13. Тараненко О.П. Сучасні заходи запобігання корупції у сфері державних закупівель / О.П. Тараненко // Державне управління: теорія та практика. – 2014. – № 2 [Електронний ресурс]. – Режим доступу: http://academy.gov.ua/ej/ej20/PDF/4.pdf.

14. Нагачевський С.В. Запобігання та протидія корупції у сфері державних закупівель / // Науковий вісник Львівського державного університету внутрішніх справ. серія юридична. - 2015. - Вип. 1. - С. 415-425.

15. Мельников О. С. Шляхи протидії корупції у сфері державних закупівель / О.С. Мельников // Актуальні проблеми державного управління. - 2016. - № 1. - С. 44-49.

Дасевич А.О.
здобувач вищої освіти, 5 курс, група С-ЮЗ-6113 факультету заочного навчання Дніпропетровського державного університету внутрішніх справ
Мирошниченко В.О.
науковий керівник, доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, кандидат технічних наук, доцент

ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ ТА ЙОГО РІЗНОВИДИ

В сучасному світі дуже поширеним явищем, яке представляє серйозну загрозу безпеці та життєво важливим інтересам як особи, так і суспільства, став тероризм. Сучасний тероризм істотно відрізняється від використання терористичної тактики екстремістськими групами у минулому. Терористична діяльність як складне, багатоаспектне негативне соціально-політичне явище давно переросла рамки національних меж і перетворилася на масштабну загрозу для безпеки всього людства.

Слід підкреслити, що інформаційний тероризм – це не тільки кібер-злочини, хоча звичайно, ж вони частина цього явища, це також некоректні маніпуляції з інформацією або її підтасування, а в деяких випадках і подача свідомо помилкових фактів, внаслідок чого відбувається залякування населення, впровадження параноїдальних думок. Інформаційні злочини суттєво впливають на інформаційну безпеку держави не тільки через те, що завдяки цим злочинам заподіюється значний економічний збиток, але насамперед через те, що наслідком вчинення зазначених злочинів є порушення нормальної роботи інформаційних і комунікаційних систем, а також поширюється інформація, що має протиправний характер [5].

Особливу небезпеку сучасності становить відносно новий вид терористичної діяльності – інформаційний тероризм, розгортання якого зумовлено широким запровадженням інформаційно-телекомунікаційних систем у всіх сферах життєдіяльності суспільства.

В наукових кругах інформаційний тероризм розділяють на:

1) інформаційно-психологічний тероризм (контроль над ЗМІ з метою поширення дезінформації, чуток, демонстрації могутності терористичних організацій): медіа-тероризм, зловживання інформаційними системами, мережами, та їхніми компонентами для здійснення терористичних дій та акцій;

2) інформаційно-технічний тероризм (завдання збитків окремим елементам і всьому інформаційному середовищу супротивника в цілому: руйнування елементної бази, активне придушення ліній зв'язку, штучне перезавантаження вузлів комунікації): кібер-тероризм – сукупність дій, що включають інформаційну атаку на комп'ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші складові інформаційної інфраструктури, яка здійснюється злочинними угрупованнями або окремими особами [2, с. 231].

У випадку медіа-інформаційного тероризму йдеться про різновид інформаційного тероризму, що є зловживанням інформаційними системами, мережами, та їхніми компонентами для здійснення терористичних дій та акцій [3, с. 164].

Для здійснення психологічного терору використовуються не лише друковані ЗМІ та мережі ефірних й кабельних мас-медіа, але й Інтернет, електронна пошта, різноманітні електронні іграшки, компакт-диски, аудіокасети тощо. За умов теперішньої розвиненості масових комунікацій у світі, що невпинно рухається до глобалізації, мас-медіа з їхніми можливостями впливу на масову ментальність і архетипи колективного несвідомого – це різна зброя, яку можна обернути й на користь антитерористичним операціям [6].

Досить типовим прикладом для розуміння сутності медіа-терору, механізмів його викликання, стимулювання й поширення може служити такий специфічний засіб масової інформації, як листівка. У ній головну роль відіграє не інформація, як така, а пропаганда, контрпропаганда, агітація, реклама. Тому головним завданням такого засобу інформаційного тероризму є не інформування, а маніпулювання [4, с. 80].

