МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ МІЖНАРОДНИХ ВІДНОСИН
КАФЕДРА МІЖНАРОДНИХ ВІДНОСИН, ІНФОРМАЦІЇ ТА РЕГІОНАЛЬНИХ СТУДІЙ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____ Ніна РЖЕВСЬКА
«___»_____ 2022 р.

КВАЛІФІКАЦІЙНА РОБОТА
ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТРА
СПЕЦІАЛЬНОСТІ 291 «МІЖНАРОДНІ ВІДНОСИНИ, СУСПІЛЬНІ КОМУНІКАЦІЇ ТА РЕГІОНАЛЬНІ СТУДІЇ»
ОСВІТНЬО-ПРОФЕСІЙНОЇ ПРОГРАМИ
«МІЖНАРОДНА ІНФОРМАЦІЯ»

Тема : «ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ ЯК ЗАГРОЗА МІЖНАРОДНІЙ БЕЗПЕЦІ»

Виконавець : здобувач вищої освіти 2 курсу, 208 М групи, Гриценко Михайло Олександрович

Керівник : к.і.н., доц., доцент кафедри міжнародних відносин, інформації та регіональних студій Дерев'янко Ігор Петрович

Нормоконтролер _____ Олексій МЕНДРИН
(підпис)

КИЇВ 2022

ЗМІСТ

ВСТУП

Актуальність теми. Сучасне суспільство розвивається швидкими темпами, йдучи динамічно вперед. Паралельно активно відбувається оновлення технологій, соціальних мереж та супутникового зв'язку. Людство звикло розпочинати свій день з перегляду новин в Інтернеті, акаунтів в соціальних мережах та фактично витрачає весь вільний час на це. Тотальна комп'ютеризація та інформатизація створюють потребу в постійному моніторингу розвитку інформаційних систем, гаджетів, способів комунікації.

Щоденні великі потоки інформації створюють загрозу для її якісного осмислення людиною. Всесвітня мережа Інтернет наповнена різноформатною інформацією, яка часто є неперевіреною, фейковою та має, в більшій мірі, маніпулятивний характер. Люди стають жертвами згубного впливу на їх психіку за рахунок споживання такої інформації. На жаль, в теперішній час не всі можуть виявити маніпулятивні технології, що застосовуються в інформаційних потоках, особливо молодь, яка найбільше часу «блукає у Всесвітньому павутинні» в пошуках цікавої інформації.

Варто відзначити, що суспільні настрої легко змінити розповсюдивши будь-яку інформацію провокаційного характеру. Користувачами мережі виступають не лише законослухняні громадяни, а й вороже налаштовані представники терористичних організацій. Трансформація світу створила передумови для переходу терористів на новий, інформаційний рівень. Вони тепер несуть загрозу не лише фізичну, а й психічну. Терористи, які перейшли в інформаційний простір, несуть більш масштабніші руйнівні наслідки, які не завжди можна передбачити.

Крім того, інформаційні терористи мають інструменти не лише для залякування та маніпулювання людей, а й використовують Інтернет задля вербування у власні організації. Враховуючи вищезазначене, на нашу думку, актуальним є вивчення інформаційного тероризму як нового явища в інформаційному суспільстві. Варто зазначити, що ця тема виникла порівняно

недавно, а відтак, наукових робіт та ґрунтовних досліджень з приводу визначення природи, ознак, першопричин та наслідків інформаційного тероризму майже немає.

Проте, в науковому обігу давно існує поняття «інформаційна війна». На мою думку, інформаційний тероризм це один із проявів такої війни. Тому доцільно розглядати роботи вчених і з питань виникнення та ведення інформаційної війни. Слід відзначити, що над даними питаннями працювало ряд науковців, серед яких : Банк Р.О., Ємельянов В.П., Кротюк В.А., Кульба В.А., Митко А.М., Свентицька О.В., Саган О.С. та ін.

Мета і завдання дослідження. Метою випускної кваліфікаційної роботи є вивчення поняття, прояву тенденцій та особливостей інформаційного тероризму в XXI столітті в умовах інформаційного суспільства.

На основі визначеної мети були поставлені наступні завдання :

– дослідити поняття інформаційного тероризму;

– розглянути вербування як стратегічний інструмент залучення в інформаційний тероризм;

– розкрити пропаганду з позиції дієвого інструменту інформаційного тероризму;

– дослідити засоби масової інформації як інструмент впливу терористів;

– осмислити можливості протидії тероризму в інформаційній сфері.

Об’єкт дослідження – суспільні відносини, які виникають під час протидії інформаційному тероризму в мережі Інтернет та засобах масової інформації.

Предмет дослідження – інформаційний тероризм як загроза міжнародній безпеці.

Методи дослідження. Основою підходу до вивчення теми стало застосування принципів історизму, системності та діалектичності у вирішенні поставлених завдань. Що стосується використаних в дослідженні методів, то серед них можна назвати загальнонаукові методи : спостереження,

систематизації явищ, методи структурно-функціонального аналізу, контент-аналізу, дедукції, індукції, а також елементи методу експертних оцінок. У дослідженні застосовувався також нормативно-ціннісний підхід, що припускає оцінку встановлених фактів з точки зору їх сприйняття.

Структура роботи. ВКР складається зі вступу, трьох розділів, висновків та списку використаних джерел. Загальний обсяг роботи становить 86 сторінок, список використаних джерел містить 70 найменувань.

РОЗДІЛ 1
ТЕРОРИЗМ ЯК СОЦІАЛЬНО-ПОЛІТИЧНЕ ЯВИЩЕ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

1.1. Поняття інформаційного тероризму

Вивчення явища інформаційного тероризму неможливе без розгляду ключових, на наш погляд понять, які паралельно існують і розвиваються в науці інформаційного права. В першу чергу слід відзначити саму суть впливу інформаційного тероризму, який націлений в першу чергу на безпеку людини.

Тлумачення терміну «безпека» доцільно розглядати крізь призму уявлень та трактувань науковців, а також його законодавчого закріплення. Сучасне українське законодавство не має чіткого закріплення цього терміну. Проте, в законі України «Про національну безпеку України» є його 4 видових підпоняття, а саме «воєнна безпека», «громадська безпека і порядок», «державна безпека», «національна безпека» [51]. Але дані поняття фактично можна розглядати лише тоді, коли йде посягання фізичного плану на безпеку загалом. Ми у нашому дослідженні будемо розглядати інший вид безпеки – інформаційну.

Поки що, тлумачення даного терміну можна відшукати виключно у наукових доробках, адже спеціального закону, який би закріплював дане поняття на даний час немає. Це є суттєвим недоліком нашого законодавства, адже зараз в Україні йде війна, в тому числі інформаційна, відповідно прийняття такого закону має бути терміновим. І. М. Стойком, О. І. Кузьмуком, Ю. М. Сиротюком 28.05.2014 року за реєстраційним номером 4949 було зареєстровано Проєкт закону України «Про засади інформаційної безпеки України» [50], в якому розкривається змістовне формулювання поняття «інформаційної безпеки України».

Так, на їх думку, інформаційна безпека – стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому

запобігається завдання шкоди через неповноту, несвоєчасність та недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій [50].

Слід акцентувати увагу на тому, що на поточний момент, діє Указ Президента України «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» [52]. Даним указом було введена в дію вищезазначена стратегія на період до 2025 року. В ній дається чітке тлумачення терміну «інформаційна безпека України».

Так, під інформаційною безпекою України розуміється складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [52].

Як бачимо, два погляди на інформаційну безпеку нашої держави збігаються хіба що в розповсюдженні інформації, яка спричиняє загрозу національній безпеці. Отже, зрозумівши основу в змістовному наповненні поняття «інформаційна безпека», перейдемо до розгляду самого явища інформаційного тероризму.

О.В. Саган в дисертаційному дослідженні «Протидія медіа-інформаційному тероризму як питання національної безпеки України» відзначає, що поява такого явища як інформаційний тероризм відбулася на початку 90-х років XX століття [25, с.59]. На її думку, поява нових медіа була детермінантом виникнення можливості у терористів перейти в нову сферу ідеологічного впливу на людей.

За словами О.В. Саган, вільні потоки інформації за допомогою слова не тільки людину формують і викликають емоційні стани, але й здійснюють руйнівну дію на її цілісність [60, с.59]. Явище інформаційного тероризму вона розглядає як 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.

Цікавим на мій погляд, є тлумачення інформаційного тероризму фахівців у галузі безпекознавства, політології та державного управління В.О. Коршунова та Т.П. Яцик. Так, В.О. Коршунов відзначає, що інформаційний тероризм – це новітній вид тероризму, орієнтування його йде на використання засобів і методів виведення з ладу інформаційної інфраструктури держави чи її елементів. Також він підтверджує тезу про те, що дані дії можуть вчиняти задля тяжких наслідків для різних сторін життєдіяльності особистості, суспільства і держави [28, с. 6].

На думку Т.П. Яцик, сучасний інформаційний тероризм розкривається як множина інформаційних війн та спецоперацій, які можуть створюватися національними або транснаціональними кримінальними структурами та спецслужбами іноземних держав [63, с. 57].

К.С. Герасименко вважає, що в інформаційному тероризмі приймають пряму участь спеціально створені медіа-кампанії, задля дестабілізації суспільства шляхом впливу на їх настрої провокативними матеріалами проти дій влади, створенні атмосфери громадянської непокори, супротиву правоохоронним органам, підбурення населення [15, с.163].

В. І. Рюміна вбачає в інформаційному тероризмі форму негативного впливу на особистість, суспільство і державу, що здійснюється всіма можливими видами інформації. Мета такої діяльності на її думку, полягає в ослабленні та розхитуванні конституційного ладу [59, с.268].

М. Джерольд вбачає у інформаційному тероризмі умисне зловживання цифровими інформаційними системами, мережами або іншими технологічними розробками з метою здійснення терористичних операцій або атак [67].

К. Вебб розглядає інформаційний тероризм як навмисне та асиметричне проведення недержавним суб'єктом інформаційної діяльності, поширення інформації, щоб реалізувати свою метою сприяння масовим терористичним актам та/або вплинути і порушити безпеку та/або добробут нації чи низки націй [70].

На його думку це робиться для :

– конкретним чином впливати на зміни у сприйнятті цільової аудиторії та керувати ними;

– проведення ринкової токсичної пропаганди, щоб через страх впливати на засоби існування та волю цільової громадськості;

– захисту себе від діяльності союзників, конкурентів і супротивників [70].

Дж. Аркілла відзначає, що медіа-орієнтовані заходи інформаційного тероризму, спрямовані скоріше на залучення, ніж примус і впливають на безпеку суспільства, військового або іншого суб'єкта. Психологічний зрив може стати такою ж важливою метою, як і фізичне руйнування. На його думку, загрози інформаційної ери, ймовірно, будуть більш дифузними, дисперсними, багатовимірними і неоднозначними, ніж традиційні загрози [64].

На думку Дороті Е. Деннінг, терористи наступальними інформаційними операції прагнуть створити диспропорцію. Це досягається за допомогою операцій, які руйнують, порушують, погіршують, заперечують, обманюють, використовують або впливають через інформацію, інформаційні системи та

прийняття рішень. На її думку, терористи вміють поєднувати свої фізичні акти насильства з інформаційними операціями. Вони роблять аудіо- та відеозаписи інцидентів для розповсюдження в Інтернеті та на телебаченні. Їх насильство стає театральною виставою, поставленою для психологічного впливу в ЗМІ [65].

Експерти в США відзначають формування «великих масивів даних» на базі мобільних пристроїв зв'язку і телекомунікації. Більше 70 % населення Землі користуються мобільними засобами зв'язку, що формують так звані великі масиви даних (понад 2,5 трлн. байт інформації в добу). Здатність спеціальних органів збирати і обробляти значні обсяги даних, стане основою для розуміння потреб і причин дій окремих користувачів і груп осіб.

Для правильного розуміння і досягнення інформаційної переваги у визначенні терміну «інформаційна операція» має бути чітко відображене значення двох концептуально неоднакових, але тісно взаємопов'язаних понять : «інформація в бойових діях», що означає використання інформації для досягнення перемоги і «інформаційна війна», що означає проведення наступальних і оборонних операцій в інформаційному протиборстві для захисту власних інформаційних систем і ресурсів, або для впливу на інформацію та інформаційні системи противника [11, с.144].

Оборонні інформаційні операції повинні проводитися безперервно, подібно стратегічній ППО, а наступальні інформаційні операції – в основному під час конфліктних і кризових ситуацій. Інформаційна війна включає проведення таких дій, як психологічні операції, фізичні та інформаційні (кібернетичні) нападу і здійснення різних програм оборонних дій. Слід особливо підкреслити, що інформаційна війна охоплює широкий спектр ситуацій від миру до війни [8, с.40].

Інформаційний напад – атака з використанням комп'ютерних програмних засобів, яка полягає у використанні інформаційних технологій і програмних і інших засобів для впливу на інформацію та інформаційні системи противника з метою порушення нормального функціонування його

систем командування і управління. При цьому можуть використовуватися такі способи, як видалення записів, маніпуляції з даними, введення неправдивої інформації, зараження вірусами, створення перевантажень і ін. [61, с.41]

У друкованих виданнях виражаються різні оцінки інформаційних операцій. Прихильники однієї точки зору вважають, що інформаційні операції – це інструмент, що дає можливість політичному і військовому керівництву приймати більш обґрунтовані рішення. Це точку зору іноді називають «війною на основі нових або розширених підходів». Такий підхід може бути реалізований на основі вдосконалення методів сучасної пропаганди з використанням цифрової техніки для маніпулювання «правдою» [8, с.40].

Прихильники іншої точки зору вважають, що інформаційні операції – це засіб руйнування соціальної структури держави, дезорганізації її систем транспорту та зв'язку, водо- та енергопостачання, фінансових і банківських установ. Операції в кіберпросторі використовуються в інтересах проведення стратегічних військових операцій і порушення нормального функціонування або руйнування національних інформаційних інфраструктур. Незважаючи на певні відмінності в цих точках зору, вони сходяться в оцінці можливого впливу інформаційних операцій на життєво важливі інфраструктури держав [5, с.102].

Слід звернути увагу на те, що подальше і неминуче поширення цифрових технологій на національному, міжнародному і глобальному рівнях представляє велику небезпеку. Ці технології дають можливість порушувати роботу системи або систем без витрат на це мільйонів доларів. Разом з тим інформаційні атаки не становлять великих загроз і небезпек для країн, де інформаційні технології і застосування цифрової техніки знаходяться на початкових рівнях розвитку і використання. Це слід враховувати при виникненні конфліктів в таких регіонах [11, с.143].

Детальний аналіз інформаційних операцій показує, що розуміння і оцінка їх значення можливі тільки з урахуванням складності всіх змін, що відбуваються в сучасних соціальної та військовій сферах. Інформаційні

операції проводяться в кібернетичному просторі, перекриваються інформаційними інфраструктурами трьох рівнів : військовими, національними та міжнародними. На всіх цих рівнях можливі інформаційні атаки на системи командування і управління, тому такі системи вимагають надійного захисту і оборони.

О.В. Бойченко розглядає такі види інформаційного тероризму, як : медіа-тероризм та кібертероризм [6, с.231]. З цих назв розуміємо, що в першому понятті основною базою, що використовується терористами для розповсюдження інформації використовуються засоби медіа, до яких можна віднести : телебачення, радіомовлення, друковані видання, а в другому – Інтернет-простір, обчислювальні системи, апаратура передачі даних.

За твердженням Б. Д. Леонова, інформаційний тероризм в наукових працях частіше розглядається виключно в межах інтелектуальної сфери. Це він пояснює тим, що інформаційний тероризм є одним із найбільш сучасних та перспективних видів тероризму, який діє безпосередньо в інтелектуальній сфері та породжує насильство в кіберпросторі, яке спрямовується проти будь-кого. Також на його думку ключовим аспектом успіху цього виду тероризму є не груба сила, а нейрони [32, с.172].

На думку В. В. Пивоварова кіберзлочинність є сукупністю злочинів, які вчиняються у кіберпросторі шляхом використання комп’ютерних систем або комп’ютерних мереж чи інших засобів, у межах або проти комп’ютерних систем або мереж і комп’ютерних даних [45, с.178].

На нашу думку, більш небезпечним є саме кібертероризм, адже на планеті суттєво зменшилась кількість людей, які до сих пір купують друковану пресу, слухають радіо та дивляться телебачення. Принаймні, відсоток людей, які звикли отримувати інформації з традиційних медіа значно нижчий від тих, які черпають інформацію з мережі Інтернет [10, с.118].

Підсумовуючи, можемо сказати, що понятійний апарат інформаційного тероризму є доволі різностороннім. Кожне тлумачення терміну «інформаційний тероризм» розкриває змістовну сутність цього явища.

Спільними ознаками інформаційного тероризму, виходячи з аналізу представлених думок дослідників, слід виокремити наступні :

– інформація, що розповсюджується терористами націлена на психічний та маніпулятивний вплив на особистість;

– розповсюдження інформації відбувається за рахунок використання технічних пристроїв, комп'ютерів, комп'ютерних мереж, Інтернету та медіа ресурсів;

– має явно виражений негативних характер змістовного наповнення інформації;

– використовується задля посягання на безпеку конкретного індивіда, групи людей, держави чи нації (націй).

1.2. Вербування як стратегічний інструмент залучення в інформаційний тероризм

Вербування (від нім. werbung) – найм людей на військову службу [26, с.13]. Міжнародна конвенція про боротьбу з вербуванням, використанням, фінансуванням та навчанням найманців від 4 грудня 1989 року звертає увагу на суспільну небезпеку вербування найманців для вчинення насильницьких дій, що підривають конституційний порядок держав [39].

