УДК 32.019.5+327

Мітін Владислав Ігорович
Студент
Національна академія Служби безпеки України
Навчально-науковий інститут інформаційної безпеки
Митин Владислав Игоревич
Студент
Национальная академия Службы безопасности Украины
Научно-исследовательский институт информационной безопасности
Mitin V.
Student
National Academy of the Security service of Ukraine
Educational and Research Institute of Information Security

ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ НА СУЧАСНІЙ МІЖНАРОДНІЙ АРЕНІ

ИНФОРМАЦИОННЫЙ ТЕРРОРИЗМ НА СОВРЕМЕННОЙ МЕЖДУНАРОДНОЙ АРЕНЕ

INFORMATION CYBERTERRORISM AT THE MODERN INTERNATIONAL SCENE

Анотація. *В статті досліджується феномен інформаційного тероризму на сучасному етапі та протидії йому. Найбільша увага сфокусована на таких поняттях як медіа та кібертероризм, що є основними складовими сучасного інформаційного тероризму. Висвітлено сутність даного явища, також охарактеризовано приклади запобігання інформаційному терору на міжнародному рівні.*

Ключові слова: *інформація, тероризм, інформаційний тероризм, кібертероризм, медіа-тероризм, інформаційний простір, ЗМІ.*

Аннотация. *В статье исследуется феномен информационного терроризма на современном этапе и противодействия ему. Наибольшее внимание сфокусировано на таких понятиях как медиа и кибертерроризм, которые являются основными составляющими современного информационного терроризма. Освещены сущность данного явления, также охарактеризованы примеры предотвращения информационном террора на международном уровне.*

Ключевые слова: *информация, терроризм, информационный терроризм, кибертерроризм, медиа-терроризм, информационное пространство, СМИ.*

Summary. *The article examines the phenomenon of terrorism information at this stage and counteract it. Most attention focuses on concepts such as media and cyberterrorism, which are major components of modern information terrorism. Deals with the essence of the phenomenon, described as examples of the information prevention of terrorism at the international scene.*

Key words: *information terrorism, information terrorism, cyberterrorism, media terrorism, information space, the media.*

Постановка наукової проблеми. Сучасні суспільні відносини вже виходять за рамки звичайного спілкування та отримання інформації з ЗМІ. Залежність людей від телефонів, Інтернету та соціальних мереж породжує нові досі не використані можливості маніпулювання та впливу, нові страхи перед невідомим, а розвиток інфраструктури в інформаційний простір та перехід державного управління на інформаційне поле обумовлює собою появу нових загроз національній, суспільній безпеці.

Виклад основного матеріалу. Кібертероризм, також відомий як електронний тероризм або інформаційний

терор за кордоном, може бути визначений як будь-який акт тероризму в інформаційному просторі, який включає в себе навмисні і широкомасштабні атаки для створення збоїв в комп'ютерних мережах з використанням комп'ютерних вірусів, інформаційної зброї або атак з використанням шкідливих програм, також атаки на окремих осіб, уряд і організації та корпорації міжнародного рівня тощо.

Кіберзлочинність часто мотивується економічною вигодою або інтернет-вандалізмом, для задовільнення потреб хакерів, на відміну від них кібертерор підживлюється ідеологією та мотивується обов'язковим розголосом в ЗМІ та мережі Інтернет, що викликає великий резонанс серед суспільства та виводить суб'єкт інформаційного терору на міжнародну арену в разі успішного досягнення мети.

Кібертероризм є актом інтернет тероризму, проявом терористичної діяльності, в тому числі акти навмисного, великомасштабного руйнування комп'ютерних мереж, програм, баз даних, навіювання, маніпулювання населенням, в особливості через персональні комп'ютери, підключені до Інтернету, та за допомогою інформаційних засобів, інструментів, таких як комп'ютерні віруси, штучні мережі, технічні засоби стеження та віддалені технології збору інформації тощо.

