

*Котерлін І.Б. асистент кафедри соціальних комунікацій та права
Івано-Франківський національний технічний університет нафти і газу,
кафедра соціальних комунікацій та права*

Козут Х. М., Шевадуцька Л. Г. студенти 3 курсу ІГПДУ

Івано-Франківського національного університету нафти та газу

КОТЕРЛІН І. Б., КОГУТ Х. М., ШЕВАДУЦЬКА Л. Г.

ОСОБЛИВОСТІ ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ В ЕПОХУ ГЛОБАЛЬНОЇ ІНФОРМАТИЗАЦІЇ СВІТОВОГО ПРОСТОРУ

Сьогодні інформаційний тероризм як важливий чинник формування нового світового порядку перетворився на невід'ємний компонент міжнародних політичних процесів. Оперуючи Інтернет та ЗМІ ресурсами, він є значною загрозою національній безпеці, в умовах основних цивілізаційних тенденцій сучасності – глобалізації та інформатизації. Якщо на початку ХХ століття було достатньо захопити пошту та телеграф для того, щоб здобути перемогу в локальному перевороті, то тепер цього зовсім недостатньо. У світі інформаційного суспільства потрібно контролювати, якщо не увесь, то хоча б 70% інформаційного простору. Подача чи замовчуванням деяких матеріалів, створення правильних акцентів, для зміни суспільної думки – такі маніпуляції стали повсякденним явищем. Але останнім часом великої популярності набув інформаційний тероризм.

Для більш чіткого розуміння сутності поняття інформаційний тероризм слід звернутися до власне поняття «тероризму». Тероризм – це метод впливу шляхом здійснення теракту задля досягнення певних цілей. На сьогодні тероризм набув всесвітнього масштабу, перетворився на багатовимірне і багатоаспектне явище, яке дуже швидко еволюціонує, а отже – набуває міжнародного характеру. Тероризм складається з наступних складових: суб'єкт, об'єкт, причина та мотив, мета здійснення, часові й просторові характеристики, використовувані інструменти (засоби), наслідки [4].

На перший погляд інформаційний тероризм – явище не таке страхітливе. Немає вибухів, закривавлених трупів і криків поранених. Але якщо заглянути

глибше, відкривається не така вже й радісна картина [9, с.57]. В.О. Коршунов вказує, що інформаційний тероризм – це 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, с.257].

Досить часто поняття інформаційний тероризм плутають з поняттям інформаційної війни. Не зважаючи на схожість цих двох понять, між ними все ж є відмінності. Перша відмінність полягає у визначенні сторін протистояння. В інформаційній війні агресором виступає держава, етнос чи релігійна група. При цьому можна виділити початок війни, військові дії та кінець війни. Терористів ж сприймаються як злочинців. Друга відмінність полягає у причині виникнення. Для інформаційної війни такою причиною, як правило, може стати неузгодженість інтересів різних держав. Для тероризму такою причиною є існування в кожному конкретному суспільстві та у світі затяжних невирішених соціальних і політичних конфліктів. Третьою відмінністю є те, що у ході воєнної боротьби супротивники часто використовують однакові засоби. Антитерористична діяльність не може включати засоби, які використовують терористи [2, с.175].

Доступність інформаційних технологій значно підвищує ризики інформаційного тероризму. Розвиненість інформаційної інфраструктури суспільства сприяє створенню додаткових ризиків інформаційного тероризму. У свою чергу, інформаційний тероризм розділяють на інформаційно-психологічний тероризм, який передбачає контроль над ЗМІ з метою поширення дезінформації, чуток, демонстрації могутності терористичних організацій та на інформаційно-технічний тероризм метою якого є завдання збитків окремим елементам і всьому інформаційному середовищу супротивника в цілому [9, с.57].

Медіа-тероризм відноситься до специфічного різновиду інформаційно-психологічного 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 [4]. Для України, де інформаційна діяльність поки що не набула належного розвитку, головні загрози у сфері інформаційного тероризму є не внутрішніми, а зовнішніми. На сьогодні державою, яка робить безпосередні медіа-терористичні атаки на Україну, є Російська Федерація. Вона поширює фейкову інформацію через мережу Інтернет та ЗМІ. Особливо підпадають під вплив інформаційних атак люди, котрі регулярно дивляться російське телебачення та знайомляться з недостовірними відомостями. Варто лише поглянути на заголовки їхніх новин, щоб зрозуміти, що «доля України» їх ой як хвилює. Та навіть більше, до нашої держави їхнім ЗМІ є «більше інтересу», ніж до власних внутрішніх проблем. Протягом довгого часу російські медіа поширюють низку неправдивих історій про «звірства», які відбуваються в Україні. Так, у 2014 році на Первом каналі вийшов репортаж про розп'ятого хлопчика у місті Слов'янськ [3]. Часто новини переповнені іншим абсурдом. Прикладом може бути новина про те, що українських школярів нібито змушують знищувати снігурів, водночас вчителі начебто закликають дітей дбати про «патріотичних» синьо-жовтих синичок [7].

