DOI: 10.18372/2307-9061.59.15615
УДК 32.019.51:323.28:323.2(477)(045)

Б. Д. Леонов,
доктор юридичних наук, старший науковий співробітник
ORCID ID: https://orcid.org/0000-0002-2488-7377

С. Я. Лихова,
доктор юридичних наук, професор
ORCID ID: https://orcid.org/0000-0003-4755-7474

ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ

Національна академія Служби безпеки України
вул. Михайла Максимовича, 22, 03022, Київ, Україна
Національний авіаційний університет
проспект Любомира Гузара, 1, 03680, Київ, Україна
E-mails: academy@ssu.gov.ua, sofia.lykhova@gmail.com

Мета: *дослідити види і форми інформаційного тероризму в контексті загрози національній безпеці України.* ***Методологічну основу*** *дослідження складають порівняльно-правовий та системний аналіз, формально-юридичний метод, метод інтерпретації, герменевтичний та методи аналізу та синтезу.* ***Обговорення:*** *проблема боротьби з інформаційним тероризмом потребує аналізу різноманітних кризових явищ та структури самого тероризму як явища, який пройшов довгий шлях еволюції від одинаків-смертників, величезних терористичних організацій, які вчиняють теракти, що тягнуть за собою загибель великої кількості людей, до використання інформації для залякування значної кількості людей.* ***Результати:*** *однією з основних загроз інформаційній безпеці доцільно визначити інформаційний тероризм як форму деструктивного впливу, спрямованого на маніпуляцію чи залякування населення або заподіяння з використанням інформаційних технологій шкоди суспільству, державі чи окремим особам з метою примусити органи державної влади, міжнародну організацію, юридичну чи фізичну особу (групу осіб) вчинити якусь дію (або утриматися від її вчинення).*

Ключові слова: *тероризм; інформаційний тероризм; інформаційні технології; кібертероризм.*

Постановка проблеми та її актуальність. Стрімкий розвиток інформаційних технологій, масштаб застосування глобальних телекомунікаційних мереж та процес побудови інформаційного суспільства обумовили виникнення нових загроз в інформаційній сфері, однією з яких на часі є використання виникаючих можливостей у терористичній діяльності, що заподіює шкоду життєво важливим інтересам особи, суспільства і держави. В таких умовах стрімко зростає рівень загрози інформаційного тероризму в інформаційному просторі. Безспірно, що сьогодні Інтернет ускладнив захист інформаційних ресурсів. Терористичні групи й окремі терористи в усьому світі користуються його особливостями і перевагами, намагаючись впливати як на внутрішню, так і на зовнішню політику держав, використовуючи різноманітні інформаційні технології для досягнення своєї злочинної мети. В юридичній літературі вказується, що доступність інформаційних технологій значно підвищує ризики інформаційного тероризму, а розвиненість інформаційної інфраструктури суспільства сприяє створенню додаткових ризиків інформаційного тероризму, який у сучасних умовах глобалізації та інтернаціоналізації набуває надзвичайно деструктивного значення. Проблема боротьби з інформаційним

тероризмом потребує аналізу різноманітних кризових явищ та структури самого тероризму як явища, яке пройшло довгий шлях еволюції від одинаків-смертників до терористичних організацій, які вчиняють теракти, що тягнуть за собою загибель великої кількості людей, до використання інформації для залякування значної кількості людей. Тому дослідження феномену інформаційного тероризму в контексті інформаційної безпеки є важливим питанням національної безпеки. Інформаційний тероризм породжує нові феномени, які досліджуються сучасними науковцями [1, с. 135-141].

Аналіз останніх досліджень і публікацій. Теоретичні аспекти протидії інформаційному тероризму досліджували Л.В. Лабенко, В.М. Брижко, М.Я. Швець, Л.А. Бураєва, Р.О. Банк, В.Г. Пилипчук, О.П. Дзьобань та ін. Особливості інформаційного тероризму як одного із способів інформаційної війни висвітлені у працях Г.Г. Почепцова, В.О. Коршунова, А.М. Митко, І.І. Кольцової, І.М. Рижова, Т.П. Яцик та ін. Сучасні загрози інформаційного тероризму досліджували О.В. Бойченко та К.С. Герасименко.