Відповідно до ч. 1 ст. 6 Конвенції Ради Європи про запобігання тероризму від 16 травня 2005 року «вербування терористів» означає залучення іншої особи до вчинення або участі у вчиненні терористичних злочинів, або до приєднання до якогось об'єднання чи групи з метою сприяння скоєнню цим об'єднанням терористичних злочинів [49].

Дії з вербування терористів спрямовані на пошук кандидатів як для участі в діяльності терористичної організації, так і в разових терористичних актах. Вербування закінчується висловленням згоди особи взяти участь у таких діях. Озброєння – це оснащення окремих терористів або терористичної організації (її підрозділів) зброєю, до якої належать будь-які види продукції

військового призначення, у тому числі бойова вогнепальна зброя, навігаційні прилади та радіолокаційна апаратура військового призначення.

Навчання терористів – це система засобів передачі знань та умінь, основою якої виступає моделювання терористичного процесу, з метою прищеплення навичок диверсійної діяльності, підвищення фізичної готовності, наприклад, навчання прийомів мінування, виготовлення з підручних матеріалів вибухових пристроїв тощо [24].

У програми навчання терористів зазвичай входять : вивчення методів збору інформації, підробки документів, використання вибухових речовин та різних видів вогнепальної зброї, правил конспірації, способів вербування агентури, правил керування повітряними, водними та залізничними транспортними засобами та ін.

В даний час терористи не зупиняються і прагнуть поповнити свої ряди всі можливі методи, щоб залучити якнайбільше людей у своє угрупування. Саме в Інтернеті така змога зростає. Від розуміння того, як вони впливають на новобранців, залежить протидія ефективності такого вербування та посилення боротьби з тероризмом.

Першим кроком, що перешкоджає набору в такі організації, є розуміння їхньої роботи, інструментів, якими вони користуються і чому. Постараємося розібратися у структурі процесу найму, визначимо модель залучення нових членів до терористичних організацій, розглянемо характеристики потенційних новобранців.

Щоб краще зрозуміти, хто і які типи людей вербує в терористи, слід проаналізувати результати соціально-психологічних та соціологічних досліджень у сфері вербування в екстремістських та тоталітарних організаціях. Слід оцінити, які методи вербування використовують терористичні організації для залучення потенційних новобранців : або через засоби масової інформації, або в особистих контактах у незвичній обстановці, наприклад, у в'язницях чи напіввійськових тренувальних таборах.

Терористи працюють за трьома напрямками : одні наводять на новобранців, інші мотивують їх, а треті вербують. Перші займаються пошуком слабохарактерних людей. Другі займаються вивченням цих людей та їх характерів. А вже наприкінці з'являється вербувальник, який звертається до ідеології терористичних організацій і пропонує різні блага [55, с.406].

Новобранцями терористичних організацій є аудиторія, пов'язана з культурною, соціальною та історичною ситуацією. Наприклад, терористи заохочують молодь, яка залишила свої будинки і приєдналася до військових організацій, спираючись на патріотичні цінності. Маргінальні чи незаконні (злочинні) групи можуть маскуватися шляхом зміни діяльностей, імен, одягу, щоб уникнути втручання правоохоронних органів. Ця організаційна адаптація може відбуватися, наприклад, у місцях позбавлення волі, школах тощо [55, с.406].

Ось короткий огляд деяких психологічних та демографічних змінних новобранців :

– проживання в районі з високим рівнем злочинів чи незадоволеності;

– культурна деградація і розчарування, нереалізовані ідеали;

– відсутність позитивної релігійної системи переконань або системи цінностей;

– дисфункція в сімейній системі;

– підвищена навіюваність особистості, низька толерантність до невизначеності.

Отже, немає жодного рівномірного сталого процесу набору терористичних груп, скоріше можна говорити про процеси найму (вербування) у різних регіонах та пунктах, у яких група вербувальників здійснює свою діяльність. Незважаючи на те, що можуть існувати подібності між методами вербування в одному місці та в іншому, там також будуть і відмінності.

Наприклад, в одному місці (скажімо, тренувальному таборі) вербувальник може користуватися відкритим, публічним доступом до аудиторії, в той же час в іншому (наприклад, у в'язниці) йому, можливо, доведеться діяти таємно. Крім того, характеристики будь-якого регіонального процесу вербування змінюватимуться з часом, як і обставини такої діяльності. Деякі методи вербування можуть бути ефективнішими в одному місці, ніж в іншому. Так, може бути ефективним втручання, коли вербувальник зміцнить волю антиурядових сил [24, с.58].

Конкретну характеристику будь-якого процесу набору можна назвати його формою поєднання як загальної картини, так і конкретних моделей. Для зручності оцінки заходи мають бути класифіковані за зразками та моделями. Незважаючи на те, що існує їх величезна різноманітність, огляд літератури з вербування в терористичні групи показує кілька загальних структур. Наведу деякі приклади.

– Мережа. У шаблоні «мережа» населення загалом сприймається як основа вербування. Вся аудиторія сприймається як однорідна і сприйнятлива, як недиференційована партія товару. Серед ключових різноманітностей, які є в цій моделі, є географія та демографічні подібності/відмінності між членами аудиторій. Наприклад, місцем, де такий підхід є кращим для терористичних організацій, є мечеть на чолі з імамом, широко визнаним «радикалом». Ті, хто відвідує таку точку, готові отримати відповідну інформацію без додаткової підготовки. На регіональному рівні ця модель буде найефективніша в таких місцях, де населення найбільше симпатизує радикалам.

– Воронка. Вербувальник може використовувати поетапний підхід, коли він вважає, що група населення при значній трансформації в ідентичності та мотивації вже дозріла для вербування. Даний підхід може бути охарактеризований етапами ритуалів та групових вправ, коли відбувається перевірка готовності використання насильства для досягнення цілей. Ці методи можуть призвести до того, що навіть ті, хто випливають з процесу

вербування, ще можуть бути повернуті назад, наприклад, шляхом розробки позитивного відношення до групи, що вже створилася, як проміжна ланка.

– Інфекція. Найчастіше найефективнішим методом вербування населення є залучення новобранців зсередини. Агент може бути занурений в таку групу для того, щоб згуртувати новобранців через прямі та особисті заклики. Цей метод вербування застосовується щодо груп, які активно виступають проти уряду. «Зараження» може бути найуспішнішим для терористичної групи в таких організаціях, як поліція чи військові, де більшість членів не є екстремістами. У цьому випадку завербувати агента для використання його в подальшому як вербувальника, можна з окремих членів, які незадоволені своєю роботою або мають образу, наприклад, на поліцію, військову організацію або уряд.

– Зерно кристалу. Часто аудиторія знаходиться так далеко або так недоступно, що довірений агент не може бути введений до неї. І тут вербувальник може шукати контакт для самостійних кадрів. Цей процес можна порівняти зі зниженням температури скла : спочатку вода охолоджується всередині, а потім крижані кристали утворюють зерна повного заморожування. До «зерна кристалу» включаються навколишні сили, які використовуються для «охолодження скла» та довговічності «заморожування». Цей підхід може бути успішнішим для діаспор або популяцій [62, с.218].

Вищезазначений перелік не є вичерпним, а лише ілюструє загальні закономірності підбору осіб в терористичну організацію. Крім того, ці форми можна розглядати як спрощені гіпотези дослідження процесу вербування. Будь-яка спроба вербування використовує переконливі інструменти : прямі (наприклад, пряме запрошення особи брати участь у напіввоєнних тренуваннях) або опосередковані (наприклад, політичні заяви та заклики, розміщені на веб-сайтах) .

Ці інструменти включають всі доступні форми : ЗМІ, які використовуються сьогодні (наприклад, газети, радіо, телебачення та

Інтернет), а також міжособистісний соціальний вплив (наприклад, проповіді, чутки, освіта та навчання). Часто використовують кілька інструментів для додаткового ефекту [25, с.107]. Наприклад, написання підручників, які підтримують ідеологію терористичної групи, а потім створення шкіл, в яких можуть бути використані ці підручники для навчання.

Розглянемо такі прийоми вербування :

1. Безпосередній. Набір новобранців у цьому секторі проводиться безпосередньо «віч-на-віч» або в невеликій групі, в умовах видимості для публіки або органів. Місця позбавлення волі, табори біженців, а також особи, які мають великомасштабний військовий досвід (наприклад, життя під час окупації), є яскравими параметрами. Робота з вербування не закінчується після того, як терориста заарештовано і позбавлено волі. Підбір може відбутися і в цих умовах, і може звести нанівець успіх арешту шляхом створення низки нових рекрутів із тюремного контингенту.

2. Громадський та опосередкований. У цьому секторі підбір новобранців, як правило, більше схожий на пропаганду, ніж на вербування. ЗМІ використовуються як у межах закону (наприклад, телебачення), так і поза законом (наприклад, графіті). ЗМІ-канали включають веб-сайти, які не захищені паролями. Фізична безпосередність не є можливою та стійкою. Наприклад, «Аль-Каїда» періодично випускає інформацію про терористів (відео) і робить заяви в різних газетах, засуджуючи Сполучені Штати та інші країни та їхню роль в Іраку та Ізраїлі.

3. Приватний. Методи комунікації у цьому секторі, як правило, використовуються у найбільш приватній обстановці, наприклад, у соціальних мережах. Такі методи підходять для тих груп людей, які працюють поза увагою влади або в опозиції до них. Вербувальники часто використовують однолітків, зокрема родичів.

4. Індивідуальний та опосередкований. Підбір у цьому секторі поєднує у собі ЗМІ-підхід і включає виробництво літератури і таємне її поширення для широкої аудиторії. З погляду технологій, цей сектор включає

захищені паролем веб-сайти, обмежений Інтернет, чат-групи і підпільну пропаганду цифрового відео [62, с.219].

1.3. Пропаганда – дієвий інструмент інформаційного тероризму

Термін «пропаганда» (від лат. Propaganda – поширення) має багато наукових визначень, з яких в якості основних можна виділити наступні :

1) система діяльності, спрямована на поширення знань, цінностей і іншої інформації з метою формування певних поглядів, уявлень, емоційних станів, надання впливу на соціальну поведінку людей;

2) поширення в масах ідеології та політики певних класів, партій, держав;

3) засоби маніпуляції масовою свідомістю [34, с.24].

На початку XX століття багато дослідників приділяли пропаганді найпильнішу увагу. Закономірності поведінки «мас» виявляли Г. Лебон, Е. Канетті, Х. Ортега-і-Гассет. Вивчення пропаганди, її організації та технік, велося після Першої Світової війни найбільш інтенсивно у Німеччині, Великій Британії та США. Незалежно від політичного режиму характер досліджуваного явища приводив авторів до більш-менш подібних висновків про її майже безмежну всемогутність в управлінні суспільством [48, с.102].

Виходячи з мети владного об'єднання масових аудиторій, пропаганда того періоду апелює та адресує своє повідомлення саме широким масам людей, адже немає сенсу проповідувати доктрину інтелектуалам, так як вони можуть самостійно сформувати свою думку, тому основна мета пропаганди – внести певні теми у поле бачення мас.

Після Другої світової війни пропаганда стала зброєю у світовому процесі ідеологічного зіткнення у період між локальними військово-політичними конфліктами. Вивчення історії розвитку поглядів на пропаганду як політичну технологію дозволяє виділити кілька підходів до її аналізу. Хоча їх поділ видається досить умовним, проте, без нього обійтися не можна, оскільки

дозволяє як вичленувати особливості пропагандистського впливу з різних сфер життя і сформувати цілісне уявлення про це досить складне явище.

Психологічний підхід досліджує питання про механізми пропагандистської дії переважно на рівні формування установок та процесів стереотипізації. Характерною особливістю цього підходу є його орієнтованість вивчення стереотипізації як властивості високоорганізованої матерії – мозку.

Підхід до пропаганди як до системи інформаційного контролю виходить з тези, що, будучи найважливішим управлінським ресурсом сучасного та постіндустріального суспільства, засоби масової інформації завжди знаходяться під тією чи іншою формою державного контролю. У зв'язку з тим, що держава не може дозволити собі відмовитися від контролю за мас-медіа, в даний час пропаганда є системою глобального інформаційного контролю, елементи якої включені практично в усі соціально значущі процеси [53, с.65].

Концепт пропаганди як інформаційно-психологічної операції зазвичай прийнято пов'язувати з такими поняттями як «психологічна війна», «інформаційна війна», «психологічна зброя» тощо. Принципова відмінність даного підходу від усіх інших полягає в тому, що він досліджує насамперед можливості та наслідки пропаганди «на ворога» (тут «ворог» – це людина з переконаннями, протилежними тим, у яких зацікавлений комунікатор), який, як правило (але не обов'язково), знаходиться за межами держави, яка ініціює таку пропаганду. Широке практичне застосування такої пропаганди у Світових війнах вже наприкінці 1940-х років дозволило провести узагальнення не лише способів та методів інформаційної війни, а й їхніх наслідків [55, с.406].

Соціологічний підхід до вивчення пропаганди виявляє неймовірну різноманітність у дефініціях, що пов’язане з наступним чинником : метою соціологічного підходу є визначення закономірностей впливу пропаганди на суспільні відносини. При цьому об'єкт пропаганди, не вдаючись у суть предмету, позначають як «свідомість мас», як «суспільну психологію» чи

«ціннісні орієнтації», як «психологічні установки» чи «суспільну думку». У зв'язку з такою різноманітністю одним із ключових питань тут є питання про те, куди спрямовуються інформаційні потоки, що синтезуються в процесі пропагандистського впливу, що прагнуть змінити або, навпаки, утримати під контролем з погляду соціології.

Системний підхід розглядає пропаганду як комплексне явище, що тісно взаємопов'язане з різними сторонами життя суспільства. Системний підхід до аналізу пропагандистської діяльності активно розроблявся в Радянському Союзі в основному щодо аналізу результативності впливу. При цьому наголошувалося на загальному методологічному значенні визнання різноманіття суспільних і політичних зв'язків [34, с. 77].

Кожен із перелічених підходів є самостійним напрямом у вивченні впливу пропаганди на суспільство. Природно, що розвиваються вони не ізольовано, тому іноді досить складно віднести ту чи іншу дефініцію до певного підходу. Разом з тим, кожен з них концентрує свою увагу на певному аспекті пропаганди, дозволяючи поглянути на неї зі своєї унікальної точки зору. Однак є одна обставина, яка дозволяє говорити про те, що пропаганда – це насамперед явище політичне : кожен із наведених підходів до вивчення цього складного явища зрештою визначає пропаганду як явну чи неявну технологію управління суспільством через формування певної системи світогляду.

Таким чином, можемо підсумувати, що пропаганда – багатоелементна технологія орієнтована на управління суспільством, шляхом формування в реципієнтів міцних соціальних установок і стереотипів, що відповідають інтересам комунікатора.

У найбільш загальному вигляді мета пропаганди – це :

1) впливати (як максимум – формувати) на світогляд суспільства загалом та кожного його члена зокрема;

2) забезпечувати спадкоємність цінностей та світогляду;

3) «виробляти імунітет» до сприйняття інших цінностей.

Чинниками пропаганди є :

1. Чим більший розрив між досвідом людей та ідеєю, тим більше брехні у пропагандиста.

2. Пропаганда має орієнтуватися на референтні групи.

Всі цілі пропаганди можна класифікувати на стратегічні (перспективні) і тактичні (поточні, ситуаційні, разові, вузькоспеціалізовані). Зрозуміло, що такий розподіл є умовним. Насправді цілі пропаганди, тісно переплітаються між собою в реальній обстановці, виступають як єдине нерозривне ціле. Принципове значення для успіху пропаганди має оптимальний вибір мети, яка впливає на ряд зовнішніх і внутрішніх чинників [53, с.118].

До зовнішніх чинників слід зарахувати такі :

– потреби соціального управління;

– комунікаційна обстановка;

– зміст та новизна положень, що затверджуються пропагандою;

– особливості аудиторії.

Внутрішні чинники включають :

– характеристики джерела пропаганди;

– обсяг інформації, що є у розпорядженні пропагандиста;

– жанрові та типологічні особливості пропагандистського матеріалу [53, с.121].

Видами пропаганди є :

– «біла» пропаганда (відоме джерело, правдиве повідомлення). Не маскує своїх цілей, спирається на правду.

– «Сіра» пропаганда (джерело невідоме, істинність не встановлена). Часто приховує свої цілі, поєднується з чорною пропагандою.

– «Чорна» пропаганда (фальсифікація джерела та повідомлення). Заснована на брехні, приховує свої цілі [7, с.51].

Важливе значення має залучення в ЗМІ нових технологій комунікації для створення, обробки і поширення інформації. Використання технологій

прихованої реклами або зв'язків з громадськістю дозволяє здійснювати латентне формування позитивного або негативного ставлення до події, особи тощо. Ми не можемо звинувачувати в пропаганді всі види комунікації, які включають елементи переконання. В основі цієї пропаганди лежать три основні елементи : риторика, міф і символізм.

Творці пропаганди прагнуть використовувати всі ці три елементи, щоб звернутися до наших основним емоційних імпульсів. Сучасна пропаганда – це послідовна, досить тривала діяльність, спрямована на створення або інформаційне оформлення різних подій з метою впливу на ставлення мас до ідеї або групи. Пропаганда добре працює тільки тоді, коли її прийоми не випадкові, а систематичні, причому у всіх областях.

Два інших підходи ідеологічно і оціночно навантажені. Один з них можна назвати радянським і в ньому пропагандистська діяльність визнається найважливішим інструментом соціальної та ідеологічної інженерії. Відповідно до ідеології радянського періоду така інженерія оцінюється за ознакою «свій–чужий» як однозначно позитивна (по намірам і змістом) в своєму власному виконанні, або однозначно негативна за тими ж параметрами у виконанні ідеологічного противника.