Кібертероризм спірний термін. Деякі автори вибирають дуже вузьке визначення, що відносяться до скоєння за допомогою відомих терористичних організацій, створення атак на інформаційні системи для досягнення первинної мети, створення тривоги і паніки. Деякі інші автори вибирають занадто широке визначення, яке має тенденцію помилково включати кіберзлочинність, коли в дійсності, кібертероризм і кіберзлочинність два зовсім різних питання, і повинні бути визначені окремо. Тероризм в Інтернеті слід розглядати, як кібертероризм, коли був створений маніпулятивний вплив на групу людей, наприклад навіювання жаху, в той час як кіберзлочинність є актом вчинення злочину або злочину в Інтернеті, як правило, без використання навіювання на населення. Кібертероризм можна також визначити як умисне використання комп'ютера, мереж та інтернету — громадськості, щоб викликати руйнування і шкоду для досягнення особистих цілей, наприклад вербування до угруповань нових потенційних терористів. Кібертерористи, їх угруповання, банди чи навіть організації, які дуже досвідчені з точки зору злому, можуть нанести величезної шкоди урядовим системам, лікарняним установам, і програмам національної безпеки, що вводить населення країни в стан смутку і страху перед очікуванням повторних атак. Мета таких терористів може бути політичною або ідеологічною, такі дії можна розглядати як форму тероризму.

Існує багато занепокоєння з боку урядових та медіа-джерел про потенційні збитки, які можуть бути викликані кібертероризмом, і це спонукає на дії служби спеціального призначення.

Аль-Каїда використовувала Інтернет, щоб спілкуватися зі своїми прихильниками і вербувати нових членів. Естонія, прибалтійська країна, яка постійно розвивається з точки зору технології, стала полем битви для кібертерористів в квітні 2007 року після суперечок, що стосуються вилучення радянського пам'ятника Другої світової війни, розташованого міста в Естонії – Таллін [1].

Існує дискусія з приводу основного визначення обсягу кібертероризму. Існує зміна кваліфікації по мотивації, цілям, методам, і використання комп'ютера як центрального засобу в акті. В залежності від контексту, кібертероризм може значно частіше пересікатися з кіберзлочинністю, інформаційною війною або звичайним тероризмом. Євген Касперський, засновник Лабораторії Касперського, стверджує, що термін «кібертероризм» є більш точним, ніж термін «кібервійна». Він стверджує, що «з досвіду вивчення сьогоднішніх атак, важко отримати інформацію про те хто це зробив, або коли вони будуть знову наносити удар. Той факт, що це поодинокі випадки, наводить на думку про терор, тому що наслідки не менш руйнівні для психіки суспільства, ніж при вибухах смертників, чи інших терористичних актах». Він також прирівнює великомасштабну кіберзброю, таку як Вірус Flame і NetTraveler вірус, які порівнюються за глобальними наслідками до біологічної зброї, тому що в них є потенціал, щоб бути настільки ж руйнівними [2].

В відміну від вірусу або комп'ютерної злочинності, що призводить до відмови в обслуговуванні, кібертерорист атакує з метою заподіяти фізичне насильство або екстремальні фінансові збитки чи оказати вплив на політичні події. За даними Комісії США щодо захисту життєво важливої інфраструктури, можливість збільшення випадків кібертероризму зростає. Включаючи банківську галузь, військові об'єкти, електростанції, центри управління повітряним рухом, а також системи водопостачання, сферу медицини та екологічної сфери.

Кібертероризм іноді називають електронним тероризмом або інформаційною війною, що включає в собі концепцію використання інформаційного тероризму.

За даними американського Федерального бюро розслідувань, кібертероризм є будь-який «навмисний, політично, релігійно, фанатично мотивований напад на інформаційний простір, комп'ютерні системи, комп'ютерні програми і дані, що призводить до насильства проти небойових цілей на субнаціональні групи або таємних агентів» [3].

Медіа-тероризм відноситься до специфічного різновиду інформаційно-психологічного терору та є складовою «інфраструктурного терору». Його сутність полягає у спробах шляхом організації спеціальних медіа-кампаній дестабілізувати суспільство, створити у ньому атмосферу громадянської непокори, недовіри суспільства до дій та намірів влади й особливо — її силових структур, покликаних захищати суспільний порядок.

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. Засобами здійснення медіа-тероризму є друковані ЗМІ, мережі ефірних й кабельних мас-медіа, Інтернет, електронна пошта, різноманітні електронні іграшки тощо. Необхідно зауважити, що більшість сучасних видів тероризму можна віднести до медіа-тероризму, адже ЗМІ виступають дієвим інструментом у швидкому поширенні інформації, залякуванні населення і досягненні терористами їхньої мети. Серед наслідків терористичної діяльності можна виділити економічні, соціальні, політичні та інші. Необхідно зауважити, що наслідки терористичної діяльності не завжди відповідають меті суб'єктів її здійснення. Таким чином, якщо користуватися запропонованою системою критеріїв, то можна визначити місце медіа-тероризму в типології тероризму. Медіа-тероризм представляє собою особливий вид терористичної діяльності, що виділений за критерієм використання інструментів (засобів) досягнення терористами власних цілей [4].