Вагомий внесок у дослідження інформаційного тероризму як засобу введення інформаційної війни зробили зарубіжні вчені, серед яких слід виділити праці Ж. Бодрійара, У. Лакера, Е. Тоффлера, Б. Хофмана, А. Шміда та ін.

Водночас, серед учених існують розбіжності поглядів щодо форм і різновидів інформаційного тероризму. Також бракує комплексного підходу до визначення місця інформаційного тероризму в системі загроз національній безпеці держави.

Мета статті – визначити особливості інформаційного тероризму як загрози національній безпеці України.

Виклад основного матеріалу. Незважаючи на численні публікації, присвячені різноманітним аспектам феномену інформаційного тероризму, належного наукового осмислення серед вчених та фахівців дана проблема ще не отримала. Відсутня єдність підходів до розуміння цього явища. Уніфікованого тлумачення у доктрині інформаційного права досі не існує. Окремі вітчизняні автори роблять досить вдалі спроби дослідити питання правового забезпечення інфомаційної безпеки [2, с. 95-102].

Якщо ж проаналізувати зарубіжні джерела, то доходимо висновку, що існує декілька точок зору щодо вказаної проблеми.

Одна з них зводиться до того, що «інформаційний тероризм» – це сфера негативного впливу на особу, суспільство, державу за допомогою усіх видів інформації з метою послаблення або повалення конституційного ладу, що це – форма негативного впливу за допомогою використання інформаційно-комунікаційних технологій [3, с. 134].

Інформаційний тероризм часто розглядається у межах виключно інтелектуальної сфери, як один із найбільш перспективних видів тероризму, який діє в інтелектуальній сфері і породжує новий вид пов'язаного з кіберпростором насильства, яке може бути спрямоване проти будь-кого, а його успіх забезпечується не грубою силою, а нейронами.

За висловленою ще однією точкою зору інформаційний тероризм – це залякування суспільства шляхом використання високих технологій для досягнення політичних, релігійних чи ідеологічних цілей, а також дії, які призводять до відключення, виведення з ладу об'єктів критичної інфраструктури або знищення інформації [4]. Такі дії можуть включати використання інформаційних технологій для організації та виконання атак проти телекомунікаційних мереж, інформаційних систем і комунікаційної інфраструктури.

Аналіз наукової літератури свідчить, що більшість зарубіжних дослідників поділяють точку зору, згідно з якою інформаційний тероризм є різновидом терористичної діяльності, яка пов'язана з досягненнями у сфері інформаційних технологій.

Українські дослідники та фахівці також визнають серйозність небезпеки інформаційного тероризму.

Так, В.О. Коршунов під інформаційним тероризмом пропонує розуміти новий вид терористичної діяльності, орієнтований на використання різних форм і методів тимчасового або незворотного виведення з ладу інформаційної інфраструктури держави або її елементів, а та-

кож за допомогою протиправного використання інформаційної структури для створення умов, що тягнуть за собою тяжкі наслідки для різних сторін життєдіяльності особистості, суспільства і держави [5, с. 6].

Правоохоронні органи в межах своєї компетенції зобов'язані протидіяти загрозам інформаційного тероризму. На думку К.С. Герасименко, головні загрози у сфері інформаційного тероризму переважно створюють іноземні держави, міжнародні терористичні та інші злочинні угрупування й організації, які користуються нерозвиненістю й слабкістю відповідних державних структур. Тому не випадково існує думка, що сучасний інформаційний тероризм характеризується як множина інформаційних війн та спецоперацій, пов'язаних із національними або транснаціональними кримінальними структурами та спецслужбами іноземних держав [6, с. 57].

Законодавство України не містить визначення інформаційного тероризму. Закон України «Про боротьбу з тероризмом» містить поняття «технологічний тероризм», яке не збігається з дефініцією «інформаційний тероризм», а Закон України «Про основні засади забезпечення кібербезпеки України» містить визначення «кібертероризму», який можна визнати лише одним із різновидів інформаційного тероризму, про що йдеться далі.