Стрімкий розвиток інформаційних технологій, комунікаційних мереж, засобів зв’язку і доступу до різної інформації, які сьогодні спостерігаємо, не могли не відбитися на соціальній сфері, на громадських і на міжнародних відносинах. Сьогодні новітні технології відіграють важливу роль в будь-якому суспільстві – вони дозволяють швидко обробляти великі обсяги інформації, змінюють структуру комунікації між людьми [5, с.129].

Швидкий розвиток інформаційних технологій, які стають загрозою і перетворюються в війну, радикально змінює структуру суспільства і значно трансформує міжнародні відносини. Інформаційна (або інформаційно-психологічна) війна історично була частиною реальної війни або будь-якого протистояння. На сучасному етапі історії людства вона є дестабілізуючим

фактором при налагодженні міжнародних відносин і породжує реальні політичні або навіть військові конфлікти.

Роль ЗМІ в сучасній світовій політиці під призмою інформаційних вій не завжди однозначно впливає на функціонування і розвиток міжнародного середовища. Посилення державної політики в сфері інформаційного простору, яка веде до контролю ЗМІ, робить їх вже не незалежними, а підконтрольними [21, с.461].

Саме ЗМІ починають втрачати свою роль незалежної «четвертої гілки» влади в державі. Відзначимо, що в даний час ЗМІ відіграють важливу роль в механізмі державної влади, формують громадянську думку з одного боку, а з іншого – протистоять тиску на державу на світовій арені. Вивчення ролі ЗМІ під час збройних конфліктів полягає в тому, що це явище деструктивне і суперечить демократичним принципам устрою суспільства [21, с.462].

Все частіше ЗМІ вибирають головним полем діяльності конфлікти як міжнародного, так і неміжнародного характеру. Оскільки прогрес не стоїть на місці, інформаційні технології розвиваються швидкими темпами, міжнародна ситуація постійно змінюється, процес дослідження впливу ЗМІ на проведення інформаційних війн під час збройних конфліктів є актуальним.

РОЗДІЛ 2
ЗМІ ТА ІНТЕРНЕТ – ЗОНА ВПЛИВУ ІНФОРМАЦІЙНИХ ТЕРОРИСТІВ

2.1. Засоби масової інформації як інструмент впливу терористів

Більшість експертів справедливо називають сучасний тероризм ЗМІ-орієнтованим тероризмом. Аналізуючи терористичну діяльність можна помітити, що в у більшості випадків вона здійснюється саме для того, щоб привернути увагу міжнародних ЗМІ. Можна сказати, що терористичні акти мають на меті спричинити великі втрати, а також викликати страх у суспільстві.

Сучасні технології зробили можливим використання невеликими терористичними групами ЗМІ, як потужну зброю, хоча ЗМІ служать інтересам терористів, проти власної волі. Але, думки про реальні відносини між ЗМІ та тероризмом дуже відрізняються. На меті у терористів є з'явитися в найпопулярніших програмах, щоб отримати масовий розголос про акти терору. Достатньо інформувати про дії революціонерів, щоб сучасні засоби масової інформації стали важливим інструментом пропаганди, а психологічна війна – це техніка ведення бою, заснована на прямому чи опосередкованому використанні засобів масової інформації [3, с.22].

Отже, тероризм можна розглядати як насильницький акт, який створено спеціально для того, щоб привернути увагу, а потім донести повідомлення. ЗМІ, як основний провідник інформації про такі діяння, відіграють важливу роль у діяльності терористів. Очевидно, що тільки шляхом поширення інформації про теракти, терористи можуть отримати максимальний розголос про свої дії і наміри, щоб спричинити зміни в політиці.

З іншого боку, інформація про тероризм, особливо про викрадення людей і ситуацію із захопленням заручників, є для ЗМІ джерелом новин, оскільки ці новини є драматичними та викликають велику увагу громадськості, вони можуть значно підвищити рейтинги, а отже й прибуток медіа компаній. Засоби масової інформації завжди будуть висвітлювати терористичні атаки через велику увагу громадськості до такої події. В. Коцур зазначає, що кожен відсоток підвищення рейтингу збільшує річний прибуток на десятки тисяч доларів [29, с.168]. Водночас на його думку, головні редактори навіть не підозрюють про політичні наслідки своєї невпинної гонитви за підвищення рейтингів.

Визначення впливу ЗМІ на тероризм є дуже складним питанням. Б.Д.Леонов розглянув дві гіпотези, одна з яких говорить про «потужну парадигму мас-медіа», яка намагається довести вагомий вплив медіа, а інша – «слабка парадигма мас-медіа», суть якої полягає в тому, що мас-медіа ефекти мінімальні [33, с.89]. Він дійшов висновку, що вплив ЗМІ зростає у випадках,

коли вони є єдиним джерелом інформації і коли немає іншої думки щодо певної події.

Деякі автори навіть намагалися розвинути теорію, згідно з якою першочерговий вплив на поширення тероризму мав розвиток ЗМІ. Д. Мельник рішуче виступав проти цієї теорії і зазначав, що терористичні організації протягом всієї історії намагалися поширювати інформацію про їх дії багатьма різними способами, спочатку через переказ, чутки а пізніше завдяки технологічному розвитку [37, с.88]. Цей дослідник подає теорію про симбіотичні відносини між тероризмом і ЗМІ, які виникають під час терористичних акцій.

П. Д. Біленчук намагається заперечити, що тероризм і ЗМІ перебувають у симбіотичних відносинах, пропонуючи теорію, згідно якої між терористами та ЗМІ існує чотири режими взаємодії :

1. Чиста байдужість – коли терористи не прагнуть ні налякати певну групу населення, ні здійснити пропаганду через їх вчинки.

2. Відносна байдужість – за якої злочинці байдужі до новин про насильство терористів.

3. Медіа-орієнтована стратегія – терористи використовують ЗМІ як інструмент для поширення повідомлення з погрозами.

4. Повний розрив – ситуації, коли терористи приходять, щоб знищити ЗМІ організації, редакторів і журналістів як ворогів, які мають бути покарані [3, с.27].

М.М.Галамба стверджує, що тероризм сам по собі є психологічною зброєю, яка залежить від передачі погрози громадськості. За його словами, в цьому суть їх симбіозу [13, с.54]. М.М.Галамба знаходить докази природи зв'язку між тероризмом і ЗМІ в наступному :

1. терористи «живляться» публічністю.

2. Свобода ЗМІ у відкритому суспільстві допомагає маніпулюванню свідомістю суспільства [13, с.55].

Я. М.Жарков розповідає про симбіотичні стосунки між тероризмом і медіа, з яких жоден учасник не може вийти. Він зазначив, що тероризм здатний створити будь-яку драму, якою б жахливою вона не була, привернути увагу засобів масової інформації [22, с.107].

Революція в масовій комунікації відкриває безліч нових можливостей спілкуватися в більших масштабах, ніж будь-коли раніше, а розвиток технологічних винаходів значно змінив спосіб передачі новин, зробивши їх доступними для великої кількості людей. Терористи вдало цим користуються. Отже, Я. М.Жарков також використовує термін «симбіоз» між медіа та тероризмом і згадує про три великі масові революції комунікації, які мали прямий вплив на тероризм [22, с.114].

Перша така революція сталася в XIX столітті і була викликана винаходом друкарської машини, яка дозволила друкувати велику кількість матеріалу. П. Д. Біленчук бачить симбіотичні відносини між тероризмом і ЗМІ протягом цієї епохи на прикладі Народної волі та їх сучасників-анархістів, які використовували газети для донесення своїх повідомлень до широкої аудиторії.

Друга велика революція в масовій комунікації відбулася в 1968 році. Цей рік став значимим не лише через зародження міжнародного тероризму, але й запуском Сполученими Штатами першого телевізійного супутника, який прискорив трансляцію новин і терористи негайно почали використовувати його для досягнення своїх цілей.

Третя революція проходила наприкінці XX ст., але в порівнянні з попередніми, меншою мірою залежала від нових основних технологій прориву, а використовувала існуючі зміни для стилю подачі новин [3, с.28]. П. Робінсон називає це «синдромом CNN», який зробив революцію в мовленні новин завдяки появі цілодобового мовлення, що стало причиною визнання американських ЗМІ «найкращим розвідувальним агентством» [68].

Окрім класичних терористичних загроз, вплив сучасних медіа спричинив так звану пропагандистську війну, якій терористичні організації

надають великого значення. Пропагандистська війна може бути дуже потужною психологічною зброєю і може значно підвищити ефект певних дій. Терористам, з одного боку, потрібна медійна пропаганда, щоб продемонструвати «абсолютну справедливість своїх цілей», але водночас вони усвідомлюють, якої шкоди їх може завдати негативна реклама.

Чотирма основними цілями терористичної пропаганди, які ставлять перед собою терористи, за допомогою ЗМІ є :

1. передати пропаганду вчинку і викликати потужний страх серед своєї цільової групи.

2. Мобілізувати ширшу підтримку своєї справи серед населення та міжнародної громадської думки, наголошуючи на таких темах, як справедливість справи і неминучість їх перемоги.

3. Зірвати реагування уряду та сил безпеки.

4. Мобілізовувати, підбурювати та збільшувати коло фактичних і потенційних прихильників, залучати більше коштів і надихати далі на вчинення терористичних актів [6, с.231].

Вільні ЗМІ є символом і основною цінністю демократичного суспільства. Але, внаслідок конкуренції у відкритому суспільстві та постійне суперництво в тому, хто стане першим, повідомляючи важливі новини, ЗМІ іноді свідомо реагують на терористичну пропаганду. О.Горошко зауважує, що було б неправильно робити висновок, що терористи контролюють ЗМІ. Вони майже не намагаються маніпулювати та експлуатувати їх для власної мети [18, с.10].

О.Горошко з цієї причини називає тероризм «збоченою формою шоу-бізнесу», а також способом інформування деяких ЗМІ про терористів. Таким чином, медіа-професіонали та громадськість повинні постійно бути напоготові перед спробами маніпулювання терористами [18, с.12].

У відкритому суспільстві з вільними ЗМІ можливо перервати антитерористичні операції через безвідповідальну поведінку ЗМІ. Надання великого розголосу терористичним діям, в першу чергу викраденням людей,

дуже посилює суспільний тиск на представників влади, щоб вони поступилися терористам. Реакція американських телевізійних мереж на ситуацію, пов'язану з викраденням американських заручників, які були вивезені до Бейрута в 1985 році, залишається безсумнівно, одним із найкращих прикладів здатності тероризму привертати увагу, використовувати ЗМІ та маніпулювати [35].

М. М. Матула проаналізувавши цей випадок, зробив висновок, що інформація в ЗМІ про заручників, справила суттєвий вплив на їх стурбовані родини та виявилася корисною для терористів. Хоча результат був успішним для обох заручників і для терористів, ЗМІ всіма засобами підірвали політику американського уряд [36].

Таким чином, ЗМІ не тільки інформують про події, але іноді йдуть набагато далі, чинячи тиск на уряд, беруть активну участь у визначенні політики країни. Були випадки, коли журналісти навіть брали на себе відповідальність і роль переговорників з терористами.

2.2. Інтернет як фактор інформаційного впливу тероризму на соціум

Деякі вчені говорять про значну роль Інтернету в процесах насильницької радикалізації. З боку політиків і громадськості зростає занепокоєння про те, що легка доступність насильницького екстремістського контенту в Інтернеті може мати насильницькі радикальні наслідки. Неможливо адекватно відповісти на питання, чому Інтернет відіграє більшу роль у сучасному насильницькому екстремізмі та тероризмі, не маючи попередніх знань про те, яку роль відіграє Інтернет в питаннях агресії [1, с.77].

На жаль, у цій галузі практично відсутні базові описові дослідження разом із більш складними теоретичними підходами, спрямованими на виявлення причинно-наслідкових зв’язків. Більше ніж через 20 років після терактів 11 вересня та майже десятиліття після зростання популярних он-лайн-форумів джихадистів, існує дуже мало емпіричних досліджень про те, як активісти джихаду використовують Інтернет для пропаганди своєї діяльності.

У той час як дослідники та політичні аналітики систематично збирали та аналізували вихідні матеріали, створені Аль-Каїдою та її союзниками, дуже мало роботи було зроблено щодо каналів, через які ця інформація поширюється і навіть того, наскільки хтось має доступ до цієї пропаганди. Іншими словами, бракує аналізу он-лайн-активності та досвіду окремих користувачів Інтернету в екстремістських кіберпросторах, на додаток до дослідження он-лайн-структур, у яких останні діють (навіть обмежено), а також їх різної роботи та функцій [9, с.318].

Враховуючи ці та інші труднощі з наявними дослідженнями, не дивно, що серед науковців тривають дебати щодо значення Інтернету в сучасному насильницькому екстремізмі та тероризмі, зокрема його ролі в процесах насильницької радикалізації. Скептицизм відносно того, що Інтернет може зіграти певну роль у насильницькому екстремізмі та тероризмі, не є новим. О.В. Глазов зробив таке спостереження : «Навіть велика кількість електронних листів, надісланих із долини Бака до Тель-Авіва, з Курдистану до Туреччини, з півострова Джафна до Коломбо чи з Індії до Пакистану не матиме і найменший політичний ефект» [17, с.80].

Це твердження цікаве з багатьох точок зору, головною з яких є те, що Лакер зазначає, що аудіокасети Хомейні контрабандою було ввезено до Ірану під час його вигнання в Наджафі, а згодом вони істотно вплинули у Парижі на Іранську революцію. Таким чином, Лакер охоче визнає той факт, що аудіокасети змінили хід історії Ірану, але не бачить, як Інтернет-технології можуть кардинально змінити щось в питаннях тероризму.

Початковий шлях Лакер до визначення ролі інформаційно-комунікаційних технологій у рухах проти політичного насильства, узгоджується з хвильовою теорією тероризму Девіда Рапопорта, змістом якої є те, що комунікаційні технології, можуть впливати на типи, час і поширення тероризму. Проте скептичний погляд Лакера залишається [66].

У 2011 році, Джейсон Берк, журналіст і автор першої книги про Аль-Каїду, зробив таке спостереження про соціальні медіа та їх вплив на сучасний

тероризм. Він зазначав, що Twitter ніколи не замінить масовий активізм. У більшій частині ісламського світу соціальні медіа призначені лише для місцевих еліт або прихильників у віддалених країнах. Ні те, ні інше не має великої користі. Соціальні медіа можуть залучати пожертви або здійснювати вербування. Це може сприяти лише пропагандистським операціям.

Берк вважає, що діяльність у соціальних мережах не може бути суттєвою формою «масового активізму» у «реальному світі». Також на його думку, не дуже багато людей в арабському та мусульманському світі є користувачами соціальних мереж, що є неправдою, адже навіть у 2011 році п’ять арабських країн (Об’єднані Арабські Емірати, Ліван, Йорданія, Кувейт і Туніс) мали понад 25 відсотків проникнення у Facebook [54, с.32].

Єдина безкоштовна он-лайн-платформа, яку можна використовувати для збору коштів, вербування, розповсюдження інформації та внутрішньогрупових комунікацій, ймовірно, буде досить важливим інструментом для досягнення цілей терористів. Сучасний Інтернет не просто дозволяє розповсюджувати та споживати «екстремістські матеріали» в односторонньому ефірі від виробника до споживача, але також забезпечує високий рівень соціальної взаємодії в мережі навколо цього матеріалу [4, с.87].

Саме функціональність соціальної мережі спонукає багатьох науковців, політиків та інших вважати, що Інтернет відіграє значну роль у сучасних процесах радикалізації. Це не означає, що немає більш переконливих аргументів на користь того, що роль Інтернету в сучасній насильницькій радикалізації перебільшена; ці аргументи мають дві основні позиції.

Згідно першої позиції, більшість сучасних насильницьких он-лайн-екстремістів є дилетантами в тому сенсі, що вони обмежуються використанням Інтернету для підтримки та заохочення насильницького екстремізму, але не становлять загрози «реальному світу». Згідно з цією позицією, їх он-лайн-діяльність замість того, щоб стати способом насильницької радикалізації, стає для багатьох механізмом розсіювання бажання насильницьких дій.

Другий скептичний підхід полягає в тому, щоб стверджувати, що заява про насильницький екстремістський он-лайн-контент, який насильно радикалізує людей, є безглуздою, враховуючи, що інші споживачі того самого контенту не мають подібного бажання вчинити акт тероризму. Фактично, велика кількість дослідників, журналістів регулярно стикається з насильницьким екстремістським контентом протягом тривалого часу, але не радикалізується, не говорячи вже про те, щоб бути залученими до тероризму [12].

Навпаки, цей досвід з перегляду екстремістського контенту, може навіть посилити огиду цих споживачів до насильницького екстремізму та тероризму, що, можливо, буде протилежним ефектом від запланово виробниками. Немає підстав говорити, що це не стосується досвіду широких верств населення. З іншого боку, це не одне й те саме, оскільки споживання насильницького екстремістського контенту має незначний вплив на всіх тих, хто його споживає.

2.3. Способи використання Інтернету та інформаційних технологій для терористичної діяльності

Терористичними групами все частіше використовуються можливості новітніх інформаційних технологій та мережі Інтернет для поширення пропаганди та обміну інформацією, залучення нових майданчиків для збору фінансових коштів на свою підтримку, планування терактів, а також для здійснення контролю за їх проведенням.

Загалом терористи використовують Інтернет майже так само, як і інші люди : вони надсилають повідомлення, координують дії з людьми, діляться зображеннями та відео. Технологічні компанії ніколи не створюють продукти для полегшення «планування атак», але вони думають про те, як забезпечити «безпечний зв’язок» [16, с.40].