Висновки. Після десяти років затишшя тероризм знову повернувся до Європи. При цьому, на думку багатьох, такої терористичної активності не було ще ніколи. Це суб'єктивне сприйняття пов'язане з поширенням комунікацій, міжнародної мережі Інтернет. На тлі масового користування соціальними мережами та свободою ЗМІ. В наші дні тероризм більше тисне на свідомість і психіку людей, ніж раніше.

Передумовами виникнення інформаційного тероризму стали фінансова сторона — дешевизна, доступність будь якій категорії фахівців в медіа просторі та психології тощо, розвиток інформаційного суспільства в міжнародному просторі, прості методи та технології втілення, ефективність, скритність, безкарність. В свою чергу, інформаційний тероризм розділяється на інформаційно-психологічний тероризм та інформаційно-технічний тероризм. Контроль над ЗМІ з метою поширення дезінформації, чуток, демонстрації могутності терористичних організацій, завдання збитків окремим елементам і всьому інформаційному середовищу супротивника в цілому: руйнування елементної бази, активне придушення ліній зв'язку, штучне перезавантаження вузлів комунікації тощо.

Кібертероризм, або ж у більш загальному розумінні Інтернет-тероризм так бачать закордонні науковці та правознавці визначення будь якого прояву агресії, жаги до насильства та маніпулятивного впливу на населення через використання інформаційного ресурсу, та інформаційної зброї.

Можна виходячи з досвіду вивчення зарубіжних дослідників можна провести аналогію до кібертероризму, тобто в нашому розумінні інформаційний тероризм — прямий вплив на психіку і свідомість людей з метою формування потрібних думок і суджень, певним чином викликаючи потрібну поведінку людей. На практиці, під інформаційним тероризмом зазвичай мають на увазі такий насильницький пропагандистський вплив на психіку, який не залишає для людини можливостей критичного сприйняття реальності подій.

«Маючи приклади кримінальних атак на промислові об'єкти, маючи хакерів, які можуть створювати складні атаки, ми отримуємо кібертероризм — атаку на критичну інфраструктуру. Насправді, комп'ютерні програми керують усім, починаючи від електрики, транспорту, медицини ... На жаль, всі ці системи уразливі», — доповів Касперський в одній з конференцій.

Соціальні мережі (соц-мережі) — найбільш доступний і небезпечний засіб впливу на загальну масову думку людей. Соціальна мережа зараз є елементом масової культури.

Досвід вивчення таких мереж виявив декілька властивостей:

- Під час віртуального знаходження в соціальні мережі виникає почуття причасності до чогось більшого, важливого, та неосяжного.
- Мережі вже давно стали першочерговим джерелом конфіденціальної інформації про людей, їх дії, добову активність, повсякденну діяльність тощо.
- Так зване Альтер Его, самовпевненість сучасного індивіда, його свобода в діях та думках, його постійне віртуальне перебування в просторі яке він на його думку формує самостійно піддане вторгненням та провокаціям з метою інформаційного терору, чи маніпулювання, що викликає бажання індивіда робити також на інших, підштовхує до цього майже відсутність негативних наслідків для нього, безкарність, скритність.
- Свобода дій, майже нічим не обмежено, це негативно впливає на жагу до розвитку, так би мовити, відбувається деградація, коли при великій кількості можливостей активність понижається до мінімуму та з'являється псевдо думка повної захищеності від негативних наслідків.

Нещодавно прикладом практичного інформаційного протиборства стала подія, коли в грудні 2016 року найбільші соціальні мережі, такі як facebook, twiter, youtube, за підтримки microsoft об'єдналися для боротьби з контентом екстремістського змісту, блокування певного виду матеріалів, що викликають підозру на вміст пропаганди до насилля, порнографії, терористичних дій тощо.

Література

1. Terrorism, Intelligence and Homeland Security By Robert W. Taylor, Charles R. Swanson Amazon Sales Rank: #58371 in Books Published on: 2015-02-27 Original language: English 432 p.

2. Cyber criminals, terrorists and break-up of euro among biggest risks facing Ireland Gareth Morgan and Tom Brady [Електронний доступ] 16/05/2015 // Режим доступу до ресурсу: http://www.independent.ie

3. FBI about Terrorism [Електронний доступ] 2017 / Режим доступу до ресурсу: https://www.fbi.gov/investigate/terrorism

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