Зауважимо, що визначення інформаційного тероризму не містять і міжнародні правові акти, серед яких варто виділити Конвенцію Ради Європи про запобігання тероризму (2005 р.), Конвенцію про кіберзлочинність (2001 р.)

Узагальнення інформації, отриманої з різних наукових джерел, дає підстави для висновку, що інформаційний тероризм – доктринальне поняття теорії інформаційної безпеки, під яким розуміють: 1) суспільне небезпечне діяння, яке є проявом тероризму; 2) форму деструктивного інформаційно-психологічного впливу на особистість, суспільство і державу; 3) 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 виникненню кризових ситуацій у державі, нагнітання страху і напруги у суспільстві; 3) певний насильницький пропагандистський вплив на психіку людини, який не дає йому можливості критично оцінювати отриману інформацію; 4) 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 [5]; 5) множину інформаційних війн та інформаційних спецоперацій, пов'язаних із національними або транснаціональними кримінальними структурами та спецслужбами іноземних держав [6]; 6) 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 [7]; 7) ідеологічно обґрунтовану практику впливу, спрямованого на залякування населення, на прийняття рішення або вчинення дії (бездіяльності) органом влади, органом місцевого самоврядування, міжнародною організацією, соціальною групою, юридичною особою або фізичною особою в межах інформаційного простору, пов'язаного з використанням інформації, інформаційних технологій і (або) інформаційного ресурсу.

Традиційно, залежно від спрямованості умовно можна виділити два види інформаційного тероризму: 1) «психологічний» (пропаганда тероризму, створення атмосфери страху і паніки в суспільстві і т.д.); 2) «технічний» (контролювання або блокування каналів передачі масової інформації, порушення функціонування об'єктів інформаційної інфраструктури та ін.).

Залежно від злочинної мети та використання інструментів (засобів) її досягнення інформаційний тероризм теж можна поділити на два види: медіа тероризм та кібертероризм.

Медіа-тероризм – зловживання інформаційним системами, мережами, та їхніми компонен-

тами для здійснення терористичної діяльності (пропаганда та поширення ідеології тероризму, сприяння вчиненню теракту). Засобами здійснення медіа-тероризму є друковані ЗМІ, мережі ефірних й кабельних мас-медіа, Інтернет, електронна пошта, спам тощо [8, с. 114].

Кібертероризм – навмисна, політично вмотивована атака на об'єкти інформаційного простору, що створює небезпеку для життя та/або здоров'я людей або настання інших тяжких наслідків, якщо такі дії були здійсненні з метою порушення державної чи громадської безпеки, залякування населення, провокації військового конфлікту чи загроза вчинення таких дій. Політично мотивовані атаки, які завдають серйозної шкоди, на кшталт серйозних економічних труднощів або тривалих зупинок енерго-, водопостачання, можна також охарактеризувати як кібертероризм.

Закон України «Про основні засади забезпечення кібербезпеки України» визначає кібертероризм як терористичну діяльність, що здійснюється в кіберпросторі або з його використанням (ст. 1). Кібертероризм є серйозною суспільно-політичною загрозою для людства, у порівнянні навіть із ядерною, бактеріологічною і хімічною зброєю, причому ступінь цієї загрози через свою новизну, не до кінця ще усвідомлений і вивчений [8, с. 114]. Окремі фахівці з кібербезпеки прогнозують, що «нові терористи» направлять свої зусилля на освоєння інформаційної зброї, руйнівна сила якої може бути у багато разів більшою від біологічної та хімічної [9]. Світовий досвід свідчить про безперечну уразливість будь-якої держави, тим більше, що кібертероризм не має державних кордонів; кібертерорист здатний рівною мірою загрожувати інформаційним системам, розташованим практично в будь-якій точці земної кулі шляхом використання спеціального програмного забезпечення, призначеного для несанкціонованого проникнення в комп'ютерні мережі та організації віддаленої кібератаки на інформаційні ресурси жертви.

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.

Для визначення таких загроз слід, насамперед, з'ясувати сутність поняття «загроза». Поняття «загроза» слід розуміти як явища та фактори, що негативно впливають або можуть вплинути на певний об'єкт або становити небезпеку порушення інтересів певних суб'єктів [10, с. 102].