Сучасні терористичні організації виробляють широкий спектр пропаганди у формі зображень, відео та аудіофайлів. До появи широкосмугового Інтернету цей вид матеріалів розповсюджувався вручну, або у формі друкованих матеріалів, або на відеокасетах, касетах або DVD. З появою широкосмугового зв'язку терористичні організації перемістили ці сховища в Інтернет спочатку через файлообмінні сайти, де користувачі могли завантажувати медіафайли, а згодом через сервіси, які дозволяють широкомасштабний обмін файлами та потокове відео.

Такі групи, як ІДІЛ, досі використовують різноманітні хмарні сервіси як медіа-сховища та постійно використовують сервіси потокового відео для розповсюдження пропагандистських матеріалів. Інші, такі як ХАМАС, мають власні веб-сайти. Не кожна Інтернет-платформа добре підходить для розміщення вмісту. Для цього використовуються сайти потокового відео та аудіо, а також хмарні сховища файлів. Деякі пропонують унікальні можливості, зокрема можливість транслювати відео в прямому ефірі з телефону чи камери. Платформи соціальних мереж, які полегшують розміщення відео та зображень, також можна використовувати для цієї мети [23].

Терористам потрібна аудиторія з різних причин : щоб безпосередньо залучити населення, на яке вони хочуть вплинути, щоб привернути увагу ЗМІ, щоб опосередковано залучити населення, на яке вони хочуть вплинути і щоб виявити потенційних вербувальників. ІДІЛ використовувала Twitter для цієї мети у 2014 та 2015 роках, оскільки платформа пропонувала широку аудиторію для витонченої пропаганди ІДІЛ і легкий доступ до журналістів, які, пишучи про цю пропаганду.

Терористичні групи по-різному думають про розвиток аудиторії залежно від своїх цілей, своєї ідеології та своєї теорії перемоги. Хоча ІДІЛ є ідеологічно жорсткою, вона уявляє себе авангардом великого популістського руху, тоді як ідеологічний двоюрідний брат ІДІЛ, Аль-Каїда, менш ідеологічно жорсткий, але сприймає свою найближчу аудиторію більш вузько. Ці

відмінності впливають на відповідну риторику груп, але також можуть впливати на тип цифрової платформи, яку кожна використовує для розвитку своєї аудиторії [38, с.89].

Такі організації, як ІДІЛ, прагнуть масово вербувати, але менші організації, які прагнуть створити елітне ядро акторів, можуть натомість зосередитися на розвитку аудиторії в межах цільової групи. Незважаючи на кричущу відсутність досліджень, які б порівнювали те, як терористи використовують соціальні медіа та традиційні засоби масової інформації, ймовірно, все ще є критично важливим методом для розвитку аудиторії. Тим не менш, нові цифрові платформи явно корисні для цих груп.

Тероризм відомий як «пропаганда справи». Бажання терористичних угруповань контролювати свої політичні меседжі породжує потребу в добре брендованих інформаційних каналах, які можна використовувати для підтвердження початкового поширення пропаганди. Таким чином, прес-секретарі, спеціалізовані медіа-виробничі будинки та надійні канали поширення інформації в Інтернеті є критично важливими.

Сучасні терористичні групи використовують спеціалізовані веб-форуми (наприклад, al-Hesbah), офіційні веб-сторінки (наприклад, Atomwaffen, Hamas і Hezbollah), облікові записи Twitter і, останнім часом канали Telegram, щоб допомогти своїй цільовій аудиторії зрозуміти, що матеріали, які там поширюються, є автентичними. Збереження контролю над брендом вимагає послідовності, що надає технологічним платформам особливо важливу роль у зриві цих зусиль серед терористичних груп [27, с.33].

Незважаючи на випадкові напади «вовків-одинаків», насильство терористів зазвичай задумують, планують і здійснюють групою. Таким чином, безпечний зв’язок між змовниками має першочергове значення. Повсюдне поширення інструментів для обміну зашифрованими повідомленнями знизило планку безпечної комунікації та, таким чином, спонукало до посилення перевірки платформ, які надають зашифровані послуги.

Однак терористи вже давно використовують різні методи для забезпечення безпечного обміну повідомленнями в Інтернеті. «Аль-Каїда» відома «мертвими каналами електронної пошти», коли користувачі обмінювалися інформацією для входу в обліковий запис і залишали повідомлення один одному як чернетки, таким чином уникаючи сканування під час передачі повідомлень.

Невідомість часто є інструментом безпеки : цьому можна сприяти через підроблені облікові записи, кілька облікових записів і таємні веб-форуми, доступні лише для запрошених учасників. Фахівці з боротьби з тероризмом можуть порушити ці методи, якщо знатимуть, де шукати. Стеганографію, або практику залишати приховане повідомлення на видноті, часто ігнорують. Такі повідомлення можуть відбуватися у формі використання заздалегідь визначеного, але нешкідливого кодового слова для надсилання повідомлення або непрямих посилань для автентифікації в Інтернеті [44, с.46].

Терористичні групи часто покладаються на «внутрішню» соціальну динаміку, щоб посилити антипатію до «негрупових» членів. Таким чином, обмежені місця, де можна ділитися пропагандою, спостерігати в унісон та обговорювати, часто є критичними. У реальному світі терористичні групи використовують зустрічі, трапези, релігійні проповіді та мітинги, щоб створити таку згуртованість у групі.

Закриті он-лайн-групи в програмах обміну повідомленнями, обмежений простір на платформах соціальних медіа та фірмові он-лайн-форуми служать для того, щоб відокремити учасників групи від сторонніх. У деяких випадках підтримку спільноти можна здійснити у більш відкритих цифрових середовищах за допомогою символів і фраз, які позначають членство в групі. Однак зробити такі публічні вивіски набагато легше після того, як базова лексика в групі буде створена в більш закритому середовищі. Ці замкнуті простори також пропонують спосіб зміцнення та нормалізації ідеологічного світогляду, який схвалює насильство як засіб досягнення мети.

Ця функція може бути особливо важливою для менш інституціоналізованих радикальних рухів, таких як прихильники переваги білої раси, на відміну від більш структурованих організацій, які зазвичай створюють джихадисти. Таке середовище слугує не лише активним терористам, а й колу потенційних прихильників, які одного дня можуть стати вербувальниками.

З цією метою часто використовуються спеціалізовані веб-форуми салафітів-джихадистів і прихильників переваги білої раси, але також використовуються закриті групи в соціальних мережах або програмах для обміну повідомленнями, на відміну від більш структурованих організацій, які зазвичай створюють джихадисти [58].

Постійні терористичні кампанії потребують грошей. Цифрові інструменти пропонують механізми як для збору коштів, так і для фінансових переказів. Основною проблемою електронних грошових переказів є безпека, яка спонукала багатьох терористів використовувати готівку або переказувати гроші через злочинні мережі, у вигляді незаконних товарів або через традиційні мережі обміну грошей.

Але деякі групи все ж використовують електронні перекази, сподіваючись уникнути перевірки через невідомість або, в останні роки, використовуючи криптовалюти. У цифровому просторі терористичні групи можуть використовувати традиційні фінансові відправники, такі як Western Union, електронні перекази між банками та он-лайн-платіжними системами (наприклад, Paypal), прямий збір коштів для благодійних організацій або перекази від людини до людини за допомогою таких платформ, як GoFundMe або Платежі Messenger.

Терористичні групи також використовують Інтернет для збору інформації. Бойовики використовують он-лайн-карти для планування атак, моніторингу новин і виявлення потенційних новобранців. Для цих цілей можна використовувати різні платформи, включаючи соціальні медіа, традиційні медіа, пошукові системи та спеціалізовані інструменти для

виявлення критичної інфраструктури та інших чутливих цілей. Усі ці інструменти використовуються звичайними людьми, щоб знайти продуктові магазини, старих друзів і найшвидший спосіб пересуватися містом.

Важливо визнати, що деякі он-лайн-платформи краще підходять для деяких із перелічених вище функцій, ніж інші, а це означає, що терористи часто використовують декілька платформ для своєї діяльності в Інтернеті. Наприклад, у 2014 році ІДІЛ широко використовував Twitter для розвитку аудиторії та контролю бренду, але оскільки Twitter не дозволяє користувачам завантажувати довгі відео або створювати сховища вмісту, пропагандисти ІДІЛ використовували YouTube, Justpaste.it або інші платформи для розміщення контенту [14, с.76].

Потім вони розміщували посилання на сайт контенту на обраній ними платформі для розвитку аудиторії. Подібним чином терорист може використовувати Facebook для розширення аудиторії. Є також ширші способи думати про переваги платформи. Наприклад, для підтримки спільноти не потрібна основна соціальна платформа, оскільки прихильники вже зацікавлені в ідеології групи, а отже, ймовірно, готові прийняти новий інструмент.

Але для розвитку аудиторії потрібно використовувати платформи з уже наявною аудиторією або активними користувачами. Telegram, наприклад, став ключовим інструментом для багатьох терористичних організацій, але насправді він корисний лише для контролю бренду, підтримки спільноти та безпечного спілкування. Він не ідеальний для розвитку аудиторії чи розміщення контенту.

Подібно до того, як платформи різняться за своєю корисністю для різних функцій, терористичні групи відрізняються за значенням, яке вони надають певним функціям. «Аль-Каїда» завжди вважала себе меншою, більш елітною організацією, ніж ІДІЛ, тому вона повільно відмовлялася від використання веб-форумів, які добре підходили для підтримки спільноти та контролю над брендом, навіть після розквіту соціальних мереж.

ІДІЛ, навпаки, давно прагнув створити широкий суспільний рух і заохочувати напади так званих «самотніх вовків». Порівняно з Аль-Каїдою, вона історично ризикувала своїм контролем над брендом через те, що так сильно зосереджувалася на розвитку аудиторії та розміщенні контенту, покладаючись на такі платформи, як : Twitter, Facebook і YouTube. Наприклад, ІДІЛ охопила неофіційні медіа-групи, які виробляють про-Ісламську державу, більше, ніж Аль-Каїду [14, с.78].

Політики як в уряді, так і в корпоративних установах, а також дослідницьке співтовариство з питань боротьби з тероризмом повинні розуміти, як терористи використовують певні платформи, щоб ефективно призначати контрзаходи. Наприклад, платформи, які використовуються для розміщення контенту, повинні надавати пріоритет механізмам виявлення терористичної пропаганди.

Але ці методи не будуть такими важливими для платформ, які використовуються для підтримки спільноти групи, безпечного спілкування та організації фінансування. Для цих платформ визначення поведінкових сигналів або обмін інформацією з партнерами може бути важливішим. Платформи, які підтримують численні функції, потребуватимуть розробки різноманітних методів. Універсального рішення цієї проблеми не існує і спільнота, яка займається боротьбою з тероризмом, не повинна робити помилку, пропонуючи інше. Особи, які приймають рішення в технологічних компаніях, добре знають відмінності між платформами, а також терористичні групи, які ними користуються [25, с.107].

Компанії, які розробляють політику боротьби з тероризмом, повинні розробити стратегію, яка є достатньо адаптованою, щоб йти в ногу зі зміною динаміки в реальному світі та мінливих технічних реалій. Вони повинні враховувати тактичні наслідки як для терористів, так і для їх численних доброзичливих користувачів. Вони також повинні розглянути, як їхній вибір вплине на більш традиційних учасників боротьби з тероризмом, будь то урядові чи некомерційні.

Експертам із політики боротьби з тероризмом дуже важливо розуміти різноманітність факторів, які впливають на те, як компанія реагує на тероризм на своїй платформі. Ці фактори дуже різноманітні та включають наступне :

- Баланс між свободою слова та конфіденційністю, безпекою користувачів і суспільства є великим. Ці принципи не завжди безпосередньо суперечать, але напругу між ними неможливо повністю вирішити без компромісів.
- Конкретні функції терористи прагнуть виконувати на певній платформі.
- Технологічні компанії мають дуже різноманітні ресурси для боротьби з такими проблемами в Інтернеті, як терористична діяльність. Політики часто сприймають компанії величезними ресурсами, але терористичні групи використовують широкий спектр технологічних платформ, найменші з яких можуть перерахувати своїх співробітників на одній руці та не мають ресурсів, щоб найняти спеціалістів з боротьби з тероризмом або присвятити великі інженерні роботи по боротьбі з тероризмом.
- Загалом технологічні компанії намагаються встановити політику, яка застосовуватиметься в усьому світі, незалежно від країни. Це прагнення до універсальності дуже відрізняється від того, як уряди підходять до геополітичних питань, де модулювання політики відповідно до кожної країни є звичайним явищем [30, с.178].

На цьому фоні он-лайн-платформи повинні прийняти низку стратегічних політичних рішень і оперативних рішень для протидії терористичній діяльності в Інтернеті, що має далекосяжні політичні наслідки. Одне з найважливіших політичних рішень, з яким стикаються технологічні компанії, полягає в тому, як визначити, хто є терористом. Є кілька варіантів, кожен зі своїми плюсами і мінусами.

Одним із варіантів є покладатися на міжнародні списки позначень, такі як ті, що підтримуються Організацією Об’єднаних Націй або Європейським

Союзом. Такий підхід дозволяє компаніям спиратися на інститути, які теоретично відображають колективну мудрість світової спільноти і дозволяє технологічній компанії уникати прийняття рішень, які можуть сприйматися як політичні.

Проблема цього підходу полягає в тому, що міжнародні організації та списки, які вони створюють, насправді відображають політизований консенсус, вироблений після багатьох політичних суперечок. Крім того, списки оновлюються дуже повільно і часто відображають підхід найменшого спільного знаменника. Зазвичай це означає, що такі списки включають найвідоміших глобальних терористів, але виключають войовничі угруповання, які привертають менше глобальної уваги або актуальні лише в певних регіонах [36].

Компанія може спробувати покладатися лише на списки терористів від певних урядів, наприклад, своєї країни чи інших демократичних держав. Але такий підхід змушує компанії визначати, які країни є достатньо демократичними. Компанії може здатися легким просто «заборонити тероризм» на своїй платформі, але запровадити надійну політику набагато складніше. Компанії повинні, наприклад, визначити, чи встановлювати обмеження на рівні вмісту, облікового запису чи користувача, а також визначити, який тип взаємодії з терористичним контентом або групами прийнятний, а який ні.

Обмеження на рівні вмісту забороняють підтримку тероризму в окремих матеріалах он-лайн. «Вміст» відрізняється залежно від платформи, але в Twitter це буде твіт; у Facebook, публікація, коментар або подібна інформація, створена користувачами; а на YouTube – одне завантажене відео. Одним із механізмів обмеженняє просто заборона формальної пропаганди, створеної або явно розробленої для просування інформації про терориста або терористичну групу [69].

Це потужний підхід проти таких груп, як ІДІЛ, які виробляють великий обсяг фірмової офіційної пропаганди, але він менш цінний для протидії

неформальній пропаганді, яка поширена серед ряду терористів, зокрема прихильників переваги білої раси та локальних прихильників ІДІЛ у деяких регіонах. світ. Однак орієнтація на неформальну пропаганду може створити проблеми із впровадженням, оскільки цей матеріал складніше ідентифікувати.

Деякі компанії можуть визначити, що просто забороняти розповсюдження терористичного вмісту на їхньому сайті є неефективним. Натомість вони вважають за краще видалити облікові записи, які представляють терористичні організації або демонструють підтримку тероризму. Найпростіший спосіб зробити це – просто видалити обліковий запис після певної кількості порушень вмісту. Перевагою цього підходу є простота. Це також гарантує, що обліковий запис оцінюється безпосередньо за його власною поведінкою в Інтернеті.

Найбільш агресивний підхід до нав'язування стандартів контенту спрямований безпосередньо на користувача. Це означає, що реальній людині просто заборонено користуватися платформою, незалежно від того, з ким вона взаємодіє або що публікує. Цей підхід є простим для відомих терористів, але складніший, коли мова йде про більш незрозумілих терористів, таких як, наприклад, члени Робітничої партії Курдистану [1, с.189].

Обмеження на рівні користувача також викликають важливі практичні питання. Чи повинна заборона поширюватися лише на лідерів терористичної організації чи на всіх членів? Як слід визначати ці категорії та який стандарт доказів для визначення того, чи належить хтось до тієї чи іншої категорії?

Найкращі методи виявлення терористичного контенту значною мірою залежать від того, як платформа визначає тероризм і вміст, який порушує її стандарти, а також від того, як побудована сама платформа. Корисно розглядати методи виявлення як такі, що поділяються на дві підкатегорії : людські підходи та автоматизовані підходи. Людські підходи мають перевагу гнучкості : люди можуть змінювати те, що шукають і швидко визначати нові моделі поведінки терористів. Автоматизовані методи цінні тим, що вони масштабуються для глобальної аудиторії. Однак вони не такі спритні, як

підходи людини і їх потенційно можуть обійти адаптивні супротивники. Багато великих технологічних компаній, включаючи Facebook, використовують як людські, так і автоматизовані методи [14, с.78].

Технічні компанії також можуть співпрацювати із зовнішніми групами для виявлення терористичного контенту. Наприклад, YouTube використовує програму «Trusted Flagger», тоді як Facebook укладає контракти з низкою постачальників, щоб надавати цільові реферали терористичного контенту. Компанія може вирішити надати спеціалізовані інструменти або доступ до API, щоб полегшити роботу таких партнерів.

Особливо яскраво ці можливості в Інтернеті проявилися на тлі сирійської кризи та активізації терористичної організації «Ісламська Держава» (ІДІЛ), діяльність якої заборонена в світі. Саме ця організація однією з перших створила адміністративні структури зі штатом блогерів для ведення цілеспрямованої роботи в Інтернеті, залучення нових рекрутів та поширення ідеології тероризму [14, с.80].