Отже, на перший погляд здається ніби то медіа-тероризм є не таким небезпечним явищем, однак якщо копнути глибше, то бачимо, що за його допомогою дезінформують людей, підривають авторитет органів державної влади, що тягне за собою страшні наслідки. В сучасному світі громадяни, на жаль, більше довіряють ЗМІ та мережі Інтернет, а ніж державі. Гучні слова щодо незалежних розслідувань не завжди мають під собою справжнє підґрунтя, а деякі представники так званої четвертої влади граючи на емоціях простих громадян, поширюють при цьому неправдиві відомості та налаштовують громадян на бік терористичних організацій.

Ще більш небезпечним видом інформаційного тероризму, на нашу думку, є кібер-тероризм. Згідно з поглядами експертів ООН, поняття «кіберзлочинність» об'єднує будь-який злочин, який можна здійснити за допомогою комп'ютерної

системи або мережі та також проти комп'ютерної системи або мережі. Зокрема, до кібер-тероризму належать: незаконне втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж, крадіжка, присвоєння, вимагання комп'ютерної інформації, організація вилученої атаки на інформаційні ресурси, закладки та розробки комп'ютерних вірусів, які здійснюють знімання, модифікацію, або знищення інформації [1, с. 58].

На сьогодні кібер-тероризм є одним із найнебезпечніших видів злочинності. Кібер-атаки можуть завдати значної шкоди на локальному, державному та навіть міжнародному рівні. Адже зовнішні кібер-атаки можуть переслідувати і більш серйозні цілі, ніж пасивний збір даних, а об'єктами кібер-тероризму можуть бути грошова і секретна інформація, апаратура контролю над космічними приладами, ядерними електростанціями, воєнними комплексами головні комп'ютерні вузли тощо.

Можна стверджувати, що під інформаційним тероризмом розуміється не тільки, кібер-тероризм, а ще й медіа-тероризм, який набув досить широкого розповсюдження. На сьогоднішні реалії ці два види інформаційного тероризму значно впливають на людей та їх свідомість. Широке розповсюдження ЗМІ та мережі Інтернет надало можливості терористичним організація впливати на громадян з метою залякування, переконання широкої аудиторії в правдивості викривлених фактів, з метою збору секретної інформації, що стосується банківських, комерційних та інших таємниць, що надалі використовуються в їхніх цілях.

Список використаних джерел:

1. Бойченко О. В. Кібертероризм у складі сучасних проблем національної безпеки [Електронний ресурс] / О. В. Бойченко, О. О. Ончурова // Форум права. - 2010. - № 2. - С. 57-62.
2. Бойченко О. В. Медіа-тероризм: особливості сучасних ознак інформаційній безпеці /О. В. Бойченко // Інтегровані інтелектуальні робото технічні комплекси (ПРТК-2009): Друга міжнародна наук.-практ. конф. (25–28 травня 2009 р.). – К.: НАУ, 2009. – С. 230–232.
3. Герасименко К. С. Сучасні ознаки загроз "інформаційного тероризму" [Електронний ресурс] / К. С. Герасименко // Форум права. - 2009. - № 3. - С. 162-166.
4. Глазов О. В. Міжнародний інформаційний тероризм у контексті загроз національній безпеці України [Електронний ресурс] / О. В. Глазов // Наукові праці [Чорноморського державного університету імені Петра Могили]. Сер. : Політологія. - 2012. - Т. 197, Вип. 185. - С. 78-82.
5. Кубишкін О. В. Міжнародно-правові проблеми забезпечення інформаційної безпеки держави [Електронний ресурс]. – Режим доступу: http://pravolib.pp.ua/mejdunarodnopravovyie-problemyi-obespecheniya.html.
6. Надьон О. В. Правовий аналіз передумов виникнення загрози тероризму в Україні / О. В. Надьон [Електронний ресурс]. – Режим доступу: http://pravoznavec.com.ua/period/ chapter/2/24/849.