпаттяобленерго» (126 тис. користувачів), «Київобленерго» (80 тис. користувачів), «Чернівціобленерго» (22,5 тис. користувачів). Зазначені події були кульмінацією довготривалої APT-атаки хакерської групи російського походження Sandworm із використанням шкідливого програмного забезпечення BlackEnergy.

Отже, сьогодні кібертерористичні угруповання діють насамперед із метою поширення хаосу, зруйнування критичної інфраструктури, завдання фізичної та матеріальної шкоди тощо. Задля цього можуть використовуватися такі ***основні методи*** (див. рис. 2):

– *APT-атаки* (різновид складних кібератак із метою отримання несанкціонованого доступу до інформаційних систем і встановлення прихованого доступу до них із метою використання або контролю в майбутньому) на об'єкти критичної інфраструктури, державні установи, спецслужби й ін.;

– *використання шкідливого програмного забезпечення*, ціллю якого стають системи керування електромереж, транспортних систем,

Рисунок 2 – Основні методи кібертероризму

об'єктів критичної інфраструктури, військових об'єктів;

– DoS/DDoS-атаки – *це атаки на сайти з метою зробити їх недоступними для користувачів*, що перешкоджають доступу до систем, пристроїв і мереж державних установ, медичних закладів, інших об'єктів критичної інфраструктури;

– *отримання несанкціонованого доступу* до державних, банківських чи інших установ із метою викрадення інформації з обмеженим доступом;

– *використання програм-вимагачів* (ransomware), що зашифровують інформацію критично важливих систем і, фактично, блокують діяльність організацій, установ чи окремих осіб.

Висновки. Проведений аналіз показав, що сьогодні різні угруповання терористичного спрямування широко використовують віртуальний простір і масмедіа задля досягнення своїх цілей, адже висока швидкість поширення інформації та комплексність її подачі і сприйняття, доступність, відсутність цензури, наявність величезної потенційної аудиторії користувачів сприяють поширенню інформаційного тероризму в сучасному світі.

Загроза тероризму з використанням медіа- та кіберпростору є комплексним викликом сучасності. Небезпека такого тероризму полягає насамперед у відсутності географічних і національних меж, адже терористичні дії можуть вчинятися з будь-якої точки світу, а також у складності ідентифікації особи терориста в інформаційному просторі та встановлення місця його перебування, адже кібер- і медіаатаки хакери здійснюють опосередковано через використання комп'ютерної техніки. Тому, на нашу думку, найближчим часом із подальшим розвитком технологій і масмедіа буде актуалізуватися питання протидії інформаційному тероризму.

Список використаних джерел

1. Бойченко О. В., Ончурова О. О. Кібертероризм у складі сучасних проблем національної безпеки. *Форум права.* 2010. № 2. С. 57–62.

2. Валюшко І. О. Феномен інформаційного тероризму та його вплив у сучасному світі. *Актуальні питання суспільних наук: наукові дискусії* : матеріали міжнар. наук. конф., (Київ, 19–20 серп. 2016 р.). Київ : ГО «Київська наукова суспільнознавча організація», 2016. С. 66–68.

3. Герасименко К. С. Сучасні ознаки загроз «інформаційного тероризму». *Форум права*. 2009. № 3. С. 162–166.

4. Глазов О. В. Міжнародний інформаційний тероризм в контексті загроз національній безпеці України. URL: http://lib.chdu.edu.ua/pdf/naukpraci/politics/2012/197-185-15.pdf (дата звернення: 10.11.2021).

5. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Безпека інформації*. 2013. Т. 19. № 2. С. 118–129. URL: http://nbuv.gov.ua/UJRN/bezin_2013_19_2_8 (дата звернення: 11.11.2021).

6. Гринчук М. Сучасні методи та технології інформаційного тероризму. *Медіафорум : аналітика, прогнози, інформаційний менеджмент* : збірка наукових праць Чернівецького національного університету. 2017. Т. 5. С. 64–75.

7. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19/Text (дата звернення: 09.11.2021).

8. Курбан О. В. Сучасні інформаційні війни в мережевому он-лайн просторі : навч. посіб. Київ : ВІКНУ, 2016. 286 с.

9. Лабенко Л. В. Інформаційний тероризм: поняття та ознаки. *Міжнародні читання, присвячені пам'яті професора Імператорського Новоросійського університету П. Є. Казанського* : матеріали міжнар. конф., (Одеса, 22–23 жовт. 2010 р.). Одеса : Фенікс, 2010. С. 195–198.

10. Матула М. М. Феномен інформаційного тероризму як загрози національній та міжнародній безпеці. *Науковий блог НАУ «Острозька Академія»*. URL: http://naub.oa.edu.ua/2014/fenomen-informatsijnoho-teroryzmu-yakzahrozy-natsionalnij-ta-mizhnarodnij-bezpetsi (дата звернення: 08.11.2021).

11. Остроухов В. В., Петрик В. М., Присяжнюк М. М. Інформаційна безпека (соціально-правові аспекти) : навч. посіб. Київ : КНТ, 2010. 776 с.

12. Петришин Г. Р. Інформаційний тероризм: джерела формування та активізації в Україні. *Габітус* : науковий журнал. 2021. Вип. 21. С. 44–50.

13. Прокоф'єв Д. Інформаційна війна та інформаційна злочинність. URL: http://www.crime-research.ru/library/Prokop.htm (дата звернення: 08.11.2021).

14. Саган О. В. Протидія медіа-інформаційному тероризму як питання національної безпеки України : автореф. дис. … канд. політ. наук : 21.01.01. Київ, 2021. 22 с.