Відповідно до п. 6 ст. 1 Закону України «Про національну безпеку України» під загрозами національній безпеці України слід розуміти явища, тенденції і чинники, що унеможливлюють чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України. У літературі існують різні підходи до визначення загроз національній безпеці залежно від об'єкта впливу. Зокрема, однією із загроз національній безпеці держави називають кіберзагрозу як об'єктивну існуючу можливість учинення кіберзлочинів, унаслідок чого можуть настати негативні наслідки як у реальному, так і віртуальному середовищах для життєво важливих інтересів держави [11, с. 345]. На нашу думку, загрози в інформаційній сфері слід розглядати як фактори, що завдають шкоду інформаційній безпеці держави. У проекті Концепції інформаційної безпеки України загрози інформаційного характеру визначаються як наявні або потенційно можливі явища і чинники, які створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства і держави в інформаційній сфері. Серед загроз національній безпеці в інформаційній сфері виділяються: створення, розповсюдження інформації з метою підтримання, супроводження або активізації терористичної діяльності (п/п. «г» п. 3 ст. 8); про-

яви кіберзлочинності, кібертероризму (п/п. «б» п. 4 ст. 8).

Стратегія національної безпеки України основним завданням розвитку системи кібербезпеки визначає гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури, зокрема в умовах цифрової трансформації (п. 52), а серед пріоритетних завдань правоохоронних, спеціальних, розвідувальних та інших державних органів виділяється активна та ефективна протидія розвідувально-підривній діяльності, запобігання тероризму, спеціальним інформаційним операціям та кібератакам. Як загроза національній безпеці України у Стратегії згадується поширення міжнародного тероризму у кіберпросторі.

Доктрина інформаційної безпеки не містить згадки про загрози інформаційного тероризму. З-поміж актуальних загроз інформаційній безпеці згадуються лише спеціальні інформаційні операції, інформаційну експансію, інформаційне домінування, зміст яких лише частково відтворює поняття інформаційного тероризму.

Очевидно, що загрози інформаційного тероризму мають знайти відображення у Стратегії інформаційної безпеки України, розробка якої передбачена Стратегією національної безпеки України (п. 66). Ця Стратегія визначатиме засади забезпечення інформаційної безпеки України, протидії загрозам національній безпеці в інформаційній сфері, захисту прав осіб на інформацію та захист персональних даних. Її метою є забезпечення інформаційної безпеки України, спрямованої на захист життєво важливих інтересів громадянина, суспільства та держави у протидії внутрішнім і зовнішнім загрозам, забезпечення захисту державного суверенітету і територіальної цілісності України. Як стратегічну ціль № 1 цієї Стратегії визначено протидію дезінформації, маніпулятивній інформації, інформаційним операціям та атакам, у т.ч. спрямованим на вчинення терористичних актів.

Для успішної протидії таким загрозам слід виокремити ряд основних напрямів:

– уніфікація та гармонізація національного законодавства та міжнародних актів;

– проведення наукових розробок у сфері створення сучасних технологій виявлення та запобігання кримінальним і терористичним впливам на інформаційні ресурси;

– створення спеціалізованих підрозділів у сфері боротьби з комп'ютерними злочинами та комп'ютерним тероризмом;

– удосконалення міжнародної організаційно-правової взаємодії з питань протидії комп'ютерній злочинності та комп'ютерному тероризму;

– удосконалення багаторівневої системи підготовки кадрів у сфері інформаційної безпеки [12].

Завдання, основні принципи та напрями вдосконалення загальнодержавної системи боротьби з тероризмом з огляду на сучасні терористичні загрози національній безпеці України та прогноз їх розвитку визначені Концепцією боротьби з тероризмом в Україні, напрями реалізації якої передбачають: визначення та аналіз причин і умов, що призводять до поширення тероризму; удосконалення правових та організаційних основ боротьби з тероризмом; удосконалення існуючих, розроблення та впровадження нових методів боротьби з тероризмом; оптимізацію шляхів та способів захисту життя і безпеки, прав і свобод людини і громадянина, захисту інтересів суспільства та держави від терористичних посягань; поліпшення інформаційного, наукового, кадрового та матеріально-технічного забезпечення суб'єктів боротьби з тероризмом. Інформаційний простір та його компоненти визначено об'єктами можливих терористичних посягань [13].