Понад 80% відповідних матеріалів, які сьогодні поширюються в Інтернеті, належать до діяльності терористичних груп, що знаходяться на території Іраку та Сирії. Як показують результати моніторингу ЗМІ та зізнань постраждалих, опубліковані в пресі, в більшості випадків пропаганда радикальних ідей та вербування відбувається переважно у популярних соціальних мережах Facebook, Twitter, Youtube.

Сьогодні можна констатувати, що саме за допомогою соціальних мереж бойовикам ІДІЛ вдалося завербувати громадян практично із ста країн світу. Вихідці з колишніх республік СРСР складають майже шосту частину іноземців у терористичному угрупованні – 4700 осіб із 30 тисяч найманців [17, с.79]. Завдяки професійній роботі агітаторів та вербувальників лави терористів продовжують поповнюватися.

У соціальних мережах активно поширюються пропагандистські фото- та відеоматеріали, грамотно змонтовані з погляду піару та психології. Вони присвячені демонстрації нібито звичайного життя бойовиків, пропаганді

військового способу життя та героїзму бойовиків, заклику боротися за свої ідеали зі зброєю в руках, трансляції сцен вдалих бойових дій та актів залякування. Фото та відеозвіти супроводжуються джихадистськими піснями, які займають важливе місце у формованій культурній матриці глобальної терористичної спільноти. У них є власний мобільний додаток та Інтернет-магазин, де можна купити футболку або худі з логотипом терористів. Вся ця небезпечна для свідомості продукція поширюються багатьма мовами світу.

Основне завдання подібних продуктів – залучити та зацікавити людей, втягнути їх у спілкування у форматі питання – відповідь з метою психологічної обробки для подальшої ізоляції людини від близького оточення та соціуму в цілому та залучення до лав терористів. Вербувальники терористичних організацій використовують ту саму технологію, що й тоталітарні секти. Для цього вони намагаються якнайсильніше розташувати людину, стати в її очах наставником, другом, підтримують емоційне життя людей порадами та добрими словами.

По суті, молоді дається установка – не будь пасивним, вступай у наші лави та стань нашим братом. Звичайно, компетентні органи відстежують і видаляють матеріали деструктивного характеру, а сайти, що їх містять, блокують, але для цього потрібен час (дні, тижні, іноді і місяці). За цей час ролик мають можливість переглянути десятки тисяч молодих людей, у яких майже у кожного є сьогодні смартфон або планшет [25, с.108].

При цьому від появи нових Інтернет-ресурсів, що одурманюють молодіжну свідомість, ніхто не застрахований. Загальносвітовою тенденцією є безперервне зростання кількості активних користувачів соціальних мереж, масова аудиторія яких має високий рівень довіри до їх електронних ЗМІ. У цьому соціальні мережі принципово відрізняється від інших видів комунікацій.

По-перше, широко використовуються візуальні образи, а вони, на відміну від символів мови чи письма, дуже схильні до того, щоб аудиторія сприймала їх як природну життєву подію. По-друге, образи, що подаються при

всій їх схожості на реальні життєві події є кодом, а не простим відображенням реальних життєвих обставин. Цей код має певний сенс, який часто не ідентичний змісту інформації, що відображається на екрані монітору.

Таким чином, кодування залишається для масової аудиторії непомітним, і в осіб, які здійснюють селекцію та оформлення Інтернет-сторінки, виникає можливість активізувати маніпулятивні механізми, спрямовані на зміну поглядів і уявлень, що склалися раніше. У результаті вдається як сформувати нові орієнтації, так і змінювати старі. Очевидно, що подання заздалегідь обробленої інформації на інформаційних сайтах соціальних мереж значною мірою сприяє формуванню громадської думки.

При цьому найчастіше застосовуються такі прийоми маніпуляції : спотворення інформації, підтасовування фактів, зміщення понять семантичного поля, фабрикація фактів, спрощення, стереотипізація. Як правило, спотворена інформація використовується разом з відповідним способом її подання, таким як затвердження, повторення, дроблення, терміновість, сенсаційність та відсутність альтернативних джерел інформації [53, с.69].

На Інтернет-сайтах після кожної статті розміщують опитувальники, при цьому кожен охочий може висловити свою думку або ознайомитись з думкою інших. За кількістю людей, які залишили свої думки (так званих «лайкарів»), оцінюється актуальність теми, порушеної в тій чи іншій статті. Якщо один користувач оцінив це відео, натиснувши на «лайк», то його бачать на своїх стрічках усі друзі та підписники цього користувача. Для підвищення ефективності впливу на співпрацю залучаються пошукові компанії.

Таким чином, на відміну від традиційного тероризму, який не загрожував суспільству, як такому і не торкався основ його життєдіяльності, сучасний високотехнологічний тероризм здатний продукувати системну кризу в будь-якій державі з високорозвиненою інформаційною інфраструктурою.

Розвиток соціальних мереж супроводжується все більш широким використанням їх можливостей для здійснення інформаційного протиборства,

зростанням координації, масштабів та складності дій його учасників, якими найчастіше виступають як держави, так і окремі організовані групи, у тому числі терористичні. Об'єктом кібератак все частіше стають інформаційні ресурси, виведення з ладу або утруднення функціонування яких може завдати значну економічну шкоду, що протистоїть стороні, або викликати великий суспільний резонанс [25, с.109].

В даний час у багатьох країнах світу вже створені на державному рівні або перебувають на стадії реалізації програми, що надають великі повноваження національним спецслужбам з контролю за інформаційними системами. Проте, як показує практика, жодна спецслужба окремо взятої країни в кіберпросторі не може протистояти міжнародним терористичним організаціям, наприклад, таким як «Аль-Каїда» та ІДІЛ.

Американські служби, що спеціалізуються на протидії інформаційній діяльності терористичних організацій, зізнаються, що нині нездатні ефективно протистояти пропагандистській активності терористів у глобальній мережі Інтернет. Використання стільникового телефонного зв'язку, можливостей електронної пошти та Інтернет дозволяє забезпечити досить високий рівень анонімності участі в терористичній діяльності.

На думку експертів американської розвідки, терористи, крім використання широко поширених каналів зв'язку в Інтернет-форумах, перейшли на спілкування один з одним під прикриттям учасників мережевих комп'ютерних ігор. Передбачається, що вони використовують сценарії даних ігор для координації дій, встановлення контактів та репетицій можливих атак на віртуальних моделях [31, с.68].

В таких умовах вразливість критичних інфраструктур перестає бути проблемою кожної держави окремо. Це загальна загроза, яку можна вирішити лише спільними зусиллями, вибудовуючи систему колективної інформаційної безпеки з урахуванням сучасних загроз у кіберпросторі. Аналіз та узагальнення існуючого досвіду антитерористичної діяльності дозволив

сформулювати завдання захисту критичної інфраструктури від кібертероризму та основні заходи, спрямовані на їх вирішення [56] :

- на національному рівні :

– організація моніторингу та прогнозування потреб економічних та інших структур у різних видах інформаційного обміну через міжнародні мережі. Для цього є можливим створення спеціалізованої структури для контролю транскордонного обміну, в тому числі за допомогою Інтернету;

– координація заходів державних та недержавних відомств щодо запобігання загроз інформаційній безпеці у відкритих мережах. З цією метою має бути вироблена та прийнята до виконання єдина політика, орієнтована на дотримання законних прав громадян на інформацію та інтелектуальну власність, що передбачає захист мережного обладнання на території країни від проникнення до нього прихованих елементів інформаційної зброї. Це особливо важливо в умовах масової закупівлі зарубіжних інформаційних технологій та мережевого обладнання;

– розробка державної програми вдосконалення інформаційних технологій, що забезпечують підключення національних та корпоративних мереж до світових відкритих мереж за дотримання вимог безпеки інформаційних ресурсів;

– удосконалення технологій своєчасного виявлення та нейтралізації несанкціонованого доступу до інформації, у тому числі у відкритих мережах. При цьому необхідно бути готовими не просто до модернізації прийомів інформаційного протистояння, а до виявлення нових факторів ризику, створення та використання випереджаючих технологій;

– розробка національного законодавства щодо правил поводження з інформаційними ресурсами, регламенту прав, обов'язків та відповідальності користувачів відкритих світових мереж;

– встановлення переліку інформації, що не підлягає передачі по відкритих мережах, та забезпечення контролю за дотриманням встановленого статусу інформації;

– організація системи комплексної підготовки та підвищення кваліфікації масових користувачів та спеціалістів з інформаційної безпеки для роботи у світових інформаційних мережах;

- на міжнародному рівні :

– організація міждержавного співробітництва у роботі міжнародних організацій, громадських комітетів та комісій у проектах розвитку світових інформаційних мереж;

– активна участь у розробці міжнародного законодавства та нормативно-правового забезпечення функціонування світових відкритих мереж;

– створення єдиного антитерористичного простору країн-союзників;

– розробка науково-методичного забезпечення щодо припинення транснаціональних (транскордонних) терористичних атак з використанням глобальних інформаційних мереж, вироблення єдиного понятійного апарату, шкали оцінки кіберзагроз та їх наслідків;

– вироблення механізмів взаємного інформування про широкомасштабні комп'ютерні атаки та великі інциденти в кіберпросторі, а також способи спільного реагування на загрози кібертероризму;

– уніфікація національних законодавств у сфері захисту критичної інфраструктури від кібертероризму.

РОЗДІЛ 3
ЗАПОБІГАННЯ ІНФОРМАЦІЙНОМУ ТЕРОРИЗМУ В СУЧАСНИХ УМОВАХ

3.1. Інформаційна складова боротьби з тероризмом в сучасних умовах

У сучасному світі, що зіткнувся з новими викликами, активно розвиваються інтеграційні процеси, що сприяють вирішенню збройних конфліктів та протидії міжнародним терористичним організаціям. В інтеграційних процесах велике значення мають інформаційні обміни, які забезпечують взаєморозуміння між країнами з різними культурами.

Тероризм з'являється як реакція у відповідь на тривале затягування вирішення різних проблем. Практично тероризм зростає з урахуванням значних суспільних протиріч. До терористичної боротьби призводить комплекс причин. Це : конфлікти політичного, соціального, національного, територіального, релігійного, психологічного (світоглядного) характеру. Сучасна ситуація показує, що часом і кримінальна злочинність набуває терористичних масштабів [2, с.110].

Вагоме значення розвитку інформаційної сфери приділяється сьогодні на державному рівні. З одного боку, в сучасному інформаційному просторі не представляється можливим прийняття ефективних рішень без системи аналізу та оцінки даних, вивчення поточних тенденцій, моделювання варіантів розвитку подій. З іншого боку, грамотна реалізація державної інформаційної політики забезпечує підтримку прийнятих політичних і економічних рішень, формує громадську думку з тих чи інших питань, запобігає розвитку екстремістських рухів.

На тлі посилення інтенсивності розвитку інформаційної інфраструктури та інтеграції у світовий інформаційний простір, з кожним днем ефективність

функціонування політичних і економічних інститутів соціуму все більше залежить від якості інформаційного середовища.

Логічно, що головним кроком, який повинна зробити Україна для посилення свого захисту в інформаційній сфері, за результатами дослідження, виявилося сприяння розвитку власних ЗМІ. Українські медіа зможуть задавати порядок денний, актуальний саме для України і просувати саме українські наративи. Розвиток діджитал компонента відповідно до вимог часу, потребам аудиторії і попитом рекламодавців є необхідною умовою збереження таких традиційних засобів масової інформації як газети і журнали, і збереження впливу телебачення на найбільш активну і заможну частину суспільства [19, с.22].

Складно уявити можливість реалізації державних функцій без чітко налагодженої державної інформаційної політики, в рамках якої закладені основи для вирішення таких завдань, як формування єдиного інформаційного простору України і її входження у світовий інформаційний простір, забезпечення інформаційної безпеки особистості, суспільства і держави, формування демократично орієнтованої масової свідомості, становлення галузі інформаційних послуг, розширення правового поля регулювання суспільних відносин, в тому числі пов'язаних з отриманням, розповсюдженням і використанням інформації.

В рамках забезпечення національної безпеки України в нашій країні проводиться державна політика реалізації комплексу заходів щодо інформаційної безпеки, що визначає основні напрямки діяльності органів державної влади, порядок закріплення їх обов'язків по захисту інтересів України в інформаційній сфері. Найважливішим завданням держави в сфері інформаційної безпеки є забезпечення гарантій конституційних прав і свобод людини і громадянина на доступ до інформації та забезпечення повноцінних можливостей для діяльності в інформаційній сфері [40, с.170].

В умовах розвитку інформаційного суспільства в нашій країні стає все більш очевидним, що забезпечити інформаційну безпеку тільки шляхом

діяльності органів державної влади, правоохоронних структур, розвитку нормативно-правової бази є достатньо важко, необхідне широке співробітництво з громадськими рухами і групами, що представляють активну частину громадянського суспільства. На думку фахівців в області інформаційної безпеки, практично будь-який програмний продукт, призначений для забезпечення функціонування ЕОМ, через специфіку свого виробництва має уразливості, що дозволяють здійснювати зовнішній деструктивний вплив.

В Україні інформаційне суспільство є найважливішим напрямком формування сучасної інформаційно-телекомунікаційної інфраструктури, надання на її основі якісних послуг у сфері інформаційних технологій. Основним завданням для реалізації цього напрямку визначено необхідність підвищення якості надання державних послуг шляхом їх переведення в електронний вигляд, розвитку сервісів на основі інформаційних технологій для спрощення процедур взаємодії та комунікації суспільства і держави, розвитку спеціальних інформаційних і інформаційно-технологічних систем забезпечення діяльності органів державної влади, створення та розвитку електронних сервісів в соціальних сферах, поширення кращої практики інформаційного суспільства на рівні держави [41, с.137].

Бурхливий розвиток інформаційної індустрії, її вплив на зайнятість, освіту, культуру, соціальні відносини і цінності призводять до необхідності сформулювати роль держави в становленні інформаційного суспільства. Держава може взяти на себе роль каталізатора змін, що відбуваються, координатора дій різних суб’єктів суспільства, сформувати таку правову і нормативну базу, яка направить їх в русло, сприятливе для розвитку суспільства й особистості. Ця задача більш масштабна, ніж формулювання державної інформаційної політики та політики інформатизації.

Перша зазвичай трактується як політика взаємовідносин держави та ЗМІ. Друга – як комплекс заходів, спрямованих на використання засобів інформатизації в державному управлінні. Вибудовування взаємин держави та

ЗМІ досить болюча проблема у всіх країнах, але вона регулюється законом про ЗМІ і фундаментальним правом на свободу слова.

Політика інформатизації розумілася спочатку в нашій країні досить широко – як дії держави, спрямовані на інформатизацію всього суспільства. Надалі це розуміння стало тягарем для державного сектору, внаслідок дій органів влади. Однак проблема тут цілком реальна і полягає в тому, що використання інформаційних технологій в органах державної влади необхідне, але дороге [46].

Тому повинна проводитися обов'язкова фінансова, правова і технологічна експертиза пропонованих проєктів інформатизації, для чого необхідний спеціалізований інформаційний аудит зі спеціальними повноваженнями, орієнтований на подібну експертизу інформатизації державних органів і спеціалізується в області системної інтеграції.

Оскільки реалізація великих телекомунікаційних проєктів – вельми інформаційний і ризикований бізнес, то держава не має права вкладати в цю сферу кошти платників податків. Тому всі ризики лягають на приватний бізнес, а держава створює умови для його діяльності, наприклад, передає на пільгових підставах створені системи в експлуатацію на певний термін. Все, що приносить прибуток має бути передане громадянам. Саме цей процес акціонування відбувається зараз з телекомунікаціями в усьому світі.

До числа найбільш значущих тенденцій в інформаційній індустрії останніх років можна віднести перегляд встановлених раніше правил функціонування інформаційної індустрії : дерегуляцію ринку телекомунікацій і ослаблення контролю за концентрацією власності в різних ЗМІ. В результаті відбувається як вертикальна, так і горизонтальна інтеграція ринків інформації та засобів її передачі [57, с.94].

Сучасні телекомунікаційні технології поступово стирають відмінності між секторами інформаційних телекомунікацій, кабельними мережами, супутниковим ефірним мовленням і т.п. Поступово поняття «засоби масової інформації» поступається місцем новому поняттю, яке об'єднує і телевізійне

мовлення в різних його формах (ефірне, кабельне, супутникове), і передачу даних та інформації з телекомунікацій. Прагнення лідирувати на ринку, усунути конкурентів – природне прагнення бізнесменів. Якщо держава не контролює цей процес, то відбувається монополізація ринку.

Концепція формування інформаційного суспільства в Україні передбачає, що держава повинна відігравати провідну роль в забезпеченні переходу до інформаційного суспільства. Відповідно, формувати і координувати політику переходу до інформаційного суспільства та створення регіонального інформаційного простору на регіональному рівні повинна влада регіону. Діючі та такі, що розробляються в даний час інформаційно-керуючі системи окремих органів публічної влади і органів місцевого самоврядування, відомчі та міжвідомчі територіально-розподільні системи та мережі збору, обробки і поширення інформації можуть слугувати базою впровадження нових інформаційних технологій [4, с.90].

Вони повинні забезпечити основу формування єдиного інформаційного простору України і гарантувати сполучення нових засобів інформаційних технологій з традиційними засобами поширення інформації і організації доступу до неї : друкованими та електронними засобами масової інформації, журнальними і книжковими виданнями, бібліотеками та архівами тощо.

Особливого значення сьогодні набуває економічна залежність ЗМІ від :

– засновників, які істотно впливають на політичні орієнтації;

– обмеження їх доступу до інформації, викликане «закритістю» органів влади;

– недостатньо розроблена правова основа діяльності ЗМІ;

– відсутність реакції органів влади на критику і ін.