15. Саміло А. В., Повстин О. В., Купчак М. Я. Інформаційно-комунікативний вплив терористичних організацій як новий виклик українському суспільству. *Вісник Львівського державного університету безпеки життєдіяльності*. 2014. № 10. С. 151–157.

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

17. Яцик Т. П. Особливості інформаційного тероризму як одного із способів інформаційної війни. *Науковий вісник Національного університету ДПС України (економіка, право)*. 2014. № 2 (65). С. 55–60.

18. Companies Still Hobbled From Fearsome Cyberattack. The Associated Press. URL: https://apnews.com/article/ce7a8aca506742ab8e8873e7f9f229c2 (дата звернення: 09.11.2021).

19. Criminal Group Originating From Russia Believed To Be Behind Pipeline Cyberattack. URL: https://edition.cnn.com/2021/05/09/politics/colonial-pipeline-cyberattack-restart-plan/index.html (дата звернення: 09.11.2021).

20. Mark M. Pollitt. Cyberterrorism-FactorFancy? Proceedings of the 20th National Information Systems Security Conference. 1997. P. 285.

21. Mohammad Iqba., Defining Cyberterrorism. 22 J. Marshall J. Computer&Info. L. 2004. 397 p. URL: https://repository.law.uic.edu/jitpl/vol22/iss2/2/ (дата звернення: 10.11.2021).

Рецензенти:
доктор психологічних наук, професор
Н. Іванова,
кандидат психологічних наук
О. Паливода

Аннотация. В статье раскрыты содержание и особенности информационного терроризма как угрозы национальной и международной безопасности в современных условиях. Актуальность темы обусловлена тем, что информация на сегодня рассматривается как стратегический ресурс, а целенаправленное манипулирование общественным мнением и совершение с этой целью террористических действий становится одним из наиболее опасных проявлений гибридного противоборства на современной международной арене. Из-за невозможности четкого разграничения с обычными компьютерными преступлениями и бытовым манипулированием в СМИ понятия «информационный терроризм» и «кибертерроризм» не имеют однозначного толкования. Поэтому информационный терроризм рассматривается в широком (манипулирование общественным сознанием с целью создания напряженности, нестабильности, хаоса, направленных на реализацию политических или экономических целей в интересах террористов) и узком значениях (кибератаки на информационные системы критической инфраструктуры государства с целью выведения их из строя, которые могут привести к экономическим, экологическим и другим катастрофам).

Abstract. The article discusses the content and characteristics of information terrorism as a threat to national and international security in contemporary circumstances. The relevance of the topic stems from the fact that information is currently considered a strategic resource, the deliberate manipulation of public opinion and the commission of terrorist acts to that end has become one of the most dangerous manifestations of hybrid confrontation in the contemporary international arena. Due to the impossibility of clear distinction with ordinary computer crimes and domestic manipulation in mass media, the concepts of «information terrorism» and «cyberterrorism» do not have a clear interpretation. Therefore, information terrorism is viewed in a broad sense (manipulation of public consciousness to create tension, instability, chaos aimed at achieving political or economic objectives in the interests of terrorists) and in narrow terms (cyberattacks on critical government infrastructure information systems to disable them, which can lead to economic, environmental and other disasters).

General characteristics of information terrorism have been defined and specific characteristics peculiar only to terrorist acts in the information sphere have been identified. The methods of information terrorism are described, which are aimed at influencing people's consciousness on a large

Определены общие признаки информационного терроризма и выделены специфические характеристики, свойственные только террористическим актам в информационной сфере. Охарактеризованы методы информационного терроризма, ориентированные на широкомасштабное влияние на сознание людей и навязывание обществу и государственным институциям своей воли через использование: дезинформирования, пропаганды, диверсификации общественного мнения, психологического давления, слухов, манипулирования, запугивания. Описаны разновидности информационного терроризма: информационно-психологический (медиатерроризм / медиа-киллерство) и информационно-технический (кибертерроризм).

Сделаны выводы о том, что на сегодняшний день виртуальное пространство и масс-медиа широко используются различными группировками террористического направления для достижения собственных целей, поскольку доступность, отсутствие цензуры, наличие огромной потенциальной аудитории пользователей, высокая скорость распространения информации и комплексность ее подачи и восприятия способствуют расширению информационного терроризма в современном мире.

Угроза терроризма с использованием медиа- и киберпространства является комплексным вызовом современности. Опасность такого терроризма состоит в отсутствии географических и национальных границ, а также в сложности идентификации личности террориста в информационном пространстве и установления места его пребывания. Поэтому в связи с дальнейшим развитием технологий и масс-медиа вопрос противодействия информационному терроризму будет особенно актуальным.

Ключевые слова: информационный терроризм, кибертерроризм, медиа-терроризм, манипулирование, виртуальное пространство.

scale and at imposing their will on society and State institutions through the use of disinformation, propaganda, diversification of public opinion, psychological pressure, rumours, manipulation, intimidation. Variants of information terrorism are described: information and psychological (media-terrorism / media-killing) and information technology (cyberterrorism).

The conclusions are that today virtual space and mass media are widely used by various terrorist-oriented groups for their own purposes, because accessibility, the absence of censorship, the large potential audience of users, the speed with which information is disseminated and the complexity with which it is presented and received are all contributing to the spread of information terrorism in today's world.

The threat of terrorism through the use of media and cyberspace is a complex challenge of our time. The danger of such terrorism lies in the absence of geographical and national borders, as well as in the difficulty of identifying the identity of the terrorist in the information space and establishing his whereabouts. Therefore, in view of the further development of technology and mass media, the issue of countering information terrorism will be particularly relevant.

Key words: information terrorism, cyberterrorism, media terrorism, manipulation, virtual space.