Висновки. Вважаємо, що однією з основних загроз інформаційній безпеці в Стратегії інформаційної безпеки України [14] доцільно визначити інформаційний тероризм як форму деструктивного впливу, спрямованого на маніпуляцію чи залякування населення або заподіяння з використанням інформаційних технологій шкоди суспільству, державі чи окремим особам з метою примусити органи державної влади, міжнародну організацію, юридичну чи фізичну особу (групу осіб) вчинити якусь дію (або утриматися від її вчинення).

Література

1. Филинович В.В. Кибersталкинг: проблемы правовой защиты. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. Київ: НАУ, 2021. № 1 (58). С. 135-141. DOI: https://doi.org/10.18372/2307-9061.58.15320

2. Кунєв Ю.Д. Правове забезпечення інформаційної безпеки як предмет правового дослідження. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. Київ: НАУ, 2021. № 1 (58). С. 95-102. DOI: https://doi.org/10.18372/2307-9061.58.15314

3. Глотина И.М. Информационный терроризм и его влияния на экономику. *Экономическая глобализация и проблемы национальной международной безопасности*. 2014. С. 132-134.

4. Tafoya W.L. Cyber Terror. *FBI Law Enforcement Bulletin*, 2011. URL: http://www.fbi.gov/stats-services/publications/law-enforcementbulletin/ november-2011/cyber-terror (дата звернення: 04.02.2021).

5. Коршунов В.О. Політичний тероризм: інформаційні методи боротьби: автореф. дис. … канд. політ. наук: спец. 23.00.02. Дніпропетровськ, 2008. 18 с.

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

7. Jerrold M. From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism / NATO Library at: Terrorismand political violence. Vol. 12, no. 2, Summer 2000. P. 97-122.

8. Банк Р.О. Інформаційний тероризм як загроза національній безпеці України: теоретико-правовий аспект. *Інформація і право*. 2016. № 1(16). С. 110-116.

9. Walter Laqueur. «Postmodern Terrorism» Foreign Affairs, Vol. 75, № 5, September/October 1996. P. 24–36.

10. Тихонова О.В. Фінансова безпека України: кримінально-правові та кримінологічні основи. Дніпропетровськ: Середняк Т.К., 2015. 484 с.

11. Шеломенцев В.П. Кримінологічна безпека у кіберпросторі: система понять. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2010. № 23. С. 342-348.

12. Гавриш С.Б. Комп'ютерний тероризм: сучасний стан, прогнози розвитку та шляхи протидії. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2009. № 20. С. 3-14.

13. Концепція боротьби з тероризмом: затв. Указом Президента України від 05 бер. 2019 р. № 53. URL: https://zakon.rada.gov.ua/ laws/show/ 53/2019#Text (дата звернення: 04.02.2021).

14. Стратегія інформаційної безпеки України. URL: https://mkip.gov.ua/ files/ pdf/ 45698712365.pdf (дата звернення: 04.05.2021).

References

1. Filinovich V.V. Kiberstalking: problemy pravovoj zashhity. Naukovi praci Nacional'nogo aviacijnogo universitetu. Serija: Juridichnij visnik «Povitrjane i kosmichne pravo». Kyiv: NAU, 2021. № 1 (58). S. 135-141.

2. Kunjev Ju.D. Pravove zabezpechennja informacijnoi' bezpeky jak predmet pravovogo doslidzhennja. *Naukovi praci Nacional'nogo aviacijnogo universytetu. Serija: Jurydychnyj visnyk «Povitrjane i kosmichne pravo»*. Kyiv: NAU, 2021. № 1 (58). S. 95-102.

3. Glotina I.M. Informacionnyj terorizm i ego vlijanija na jekonomiku. *Jekonomicheskaja globalizacija i problemy nacional'noj mezhdunarodnoj bezopasnosti*. 2014. S. 132-134.