Існує кілька варіантів розвитку конфлікту між владою та ЗМІ :

1. «влада-влада» (конфлікт між різними рівнями влади, в цьому випадку в конфлікт втягнуті державні ЗМІ);

2. «ЗМІ – ЗМІ» (конфлікт між ЗМІ, що представляють різні рівні влади).

3. «Влада – ЗМІ» (тиск держави на ЗМІ з метою дотримання законності і висловлення власних інтересів і, навпаки, тиск ЗМІ на владу для максимальної об'єктивності інформації або виконання політичного замовлення щодо зниження рейтингів тієї чи іншої владної структури) [6, с.231].

Таким чином, взаємини влади і ЗМІ дуже багатопланові й можуть мати безліч форм (як конфронтації, так і позитивної взаємодії).

В реальності допускається використання цензури з метою підтримки курсу соціально-економічного розвитку держави, що відповідає моделі країн, що розвиваються. При цьому існує безліч «кишенькових» ЗМІ, а інформаційна тематика, в основному, зосереджена на зовнішній політиці, що більше характерно для радянської моделі. Така суперечлива картина, відсутність належної уваги до проблеми зі сторони органів публічної влади, застаріле законодавство в сфері ЗМІ, говорить про те, що у держави немає чіткої політики взаємодії зі ЗМІ, а також немає розуміння цілей цієї взаємодії, що веде до неузгодженості і виникнення проблем взаємодії органів влади та ЗМІ.

В цілому ми можемо визначити модель взаємодії органів влади та ЗМІ в Україні як змішану, з переважаючими характеристиками моделі країн, що розвиваються, основною характеристикою якої є наявність обмежень і цензури, заснованих на потребах розвитку всього суспільства і пріоритетах розвитку економіки. Виходячи з цього, проаналізуємо проблеми, що виникають при взаємодії ЗМІ та органів влади [8, с.40].

Найкращою для суспільства є інформаційно-політична диспозиція ЗМІ, що висуває на перший план виконання громадського (масового) інформаційного замовлення і «діалектично» поєднує в собі критику і підтримку владних структур як раціонально продуктивну публічну реакцію на позитивні і негативні моменти в їх практичній діяльності.

Наприклад, напередодні парламентських і президентських виборів у владних колах і біля них, все частіше стали говорити про необхідність збереження наступності нинішнього курсу і досягнутої стабільності. Але при

цьому ніхто доказово не говорить, якою мірою спадкоємність й стабільність відповідають інтересам самого суспільства і історичного прогресу. І ніхто не бажає згадувати, які наслідки для країни і суспільства мало прагнення панівного класу на різних етапах нашої історії під виглядом збереження наступності і стабільність зберігати самих себе у владі.

При визначенні імперативів і розробці інформаційної політики мова повинна йти, згідно з Конституцією України, про задоволення інформаційних потреб (інтересів) усіх верств населення, незалежно від їх майнового стану. Провідна політика друку і стимулювання її владою, з одного боку, культивують інформаційні привілеї для вищих верств населення, надаючи їм полегшений доступ до публічних засобів комунікації, а з іншого – вводять в повсякденність інформаційне притиснення інтересів низових і середніх соціальних верств, фактично позбавляючи їх можливості висловлюватися вголос про те, що відбувається [19, с.26].

З цього виходить, що : по-перше, в інформаційній політиці державних і громадських структур регіону абсолютно не враховується конституційна норма рівності всіх громадян в частині задоволення їх інформаційних потреб (інтересів), при цьому в пресі превалює елітарна думка замість громадської думки, в результаті чого в соціумі провокується, ефект «спіралі мовчання», фактично вимикає з активного громадського життя великі маси людей; по-друге, недотримання закону інформаційно-стратифікаційного балансу, що допускається владою і пресою (завищення інформаційної норми меншини (еліти) і, навпаки, заниження інформаційної норми більшості (маси) призводить до зростання на цьому ґрунті соціально-політичної напруженості і нестабільності в регіоні. «Недодача» народу можливостей інформаційного спілкування в масової комунікації зазвичай компенсується «перебором» мітингових його варіантів.

При збігу несприятливих обставин внутрішнього і зовнішнього характеру в інформаційній сфері життєдіяльності соціуму може трапитися найнеприємніше – інформаційний дефолт. У першому значенні він,

визначається як фактична відмова держави від юридичних (конституційних) зобов'язань перед суспільством (громадянами) в інформаційній сфері, пов'язаний зі значним скороченням джерел масової інформації та суттєвим звуженням каналів і способів її поширення [29, с.170].

Перша ознака цієї відмови – відсутність державного протекціонізму в духовній галузі соціального відтворення. У другому значенні інформаційний дефолт визначається як реальна втрата мас-медіа та пресою довіри в суспільстві в зв'язку з виробництвом масової інформації, що не відповідає принципам об'єктивності, повноти, вірогідності, оперативності, цінності, правдивості, добросовісності, корисності, моральності.

Але, схоже, цей тривожний сигнал не особливо хвилює служителів преси, що повірили в те, що невидима рука інформаційного ринку рано чи пізно «виховає» адекватного низькопробного креативу читача, глядача, слухача. А про інформаційну безпеку країни, пов'язаної, з високим рівнем інформаційної культури громадян, що володіють імунітетом до деструктивної журналістики, виходить повинен думати той, хто наділений спеціальними повноваженнями [32, с.175].

В принципі, високим ступенем ризику володіють й інші тенденції, зокрема, спотворення за допомогою «підручних» засобів масової інформації соціальної реальності в регіонах і формування культу особи місцевих лідерів. Нейтралізувати аномалії, що виникають у сфері інформаційно-комунікативної складової життєдіяльності соціуму, цілком можливо за допомогою «інформаційно-організаційного фактора», в арсеналі якого з давніх пір перебуває державна інформаційна політика.

Тим часом цей шлях в Україні фактично не використовується : по-перше, він, з регулярністю і методичністю, піддається остракізму з боку самого журналістського співтовариства, яке асоціює його з реставрацією цензури, цього явно гіперболізованого «монстра»; по-друге, в його реальному бутті (точніше : в механізмах реалізації інформаційної політики) фіксуються

«вузькі місця», які вимагають від державних і громадських структур та інститутів термінового інтелектуально-управлінського втручання.

Особливу занепокоєність викликає практична відсутність соціального контролю : з боку преси – за політикою держави і з боку суспільства – за діяльністю преси. Остання, особливо державного і приватного типів засновництва, орієнтується в першу чергу на інформаційні інтереси еліти, а не на інформаційні потреби маси і тим самим фактично блокує необхідну для самозбереження і розвитку демократичної держави її зворотний зв'язок із суспільством [35].

В результаті виникають «розриви» в інформаційному просторі, що істотно обмежують взаємодію між особою і суспільством, різними соціальними, професійними, етнічними, територіальними та іншими спільнотами, до яких ця особа належить. Це також обмежує взаємодію між державою і громадянами, центром і регіонами, а також в сферах практичної, духовної та духовно-практичної діяльності та між ними.

Односторонній (владно-монологічний) характер медіа комунікацій стосовно масової свідомості – теж неминучий наслідок гіпертрофії товарних відносин і управлінських повноважень, коли журналіст, всупереч своїй місіонерській ролі, швидко засвоює велику вигоду і вбачає особисту безпеку в служінні не суспільству і народу, а державі і олігархам. До того ж така лінія поведінки преси стимулюється і недосконалим в цій області законодавством.

В цьому випадку відбувається не формування масової свідомості засобами медіакомунікацій за демократичним алгоритмом в діалогових формах спілкування, а його інформаційне «вимуштрування». Такий медіа комунікативний варіант проходить гладко, поки кількість не комунікативних ситуацій і не інформованість акторів не складе критичної маси, за якою може статися вибух соціального невдоволення [42, с.83].

Інформація нині є одним з найбільш важливих ресурсів в системі державного управління. Інформаційну зброю намагаються використовувати в

своїх інтересах як авторитарні, так і ліберальні уряди, проте інформаційні потоки все більше сприяють демократизації політичних систем.

В рамках забезпечення національної безпеки України в нашій країні проводиться державна політика реалізації комплексу заходів щодо інформаційної безпеки, що визначає основні напрямки діяльності органів державної влади, порядок закріплення їх обов'язків по захисту інтересів України в інформаційній сфері. Найважливішим завданням держави в області інформаційної безпеки є забезпечення гарантій конституційних прав і свобод людини і громадянина на доступ до інформації та забезпечення повноцінних можливостей для діяльності в інформаційній сфері [53, с.208].

В підсумку вибудовується своєрідна система управління свідомістю і поведінкою як конкретного індивіда, так і цілих націй. Комп'ютерні технології відкривають величезні можливості контролю над суспільством. На цей час немає засобу, здатного гарантовано забезпечити конфіденційність спілкування в Інтернеті. Інтернет з вільної зони спілкування сьогодні перетворився в засіб впливу на свідомість користувача з боку політичних і бізнес-структур. Користувач Інтернету психологічно впевнений у власному вільному виборі інформації і неможливості ним маніпулювати, внаслідок чого значно знижується поріг раціонально-критичного сприйняття. Саме Інтернет став ланкою, що з'єднав інформаційну та психологічну війни.

Висловлюються думки, що в третьому тисячолітті лідерство в світі буде визначатися не стільки економічним потенціалом держави, скільки її здатністю контролювати інформаційні процеси, перетворювати інформацію в зброю.

Інформаційна зброя – це сукупність засобів і методів, що дозволяють викрадати, спотворювати або знищувати інформацію, обмежувати або припиняти доступ до неї законних користувачів, порушувати роботу або виводити з ладу телекомунікаційні мережі і комп'ютерні системи, які використовуються в забезпеченні життєдіяльності суспільства і держави [47, с.80].

Інформаційна зброя здатна керовано змінювати політичну свідомість людей, змушуючи їх неадекватно сприймати реальність, жити в світі ілюзій і здійснювати згубні для себе вчинки, що призводять до руйнування політичних систем і держав. Нині абсолютною більшістю експертів визнається той факт, що володіння ефективною інформаційною зброєю і засобами захисту стає одним з головних умов забезпечення національної безпеки держави. Інформаційні загрози набувають особливого значення в умовах модифікації ідеологій – від раціональних доктрин до ірраціональних релігійних ідеологем екстремістського характеру [54, с.39].

Отже, виділимо нові компоненти в системі державної інформаційної політики, необхідні для широкого впровадження :

– формування компетенції інформаційної безпеки як обов'язкового елементу підготовки державних службовців в системі вищої освіти і підвищення кваліфікації;

– введення в системі середньої шкільної освіти навчальної дисципліни, що дозволяє сформувати уявлення про основи феномену інформаційно-політичної безпеки;

– розширення взаємодії державних інститутів з громадянським суспільством, соціальними активістами;

– підвищення прозорості в роботі державних установ;

– посилення адміністративного і кримінального покарання за правопорушення в інформаційній сфері.

У сучасних умовах світового розвитку особливого значення набуває проблема інформаційного прогресу. Зараз вже визнано, що перетворення традиційних суспільств в індустріальні і постіндустріальні – це глобальна тенденція. Поряд з цим, всередині загального процесу можна виявити багато форм і варіантів (національних, регіональних та інших). Слід враховувати, що нова інформаційна реальність розвивається в межах людського суспільства і створює нові суспільні відносини, які потребують всебічного дослідження. Важливе значення набуває дослідження національних і регіональних

особливостей та специфіки, а також історичного досвіду формування інформаційних відносин в тій чи іншій державі [59, с.268].

Законодавче регулювання інформаційних процесів і програм дозволяє найбільш повноцінно вирішувати теоретичні та практичні питання подальшого розвитку інформаційного суспільства з урахуванням специфіки та історичного досвіду його формування в нашій країні. У сучасному світі склалися такі передумови, які вимагають прискореного розвитку нових суспільних відносин в умовах глобального інформаційного і науково-технічного прогресу. Перш за все це пов'язано з соціально-економічною нерівністю, яка виникає між розвинутими в інформаційно-технічному відношенні країнами, що розвиваються внаслідок суттєвої різниці в темпах впровадження і використання інформаційно-комунікаційних технологій

Така нерівність негативно впливає на конкурентоспроможність держав і окремих регіонів, а також на життєвий рівень людей. Стає зрозуміло, що в умовах розвитку інформаційного суспільства та глобалізації, проблеми сучасної України повинні вирішуватися не стільки на рівні модернізації «традиційних» галузей промисловості, скільки на рівні передових інформаційно-комунікаційних технологій і взаємовигідній рівноправній економічній інтеграції. На думку вітчизняних дослідників, з урахуванням наших труднощів і нашої спадщини, необхідно вжити всіх заходів для прискорення реалізації інформаційних процесів [2, с.115].

Формування і розвиток інформаційного суспільства вимагає регулювання на основі науково розроблених і законодавчо затверджених програм. Національна політика розвитку інформаційного суспільства в Україні передбачає проведення таких загальнодержавних заходів як перехід до пріоритетного науково-технічного та інноваційного розвитку, законодавче забезпечення розвитку інформаційного суспільства, формування сприятливих економічних умов, розвиток загальнодоступної інформаційної інфраструктури, забезпечення загального доступу до телекомунікаційних послуг та інформаційних ресурсів, сприяння збільшенню різноманітності і

кількості електронних послуг, забезпечення створення загальнодоступних електронних інформаційних ресурсів, підготовка людини для роботи в інформаційному просторі , створення системи мотивацій щодо впровадження і використання інформаційно-комунікаційних технологій, забезпечення подальшого розвитку науки, забезпечення інформаційної безпеки [4, с.91].

Все вищесказане свідчить про те, що теоретичне та концептуальне забезпечення інформаційного суспільства є одним з найважливіших умов його повноцінного розвитку. Такий стан актуалізує соціально-філософський аналіз специфіки формування інформаційного суспільства в Україні в складних умовах існування людини, суспільства і держави в інформаційну епоху.

Враховуючи викладене, пропонуються шляхи забезпечення поширення «позитивної» інформації засобами масової інформації :

– забезпечення висвітлення напрямків публічної інформаційної політики в державних засобах масової інформації;

– формування, розміщення та виконання державного замовлення на «позитивні» новини, телепрограми і передачі;

– забезпечення можливості доступу громадськості до широкого кола засобів масової інформації (вітчизняних і закордонних);

– притягнення до відповідальності за зміст телепрограм і передач, в яких необґрунтовано показується насильство, містяться відео сюжети, які можуть завдати шкоди фізичному, психічному чи моральному розвитку дітей та підлітків, включаючи анулювання ліцензій.

В рамках формування національної інфраструктури інформатизації основна увага приділяється виконанню інтегруючих завдань :

– розробці концепції та програми створення національної телекомунікаційної інфраструктури, а також створення першої черги телекомунікаційної інфраструктури;

– розробці концепції та програми створення інформаційних ресурсів органів публічної влади [16, с.40].

Порядок взаємодії влади і ЗМІ, встановлений законом, безумовно, підлягає неухильному дотриманню. Так, на державних структурах лежить обов'язок своєчасно реагувати на інформаційні запити. Відповідні підрозділи регіональних і місцевих органів влади ці функції зобов'язані виконувати. І така робота ведеться. Але треба усвідомлювати те, що повністю відповідати очікуванням творчих співробітників ЗМІ, особливо працюючим в максимально оперативному режимі, чисто технічно дуже складно.

Звичайно, існують можливості поліпшити такого роду комунікацію, але мова зараз не про ці форми співробітництва. Ми ставимо питання про новий виток розвитку аналітичної журналістики. А він передбачає не стандартний інформаційний обмін по лінії «Влада – ЗМІ», що має односторонній характер (питання-відповідь). Він передбачає врахування думки аналітичних журналістів при прийнятті державних рішень. І перебудовувати відносини виконавчої влади з медіаспільнотою в такому ключі закон не зобов'язує [29, с.170].

Час вимагає більш відповідального реагування на сигнали, що виходять від суспільства, тому розвиток нових форматів державно-медійного партнерства видається цілком доцільним. Разом з тим у регіональної влади є повне право визначати, які ЗМІ включати в ці нові формати взаємодії, а які – ні. В даному випадку принцип рівності мас-медіа, дотримання якого є обов'язковим в рамках встановлених законом форм співпраці (при роботі з запитами), не має значення.

Залучення всіх ЗМІ в такий діалог втрачає сенс. Далеко не всім з них є що сказати владі. І звідси випливає одна проста проблема. Якщо державні структури будуть оцінювати ЗМІ і журналістів, з якими слід або не слід контактувати в нових форматах, природно, їх буде легко звинуватити в упередженості. Тому необхідний якийсь арбітр, який зможе компетентно оцінювати відповідність конкретного журналіста або видання професійним стандартам аналітичної журналістики. А, значить, і давати зрозуміти всі

зацікавлені сторони в конструктивній медіаспівпраці, до чиєї думки в журналістському середовищі варто прислухатися [30, с.217].

Таким арбітром могла б стати, наприклад, гільдія аналітичних журналістів – як колективний виразник позицій медіаспільноти, який об'єднав журналістів різних поглядів, що спеціалізуються на осмисленні суспільно-політичної та соціально-економічної проблематики. Питання про уточнення професійних стандартів і рівні їх дотримання певними виданнями (каналами) і журналістами необхідно вирішувати як поза стінами конкретної редакції, так і, зрозуміло, поза коридорами влади. Тільки при такому підході можливе винесення зважених і адекватних оцінок. Саме на них влада могла б орієнтуватися при побудові нової моделі взаємодії влади і ЗМІ – інтерактивної, а не директивної [30, с.220].