Тому сьогодні світ активно готується до того, щоб протидіяти будь-якій умисній шкоді не тільки людській свідомості, а й державній інформаційній безпеці. Так, нещодавно, служба безпеки Чехії (BIS) вперше у своїй історії оголосила набір студентів вишів на стажування за спеціалізаціями: «тероризм», «кібернетична безпека», «право», «інформаційні технології» – й триватиме тиждень. Речник чеської Служби безпеки та інформації Ян Шуберт зазначив: «Адже не будемо ми сидіти, склавши руки, і чекати, хто до нас прийде. З іншого боку, це у світі не є чимось надзвичайним» [5].

Наступним видом інформаційного тероризму є кібертероризм, як 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 [4]. Кібертероризм відносять до інформаційно-технічного тероризму. Він не має національних меж та в проблематичності виявлення терориста в інформаційному просторі [9, с.58]. Сьогодні кібертероризм набуває все більших масштабів. Так, минулого року були взламани поштові акаунти високопосадовців США. У мережу потрапила ймовірна переписка тоді ще кандидата в президенти США від Демократичної партії Гіллари Клінтон. Американська розвідка звинуватила у цих атаках Росію та підкреслила, що це було зроблено, щоб сфальсифікувати результати виборів на користь Дональда Трампа. «Ці крадіжки і розкриття інформації призначені для втручання в процес виборів в США. Така діяльність не є новою для Москви – росіяни використовували аналогічні тактики і техніки по всій Європі і Євразії, щоб, наприклад, вплинути там на громадську думку», – стверджували в американській розвідці [6]. Проте, кібертероризм націлений не тільки на держустанови та ключових осіб. Хакери не гребують й викраденням інформації звичайних людей та поширення через їхні акаунти неправдивої та провокативної інформації. Соціальна мережа Twitter була змушена заблокувати понад 125 тисяч облікових записів користувачів через терористичні погрози або за пропаганду тероризму, в першу чергу пов'язаних з Ісламською державою [1].

Хоч у світі досить нестійка ситуація у плані інформаційної безпеки, адже щодня здійснюються різноманітні кібератаки на системи різних держав, а також ведеться постійна маніпулятивна провокація з боку держав-агресорів, світ не стоїть на місці. Щодня впроваджують нові технології та засоби і людство хоче сказати терористам: «Технічні засоби не для вбивства. Вони для того, щоб зробити наше життя комфортнішим».

Список використаних джерел

1. Twitter заблокував понад 100 тис. акаунтів: [Електронний ресурс]. – Режим доступу: <http://ukranews.com/ua/news/408453-twitter-zablokuvav-ponad-100-tys-akauntiv>.

2. Єрохіна Т. Медіа-тероризм та інформаційна війна: до питання співвідношення [Текст] / Тетяна Єрохіна // Освіта регіону. – 2013. – № 4. – С. 171-176.
3. Ложь: распятие в эфире Первого канала: [Електронний ресурс]. – Режим доступу: <http://www.stopfake.org/lozh-raspyatie-v-efire-pervogo-kanala/>.
4. Матула М. Феномен інформаційного тероризму як загрози національній та міжнародній безпеці: [Електронний ресурс]. – Режим доступу: <http://naub.oa.edu.ua/2014/fenomen-informatsijnoho-teroryzmu-yak-zahrozy-natsionalnij-ta-mizhnarodnij-bezpetsi/>.
5. Служба безпеки Чехії оголосила набір студентів на стажування: [Електронний ресурс]. – Режим доступу: <http://www.radiosvoboda.org/a/28330767.html>.
6. США офіційно звинуватила Росію в організації хакерських атак: [Електронний ресурс]. – Режим доступу: http://ostannipodii.com/a/201610/ssha_oficiyno_zvinuvatila_rosiyu_v_organizaciyi_hakerskih_atak-100012711/.
7. Фейкові новини від російських ЗМІ: полювання на снігурів, «мученики Новоросії» та заборона Діда Мороза: [Електронний ресурс]. – Режим доступу: <http://tyzhden.ua/News/126136>.
8. Форос Г. В. Інформаційний тероризм як загроза національній безпеці України [Текст] / Г. В. Форос, А. В. Форос // Правова держава. – 2010. – № 12. – С. 256-261.
9. Яцик Т. П. Особливості інформаційного тероризму як одного із способів інформаційної війни [Текст] / Т.П. Яцик// Науковий вісник Національного університету ДПС України (економіка, право). – 2014. – № 2. – С. 55-60.