4. Tafoya W.L. Cyber Terror. *FBI Law Enforcement Bulletin*, 2011. URL: http://www.fbi.gov/stats-services/publications/law-enforcementbulletin/ november-2011/cyber-terror (дата звернення: 04.02.2021).

5. Korshunov V.O. Politychnyj teroryzm: informacijni metody borot'by: avtoref. dys. … kand. polit. nauk: spec. 23.00.02. Dnipropetrovs'k, 2008. 18 s.

6. Gerasymenko K.S. Suchasni oznaky zagroz «informacijnogo teroryzmu». *Forum prava*. 2009. № 3. S. 162–166.

7. Jerrold M. From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism / NATO Library at: Terrorismand political violence. Vol. 12, no. 2, Summer 2000. P. 97-122.

8. Bank R.O. Informacijnyj teroryzm jak zagroza nacional'nij bezpeci Ukrai'ny: teoretyko-pravovyj aspekt. *Informacija i pravo*. 2016. № 1(16). S. 110-116.

9. Walter Laqueur. «Postmodern Terrorism» Foreign Affairs, Vol. 75, № 5, September/October 1996. P. 24–36.

10. Tyhonova O.V. Finansova bezpeka Ukrai'ny: kryminal'no-pravovi ta kryminologichni osnovy. Dnipropetrovs'k: Serednjak T.K., 2015. 484 s.

11. Shelomencev V.P. Kryminologichna bezpeka u kiberprostori: systema ponjat'. *Borot'ba z organizovanoju zlochynnistju i korupcijeju (teorija i praktyka)*. 2010. № 23. S. 342-348.

12. Gavrysh S.B. Komp'juternyj teroryzm: suchasnyj stan, prognozy rozvytku ta shljahy protydii'. *Borot'ba z organizovanoju zlochynnistju i korupcijeju (teorija i praktyka)*. 2009. № 20. S. 3-14.

13. Koncepcija borot'by z teroryzmom: zatv. Ukazom Prezydenta Ukrai'ny vid 05 ber. 2019 r. № 53. URL: https://zakon.rada.gov.ua/laws/ show/ 53/2019#Text (data zvernennja: 04.02.2021).

14. Strategija informacijnoi' bezpeky Ukrai'ny. URL: https:// mkip.gov.ua/ files/ pdf/ 45698712365.pdf (data zvernennja: 04.05.2021).

B. Leonov, S. Lykhova

INFORMATION TERRORISM AS A THREAT TO THE NATIONAL SECURITY OF UKRAINE

National Academy of Security Service of Ukraine
Mykhailo Maksymovych str., 22, 03022, Kyiv, Ukraine
National Aviation University
Liubomyra Huzara Avenue, 1, 03680, Kyiv, Ukraine
E-mails: academy@ssu.gov.ua, sofia.lykhova@gmail.com

Purpose: *to investigate the types and forms of information terrorism in the context of the threat to Ukraine's national security.* ***The methodological basis*** *of the study consists of comparative law and system analysis, formal law method, method of interpretation, hermeneutic and methods of analysis and synthesis.* ***Discussion:*** *the problem of combating information terrorism requires an analysis of various crisis phenomena and the structure of terrorism itself as a phenomenon that has come a long way from lone suicide bombers to huge terrorist organizations that carry out terrorist attacks, to the use of information for intimidation of a significant number of people.* ***Results:*** *one of the main threats to information security is information terrorism as a form of destructive influence aimed at manipulating or intimidating the population or causing harm to society, the state or individuals through information technology in order to force public authorities, international organizations, legal entities or individuals (group of persons) to take an action (or refrain from doing so). It is indisputable that today the Internet has complicated the protection of information resources. Terrorist groups and individual terrorists around the world enjoy its features and benefits, trying to influence both domestic and foreign policies of states, using a variety of information technologies to achieve their criminal goal. The legal literature indicates that the availability of information technology significantly increases the risks of information terrorism, and the development of information infrastructure of society contributes to the creation of additional risks of information terrorism, which in today's globalization and internationalization becomes extremely destructive.*

Keywords*: terrorism; information terrorism; information technologies; cyberterrorism.*