Але для запуску такого механізму відбору для партнерства і розвитку учасників медійного поля потрібні певні важелі впливу. Такими можуть стати державні гранти для ЗМІ на висвітлення соціально значущої тематики. Гільдія, як ланка в їх розподілі, здатна спільно з органами влади формувати інформаційні замовлення і визначати його виконавців (на конкурсній основі), керуючись не кон'юнктурними міркуваннями, а професійними вимогами. Вважаємо, державні гранти слід розглядати насамперед як спосіб дати імпульс для переходу на нові рейки ефективнішої і конструктивної медіа-співпраці не тільки органів влади та ЗМІ, а й інших сторін, присутніх в публічному просторі : громадських організацій, бізнесу, громадських активістів та ін.

Нині у розвитку комунікаційних суспільних процесів інформація стає головним ресурсом соціального управління. Відповідно і в державному управлінні інформаційна сфера набуває особливого значення. Органи влади змушені своєчасно і в належному обсязі інформувати широкий загал громадськості про свою діяльність.

Постає питання ефективної організації взаємодії між інститутами влади і ЗМІ. Під взаємодією органів державної влади та ЗМІ розуміється сукупність цілеспрямованих впливів, а також інших дій органів державної влади та ЗМІ

по відношенню один до одного, пов’язаних з отриманням, обробкою та розповсюдженням інформації. Подібна сукупність взаємних дій є процесом, оскільки має фазовий характер і обмежена часовими і змістовними рамками надзвичайної ситуації, як особливого соціального явища [35].

Для кожної фази взаємодії із засобами масової інформації можуть бути визначені свої цілі і завдання. Процес взаємодії поряд із зовнішніми умовами визначається також інституційними інтересами і суперечностями, що виникають в цей період, між органами державної влади та ЗМІ. При взаємодії в умовах надзвичайної ситуації становище значно ускладнюється. Громадськість вимагає від влади негайно пояснити, що сталося, і які заходи до запобігання вже прийняті. Це пов'язано з природою надзвичайної ситуації, як кризового соціального явища.

У загальному вигляді надзвичайна ситуація – це обставина, що склалася на певній території в результаті аварії, небезпечного природного явища, катастрофи, стихійного чи іншого лиха, які можуть спричинити або призвели до людських жертв, шкоду здоров'ю людей або навколишньому природному середовищу, значні матеріальні втрати і порушення умов життєдіяльності людей.

Соціальний контекст надзвичайної ситуації полягає в тому, що надзвичайною є антигуманна ситуація, яка порушує безпеку громадян і викликає громадський резонанс. З цих визначень випливає, що суспільна увага повністю прикута до надзвичайної ситуації, якщо вона є резонансною : така ситуація займає на деякий час практично весь інформаційний простір, стає актуальною, соціально значущою [40, с.168].

У такій ситуації має місце :

– дефіцит тимчасових і інформаційних ресурсів для прийняття управлінського рішення;

– пильна увага громадськості до ситуації;

– завищені очікування громадськості щодо того, що органи влади негайно приймуть адекватні заходи з ліквідації надзвичайної ситуації.

Таким чином, для органів державної влади особливо актуальна наявність партнерських взаємовідносин зі ЗМІ в період несподіваної резонансної надзвичайної ситуації. Від професіоналізму, вміння чиновників спілкуватися з населенням, взаємодіяти зі ЗМІ в подібні критичні моменти залежить рівень легітимності влади.

Трендом сучасного регіонального медіаполя стає створення видавничих будинків, що включають в себе друковані видання, а також використання нових технологій в телебаченні. В цілому можна констатувати, що відбуваються трансформації, обумовлені побудовою інформаційного суспільства, але при цьому не завжди поділ ринку масмедіа є системним.

Моніторинг свідчить, що проблемою залишається мінімізація критичних виступів в ЗМІ з питань діяльності органів державної влади; незатребуваність владними структурами єдиної думки при прийнятті соціально значимих рішень; часто необґрунтованим є використання ЗМІ для власного іміджу [43, с.90].

Яскравою ілюстрацією недостатньої відкритості органів державної влади є наявність фактів відмов у наданні інформації журналістам. Крім відсутності зворотного зв'язку між населенням та іншими суб'єктами інформаційного простору в числі найбільш її актуальних проблем для розвитку інформаційного суспільства експертами називається необґрунтовано підвищений контроль над засобами масової інформації з боку держави і, отже, висока залежність ЗМІ. В даному контексті озвучується і інша дуже важлива проблема – зниження довіри до засобів масової інформації, а відповідно і їх ступеню впливу на громадську думку.

У той же час саме державні засоби масової інформації в більшій мірі забезпечують функцію інформування громадян з актуальних суспільно політичним, соціально значущих питань. Основними темами, які висвітлюються в засобах масової інформації, як свідчить моніторинг, стали модернізація політичної системи, освіти і правоохоронних органів, реформування МВС, підтримка соціально-орієнтованих не комерційних

організацій, заходи щодо поліпшення інвестиційного клімату та інноваційної діяльності держави. Пріоритетними являються теми соціальної спрямованості.

Далеко не у всіх районах склався рекламний ринок, який здатний забезпечити існування видань, а він для людей є одним з найважливіших джерел інформації. Новітні тенденції в розвитку зарубіжних ЗМІ характеризуються перш за все перенесенням ділової та оперативної інформації в комп'ютерні мережі, збільшення питомої ваги аналізу, коментарями і прогнозами, перенесенням центру уваги на персональну журналістику. Така тенденція пробиває собі дорогу і в Україні.

Засоби масової інформації покликані стати реальним механізмом взаємодії суспільства і влади, нести місію духовного оздоровлення. Отже, основу державної інформаційної політики має складати формування такої системи діяльності засобів масової інформації, яка дозволить суспільству отримувати різноманітну, достовірну інформацію соціально-політичного плану і адекватно сприймати її [55, с.406].

Загальний соціально-психологічний клімат в Україні характеризується втратою багатьма громадянами впевненості у своєму реальному становищі і перспектив у майбутньому, руйнацією багатьох ідеалів суспільства, атмосфери насильства, жорстокості, що панує та культивується найчастіше засобами масової інформації. На цьому благодатному ґрунті виростає насіння злочинності і тероризм набуває масштабів національного лиха.

Разом з позитивними аспектами інтеграційних процесів є і негативні, пов'язані з єдиним інформаційним простором. Нав'язлива участь країн-сусідів у вирішенні внутрішніх проблем інших держав закінчується часом їх жорсткими діями : від економічної та політичної блокади до проведення військових акцій.

Є одна сфера – етнокультурна, яка у відкритому інформаційному просторі зазнає втручань інших країн. Ще одним небажаним моментом стає перенесення негативних цінностей та установок з одного суспільства до іншого, а іноді привнесення ідей та норм, що дисонують з історичною та

етнографічною культурою суспільства. Подібні моменти провокують внутрішні соціально-психологічні кризи, що викликають посилення сепаратистських настроїв, розвиток етнічного, релігійного, політичного та інших форм екстремізму, руйнують механізми соціального контролю [60, с.174].

Найбільшою загрозою стають процеси підміни культурної складової суспільного життя принципами та нормами суспільства-споживання, це неминуче знижує освітній, демографічний та культурний потенціал суспільства, спричиняє формування інертних суспільств. Національні ЗМІ можуть самостійно збирати, аналізувати та оцінювати інформацію, створювати свій порядок денний.

Однак аудиторія до цього моменту, можливо, вже отримала первісне уявлення про проблему через систему глобального мовлення : каналами телебачення і через Інтернет. Тому національним ЗМІ потрібно виробити унікальний інструмент з формування суспільного уявлення про проблему всередині національного інформаційного поля. При цьому ЗМІ повинні самі вирішити, яку позицію вони займуть відносно подій : чи підтримають позицію глобального мовника, чи відстоюватимуть власні переконання, чи стануть на позицію свого уряду.

У момент початку інформаційно-психологічного протиборства неминуче відбувається розкол та позиціонування сторін учасників інформаційного процесу. При найбільшому розмаїтті причин, що викликали інформаційно-психологічне протиборство, завжди утворюється атакувальна сторона. Такою атакуючою стороною є ЗМІ, які співчувають терористичним організаціям. Є і сторона, що обороняється. Як правило, це засоби масової інформації, що підтримують позиції сторони, що бореться з тероризмом, хоча деякі можуть зайняти позицію спостерігача. Найчастіше цю роль відіграють мас-медіа інших держав, які не беруть участь у конфлікті, та власні опозиційні ЗМІ, здатні не лише висвітлювати конфлікт зі сторони, а й саботувати контртерористичну інформаційну політику [63, с.58].

Таким чином, на міжнародному рівні необхідно забезпечити :

– організацію міждержавного співробітництва у роботі міжнародних організацій, громадських комітетів та комісій у проектах розвитку світових інформаційних мереж;

– створення єдиного антитерористичного простору країн-союзників;

– вироблення механізмів взаємного інформування про широкомасштабні комп'ютерні атаки і великі інциденти у мережі Інтернет-просторі і навіть методів спільного реагування на загрози інформаційного тероризму.

3.2. Протидія тероризму в інформаційній сфері

Метою протидії тероризму в Україні є захист особистості, суспільства та держави від терористичних загроз та проявів. Основними завданнями у досягненні зазначених цілей є :

– виявлення та усунення факторів, що сприяють виникненню та поширенню тероризму;

– виявлення, попередження та припинення дій осіб та організацій, спрямованих на підготовку та скоєння злочинів терористичного характеру та (або) надання сприяння такій діяльності;

– притягнення до відповідальності суб'єктів терористичної діяльності відповідно до чинного законодавства України;

– припинення спроб перенесення на територію України діяльності міжнародних терористичних організацій, залучення до цього процесу потенціалу міжнародної антитерористичної коаліції;

– постійне вдосконалення правоохоронних органів, підтримка у стані готовності до використання сил та засобів, призначених для виявлення,

попередження, припинення терористичних актів та мінімізації (ліквідації) їх наслідків;

– забезпечення антитерористичного захисту об'єктів терористичних посягань – критичної інфраструктури, життєзабезпечення та місць масового перебування людей;

– протидія розповсюдженню ідеології тероризму, здійснення активних інформаційно-пропагандистських заходів антитерористичного спрямування [6, с.269].

Загальнодержавна система протидії тероризму (далі – ЗСПТ) являє собою сукупність організаційних структур (суб'єктів протидії тероризму), які в рамках повноважень, встановлених законами та виданими на їх основі нормативно-правовими актами, здійснюють діяльність з протидії терористичним загрозам, розробляють та реалізують антитерористичні заходи, а також діяльність з виявлення та припинення терористичної діяльності, мінімізації та ліквідації можливих наслідків терористичних актів.

В силу покладених завдань ЗСПТ, покликана забезпечити системне та ефективне використання потенціалу держави та суспільства для захисту від загроз терористичних актів. Форми та методи протидії терористичним проявам визначаються складною соціально-політичною та військовою природою тероризму. Суб'єктами ЗСПТ є уповноважені органи державної влади, до компетенції яких входить проведення заходів щодо протидії тероризму, недержавні організації та об'єднання, а також окремі громадяни, які сприяють органам державної влади у здійсненні заходів у цій сфері.

Відповідно до Конституції України Президент :

– визначає основні напрями державної політики в галузі протидії тероризму;

– встановлює компетенцію державних органів виконавчої влади щодо боротьби з тероризмом;

– приймає рішення в установленому порядку про використання за межами території України формувань Збройних Сил України та підрозділів

спеціального призначення для боротьби з терористичною діяльністю, що здійснюється проти України.

ВРУ формує законодавчу основу протидії тероризму на державному рівні. КМУ :

– визначає компетенцію державних органів виконавчої влади, у сфері протидії тероризму;

– організує розробку та здійснення заходів щодо запобігання тероризму та мінімізації та (або) ліквідації наслідків його прояву;

– організує забезпечення діяльності державних органів виконавчої влади, органів виконавчої влади України та органів місцевого самоврядування щодо протидії тероризму необхідними силами, засобами та ресурсами [2, с.113].

Державні органи виконавчої влади здійснюють діяльність із протидії тероризму у межах своїх повноважень. Органи місцевого самоврядування в межах своїх повноважень організовують та здійснюють діяльність із профілактики тероризму, а також щодо мінімізації та (або) ліквідації наслідків його прояву.

Для протидії терористичним загрозам, спрямованим проти українських громадян та установ за кордоном, у тому числі військових та важливих державних об'єктів, організації та проведення невідкладних дій щодо реагування на загрози терористичних актів при дипломатичних представництвах створюються кризові штаби. У разі нових загроз терористичних актів у законодавчому порядку можуть створюватися й інші організаційні структури протидії тероризму.

Необхідними умовами ефективності ЗСПТ є постійна та активна участь у протидії тероризму адміністрації підприємств, установ, а також громадян, громадських об'єднань, інших інститутів громадянського суспільства та координація їхньої діяльності із суб'єктами ЗСПТ.

Основними напрямками діяльності системи протидії тероризму є :

– силова протидія тероризму;

– усунення внутрішніх джерел тероризму;

– протидія міжнародному тероризму та участь в усуненні його джерел;

– зниження тяжкості наслідків терористичних атак;

– моніторинг обстановки всередині країни та за її межами з метою виявлення потенційних терористичних загроз [4, с.92].

Профілактика тероризму здійснюється за трьома основними напрямами :

– організація та здійснення на системній основі протидії ідеології тероризму та екстремізму;

– вдосконалення антитерористичної захищеності потенційних об'єктів терористичних цілей;

– посилення контролю над дотриманням адміністративних, правових та інших режимів, які сприяють протидії тероризму [16, с.41].

Протидія ідеології тероризму включає комплекс організаційних, соціально-політичних, інформаційно-пропагандистських заходів щодо попередження поширення в суспільстві переконань, ідей, настроїв, мотивів, установок, спрямованих на докорінну зміну існуючих соціальних і політичних інститутів держави.

Як потенційні об'єкти терористичних посягань можуть розглядатися будь-які фізичні та юридичні особи, місця масового перебування людей, об'єкти нерухомості, критичної інфраструктури, транспорту, життєзабезпечення, комунікаційні та інформаційні мережі. Під антитерористичною захищеністю потенційних об'єктів терористичних намірів слід розуміти комплексне використання сил фізичного захисту, інженерно-технічних засобів та режимних заходів, спрямованих на забезпечення їхнього безпечного функціонування.

У зв'язку з цим особлива роль належить ефективній реалізації адміністративно-правових режимів, передбачених законодавством України [20, с.316].

Зусилля світової спільноти можуть бути зосереджені на таких напрямках :

– вироблення міжнародно-правових механізмів захисту інформаційного простору держав-партнерів від поширення ідеології тероризму, пропаганди насильства, тероризму та радикалізму, вдосконалення національного законодавства держав, спрямованого на підвищення соціальної відповідальності масової інформації, що блокує їхню деструктивну діяльність;

– припинення державами-партнерами терористичної та екстремістської пропаганди в мережі Інтернет, з урахуванням того, що запровадження лише національних заборонних правових норм виявляється малоефективним через створення та реєстрацію сайтів терористичної спрямованості в доменній зоні на території інших країн;

– координація діяльності громадських, культурних та інших гуманітарних ресурсів держав-партнерів у сфері протидії ідеології тероризму та екстремізму для забезпечення населення достовірною та об'єктивною інформацією, що гарантує від упередженості та цілеспрямованого спотворення фактів, що завдають морально-психологічних збитків користувачам і слухачам засобів масової інформації.

Сучасна наукова думка має бути спрямована на пошук відповідей на проблемні питання, пов'язані з інформаційною протидією тероризму. Необхідне вироблення єдиних підходів до розуміння суті проблеми, механізмів формування та реалізації державної політики у сфері інформаційної протидії тероризму. Зберігається потреба у наукових дослідженнях узагальнюючого характеру, що створюють методологічну основу вирішення практичних завдань розробки та реалізації державної політики у сфері інформаційної протидії тероризму, уточнення її предметної галузі, цілей, принципів та методів реалізації [30, с.123].

Додаткового наукового обґрунтування вимагає процес ліквідації організаційного розриву між рівнями та напрямками інформаційного протиборства в країні, гармонійного вбудовування інформаційної протидії тероризму в загальну систему внутрішнього і зовнішнього інформаційного протиборства України.

При цьому як пріоритетні напрямки наукових досліджень і тем дисертаційних робіт у галузі інформаційної протидії тероризму в Україні доцільно визначити :

– загальнометодологічні проблеми інформаційної протидії тероризму в Україні;

– проблеми нормативного правового регулювання відносин у галузі інформаційної протидії тероризму;

– проблеми забезпечення безпеки особистості, суспільства та держави від деструктивних інформаційних впливів;

– проблеми забезпечення безпеки індивідуальної, групової та масової свідомості від терористичних загроз;

– проблеми оцінки ефективності заходів щодо інформаційної протидії тероризму;

– проблеми формування та реалізації державної політики в галузі інформаційної протидії тероризму як гармонійної складової державної політики в галузі забезпечення національної безпеки України;

– загальнометодологічні проблеми кадрового забезпечення діяльності у сфері інформаційної протидії тероризму.

ВИСНОВКИ

В результаті проведеного дослідження вдалося сформулювати такі висновки.

1. Активізація тероризму, що ставить під загрозу нормальне існування світоустрою, вимагає від світової спільноти пошуку ефективних методів протидії. Відмінною рисою інформаційного тероризму є його дешевизна та складність виявлення. Анонімність, що забезпечується Інтернетом, дозволяє терористу стати невидимим і, як наслідок, практично невразливим, адже він не ризикує життям під час проведення злочинної акції.

Ситуація погіршується тим, що злочини в інформаційній сфері караються суттєво менше, ніж за здійснення «традиційних» терористичних актів. Однією з найважливіших проблем протидії тероризму є проблема обґрунтування заходів щодо забезпечення антитерористичного та протикримінального захисту об'єктів. Вирішення цієї проблеми можливе при адекватній оцінці ефективності цих заходів, у тому числі методами аналітичного моделювання.

2. На відміну від традиційного тероризму, який стосувався основ життєдіяльності суспільства, сучасний високотехнологічний тероризм здатний продукувати системну кризу в будь-якій державі з високорозвиненою інформаційною інфраструктурою. Розвиток соціальних мереж супроводжується все більш широким використанням їх можливостей для здійснення інформаційного протиборства, зростанням координації, масштабів та складності дій його учасників, якими найчастіше виступають як держави, так і окремі організовані групи, в тому числі терористичні.

Об'єктом атак все частіше стають інформаційні ресурси, виведення з ладу або утруднення функціонування яких може завдати значній економічній шкоді, стороні, яка бореться з тероризмом, або викликати великий суспільний резонанс. Усі провідні держави серйозно стурбовані проблемами інформаційної безпеки, і це, зазвичай, швидко відбивається у їх законодавстві.

3. Комплексне вирішення завдань протидії інформаційному тероризму дозволить суттєво знизити ймовірність реалізації його загроз щодо критичної інфраструктури та забезпечити захист національних інтересів. Економічну та науково-технічну політику підключення до світових відкритих мереж слід розглядати крізь призму вирішення питання національної інформаційної безпеки. Участь України у міжнародних системах телекомунікацій та обміну інформацією має мати плановий характер, здійснюватися відповідно до потреб, економічних і технологічних можливостей та бути монополією держави.

В даний час актуальною є необхідність вироблення жорстких кордонів інформаційного тероризму, що дозволяють чітко відмежовувати інформаційний тероризм від дій, які зовні мають його ознаки. Одночасно необхідно звернути увагу і на об'єктивно існуючі труднощі, викликані тим, що інформаційний тероризм – явище досить складне, багатогранне, що найчастіше має міжнародний характер. Тому виникають проблеми відповідності понять інформаційного тероризму, зафіксованих у міжнародних документах та національних законодавствах, та вироблення комплексних заходів колективної безпеки, спрямованих на боротьбу із цим видом злочинів.

4. Як кримінально-правове явище інформаційний тероризм повинен мати чіткий характер і чіткі межі. Це необхідно в силу відомої формальності права та обов'язковості встановлення достатніх підстав для притягнення до кримінальної відповідальності (ознаки складу кримінального правопорушення). Як кримінально-правовий феномен інформаційний тероризм може мати міжнародний характер і відповідно до ряду міжнародних документів, належати до міжнародних кримінальних правопорушень. Форми його прояву у цій якості досить різноманітні.

Однак у зв'язку з відсутністю міжнародних кримінально-правових санкцій та органу, який би розглядав такі справи, відповідальність за скоєння названих злочинів настає за національним кримінальним законодавством. На наш погляд, у нормативно-правових актах необхідно відобразити, що

інформаційний тероризм як кримінально-правове явище має такі відмітні ознаки :

– найчастіше як інструмент використовується мережа Інтернет;

– інформаційний тероризм завжди має публічний, тобто демонстративний та ультимативний характер;

– навмисно створює та підтримує обстановку страху, паніки, напруженості, пригніченості та паралізує соціально корисну діяльність громадян, нормальне функціонування органів влади та управління, а також громадських формувань та об'єднань;

– породжує загальну небезпеку для невизначеного кола осіб і створює реальну загрозу загибелі людей, заподіяння значної матеріальної шкоди чи інших суспільно-небезпечних наслідків, тобто представляє «розсіяну» загрозу та небезпеку для населення та суспільства;

– шляхом створення обстановки страху впливає на інших осіб або примушує їх до будь-яких дій на користь терористів або прийняття їх умов;

– небезпечне насильство при інформаційному тероризмі застосовується щодо одних осіб чи майна, а психологічний вплив направляється на інших осіб.

5. Існує багато способів, за допомогою яких терористичні групи використовують можливості новітніх інформаційних технологій та глобальну мережу Інтернет у своїх цілях :

– інформування про терористичні рухи, їх цілі та завдання, звернення до масової аудиторії для пропаганди своїх цілей та ідеології, інформування про майбутні і вже сплановані дії, а також оприлюднення своєї відповідальності за вчинення терористичних актів;

– інформаційно-психологічний вплив, у тому числі ініціація «психологічного тероризму» – за допомогою соціальних мереж можна розповсюджувати різні чутки, у тому числі і тривожні, посіяти паніку, ввести в оману;

– деталізація даних про передбачувані цілі, їх місцезнаходження та характеристики;

– збір, у тому числі здирництво грошей для підтримки терористичних рухів;

– публікація відомостей про вибухові речовини та вибухові пристрої, отрути, отруйні гази, а також інструкцій щодо їх самостійного виготовлення;

– використання можливостей електронної пошти або електронних дощок оголошень для надсилання зашифрованих повідомлень, у тому числі візуальної інформації у вигляді карт, військової та технічної документації. Тероризм більше не обмежений територією тієї держави, де ховаються терористи, бази підготовки терористичних операцій вже, як правило, не розташовуються в тих країнах, де є цілі терористів, а самі терористичні організації приймають мережеву структуру;

– залучення в терористичну діяльність нових членів, у тому числі хакерів, яким не відомо до якої кінцевої мети приведуть їх дії;

– заміна інформаційного змісту сайтів, яка полягає у заміні електронних сторінок або їх окремих елементів внаслідок злому. Такі дії вживаються в основному для привернення уваги до атакуючої сторони, демонстрації своїх можливостей або є способом вираження певної політичної позиції. Крім прямої заміни сторінок широко використовується реєстрація в пошукових системах сайтів протилежного змісту за однаковими ключовими словами, а також перенаправлення (підміна) посилань на іншу адресу, що призводить до відкриття спеціально підготовлених сторінок;

– семантичні атаки, метою яких є злом сторінок і подальше розміщення (без помітних слідів злому) на них явно неправдивої інформації. Подібним атакам, як правило, піддаються найчастіше популярні інформаційні сторінки, змісту яких користувачі повністю довіряють;

– виведення з ладу або зниження ефективності функціонування структурних елементів інформаційно-телекомунікаційних систем шляхом : застосування спеціальних програмних та апаратно-програмних засобів на основі програмного коду (програмні та апаратні закладки, комп'ютерні віруси, мережні черв'яки тощо);

– масового розсилання електронних листів (одна з форм «віртуальної блокади»);

– DOS-атаки, проведення яких аналогічне технології масової розсилки електронних листів, що призводить до уповільнення роботи серверу, що обслуговує, або повного припинення зовнішнього доступу до його ресурсів.

Комплексне вирішення проблем інформаційного тероризму дозволить вживати в централізованому порядку необхідні контрзаходи для протидії кібертероризму, суттєво знизити ймовірність реалізації його загроз щодо критичної інфраструктури та забезпечити захист своїх національних інтересів.

Економічну та науково-технічну політику підключення до світових відкритих мереж слід розглядати крізь призму вирішення питання національної інформаційної безпеки. Участь України у міжнародних системах телекомунікацій та обміну інформацією має мати плановий характер, здійснюватися відповідно до існуючих потреб, економічних і технологічних можливостей і бути монополією держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Арквілл Дж., Ронфельдт Д. Мережі і мережні війни : майбутнє терору, злочинності та бойових дій Київ : Києво-Могилянська академія, 2005. 350 с.

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

3. Біленчук П. Д. Засоби масової інформації і тероризм // Віхи історії. 2003. № 2 (4). С. 21–29.

4. Богданович В.Ю., Рижов І.М., Варенья Н.М. Концепція побудови системи протидії загрозам терористичного характеру як складової системи забезпечення національної безпеки // Зб. наук. пр. НА СБ України. 2016. № 60. С.85 – 93.

5. Богуш В. М. Інформаційна безпека держави Київ : МК – Прес, 2015. 432 с.

6. Бойченко О.В. Медіа – тероризм : особливості сучасних ознак інформаційній безпеці. Інтегровані інтелектуальні робототехнічні комплекси // (ПРТК – 2009) : друга міжнар. наук. – практ. конф. (25 – 28 травня 2009 р.). Київ : НАУ, 2009. С. 230 – 232.

7. Бондарсук О.В. Відображення у дискурсі ЗМІ пропагандистських кампаній // Political science. № 12 (104). 2013. С.49 – 53.

8. Борисова Л. В. Інформаційна безпека як визначальний компонент національної безпеки України. // Право і безпека. 2013. №1. С. 39–42.

9. Бутузов В.М. Сучасні загрози : комп'ютерний тероризм // Боротьба з організованою злочинністю і корупцією (теорія і практика). 2007. Вип. 17. С. 316 – 324.

10. Валюшко І. О. Кібербезпека України : наукові та практичні виміри сучасності // Вісник НТУУ «КПІ» Політологія. Соціологія. Право. 2016 № 3/4 (31 – 32). С. 117 – 124.

11. Валюшко І. О. Основні виклики і загрози в епоху інформаційних війн // Науковий вісник Дипломатичної академії України. Зовнішня політика і дипломатія : традиції, тренди, досвід. Частина ІІ. Серія «Політичні науки» / За заг. ред. В.Г. Ціватого, Н.О. Татаренко. 2016. С. 142–147.

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.

13. Галамба М.М**.** Інформаційно – психологічна складова терористичної діяльності // Юридичний журнал. 2006. № 11. С. 53 – 57.

14. Галицький І. Екстремізм в соціальних мережах : організаційно – правові заходи протидії // Альманах міжнародного права. 2014. Вип. 4. С. 74 – 83.

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

16. Геращенко О.С. Кібертероризм як фактор загрози національній безпеці України : генеза поняття та шляхи протидії // Південноукраїнський правничий часопис. 2016. № 3–4. С. 39–42.

17. Глазов О. В. Міжнародний інформаційний тероризм в контексті загроз національній безпеці України // Наукові праці. Політологія. 2012. Випуск 185. Том 197. С. 78 – 82.

18. Горошко О. Гендерні аспекти Інтернет – комунікацій : автореф.дис. д-ра соціол. наук : спец. 22.00.04 // «Спеціальні та галузеві соціології» ; Харківський національний університет імені В. Н. Каразіна. Харків, 2009. 36 с.

19. Гребенюк М.В., Рижов І.М., Кузьмін С.П. Перспективи інноваційного розвитку антитерористичних стратегій // Вісник прокуратури. 2016. 5 (179). С.19 – 28.

20. Грицун О. О. Питання міжнародно-правового регулювання інформаційного тероризму // Часопис Київського університету права. 2014. № 4. С. 312 – 317.

21. Демків Т. Ф. Взаємодія органів державної виконавчої влади з засобами масової інформації (на прикладі досвіду Державної податкової служби України) Сучасна регіональна політика : формування, реалізація та розвиток публічної служби // матеріали підсумк. наук. – практ. конф. за міжнар. участю. Одеса : ОРІДУ НАДУ, 2010. С. 461−463.

22. Жарков Я. М., Компанцева Л. Ф., Остроухов В.В. Історія інформаційно – психологічного протиборства // підручник. Київ : Наук. – вид.відділ НА СБ України, 2012. 209 с.

23. Жарков Я. Небезпеки особистості в інформаційному просторі // Юніан. URL : http : //webcache.ghttp : //www.justinian.com.ua/article.php?id=2554. (дата звернення : 07.11.2022)

24. Ізетов А. Е. Втягнення у вчинення терористичного акту : кримінально – правове дослідження // монографія. За заг. ред. д – ра юрид. наук, проф. В. П. Ємельянова. Харків : Право, 2010. 174 с.

25. Ірха Ю.Б. Екстремістська діяльність у мережі Інтернет : правові проблеми виявлення та протидії в Україні. Інформаційні технології та безпека // матеріали XV Міжнародної науково – практичної конференції. Київ, 2015. С. 106 – 109.

26. Клименко О.Ю. Залучення дітей до участі у збройних конфліктах : моделі та методи вербування (український досвід) // Соціологічні студії. 2019. №2(15). С. 13–20.

27. Корченко О.Г. Ознаковий принцип формування класифікацій кібератак // Вісник Східноукраїнського національного університету імені Володимира Даля. 2010. №1. С. 32 – 38.

28. Коршунов В. О. Політичний тероризм : інформаційні методи боротьби // автореф. дис. на здобуття наук. ступеня канд. політ. наук : спец. 23.00.02 – Політична інститути та процеси. Дніпропетровськ, 2008. 18 с.

29. Коцур В. Тероризм і засоби масової інформації : межа об’єктивності і мас – медіального продовження теракtів. Політичний менеджмент. 2009. №6. С. 167 – 172.

30. Крутов В. В., Стрельбицький М. П., Шевченко О. А.Протидія інформаційному тероризму та його фінансуванню в сучасних умовах // Монографія. Київ : Вид – во НАПрНУ, 2014. 310 с.

31. Кудінов С. С., Рижов І. М., Івахненко О. А. Основи антитерористичної безпеки соціальних систем : монографія. Київ : Кафедра, 2017. 212 с.

32. Леонов Б. Д., Лихова С. Я. Інформаційний тероризм як загроза національній безпеці України // Наукові праці Національного авіаційного університету. Серія : Юридичний вісник «Повітряне і космічне право». 2021. Т. 2, № 59. С. 170 – 176.

33. Леонов Б.Д. Тероризм в аспекті діяльності засобів масової інформації // Інформація і право. 2014. № 1(10). С.87 – 92.

34. Леонтьєва Л. Є. Пропаганда як інформаційно – психологічний складник політичних процесів Львівський нац. Ун-т ім. Івана Франка. Київ, 2004. 298 с.

35. Манаєнко Д., Гамова І. Медіа – тероризм та проблеми боротьби з ним у сучасному суспільстві // ДТЕУ. URL : https : //knute.edu.ua/file/NjY4NQ==/b834713145faf 79086ceda048007cfe0.pdf. (дата звернення : 03.11.2022)

36. Матула М. М. Феномен інформаційного тероризму як загрози національній та міжнародній безпеці. // Науковий блог Національний університет «Острозька академія». 2014. URL : https : //naub.oa.edu. ua/2014/fenomen-informatsijnoho-teroryzmu-yak-zahrozy-natsionalnij-ta-mizhnarodnij- bezpetsi. (дата звернення : 03.11.2022)

37. Мельник Д. ЗМІ – «рупор» тероризму чи елемент протидії? // Проблеми безпеки : особистості, суспільства, держави. 2007. № 7/07. С. 88.

38. Мельник Д. Мережа Інтернет як засіб поширення інформації екстремістського змісту // зб. матеріалів «круглого столу» «Запобігання радикалізації і тероризму : міжнародний досвід і національний вимір» за ред. М.Г. Гуцало. Київ : НІСД, 2012. С. 88 – 91.

39. Міжнародна конвенція про боротьбу з вербуванням, використанням, фінансуванням та навчанням найманців від 4.12.1989 року. № 3381-XII // База даних «Законодавство України» / ВР України URL : https : //zakon.rada.gov.ua/go/995_103 (дата звернення : 07.11.2022)

40. Нестеряк Ю. Державна інформаційна політика України : теоретико – методологічні засади // монографія. Київ : НАДУ, 2014. 292 с.

41. Остроухов В., Петрик В. До проблеми забезпечення інформаційної безпеки України // Політичний менеджмент. 2008. № 4(31). С. 135 – 141.

42. Панченко В., Семчишина С. Тактичні пріоритети України у сфері забезпечення інформаційної безпеки у сучасних умовах // зб. матер. наук. – практ. конф. Актуальні проблеми управління інформаційною безпекою держави. Київ : Центр навчальних наукових. та періодичних видань НА СБ України, 2015. С. 83 – 85.

43. Петрик В. Пропозиції щодо підготовки фахівців з інформаційної безпеки держави та формування критичного мислення населення для захисту від шкідливих інформаційно – психологічних впливів зб. матер. наук. – практ. конф. Актуальні проблеми управління інформаційною безпекою держави // Київ : Центр навчальних, наукових та періодичних видань НА СБ України, 2015. С. 89 – 93.

44. Петришин Г. Р. Інформаційний тероризм : джерела формування та активізації в Україні. Габітус // науковий журнал. Одеса : Гельветика, 2021. Вип. 21. С. 44 – 50.

45. Пивоваров В. В., Лисенко С. Ю. Кіберзлочинність : кримінологічний погляд на генезис явища та шляхи запобігання // Право і суспільство. 2016. № 3. С. 177–182.

46. Пилипчук В.Г., Дзьобань О.П. Теоретичні та державно – правові аспекти протидії інформаційному тероризму в умовах глобалізації // Стратегічні пріоритети. № 4. 2011. URL : http : //www.nbuv.gov.ua/old_jrn/soc_gum/sp/2011_4/012-017.pdf. (дата звернення : 07.11.2022)

47. Погорецький М.А. Поняття кіберпростору як середовища вчинення злочину. Інформаційна безпека людини, суспільства, держави. №2 (2). 2009. С. 80.

48. Притула А. М. Пропаганда – компонент гібридної війни : шляхи протидії засобами кримінального права // Юридична наука. 2015. № 3. С. 99–104.

49. Про запобігання тероризму Конвенції Ради Європи від 16.05.2005 р. № 54-V // База даних «Законодавство України» / ВР України URL : https : //zakon.rada.gov.ua/laws/show/994_712#Text (дата звернення : 03.11.2022)

50. Про засади інформаційної безпеки України : Проект Закону України від 28.05.2014 р. № 4949. URL : https : //ips.ligazakon.net/document/JG3TH00A?an=3/ (дата звернення : 03.11.2022)

51. Про національну безпеку України : закон України від 21 червня 2018 року № 2469 – VIII. // База даних «Законодавство України» URL : https : //zakon.rada.gov.ua/laws/show/2469 – 19#Text (дата звернення : 03.11.2022)

52. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» від 28 грудня 2021 р. № 685/2021. // База даних «Законодавство України» URL : https : //zakon.rada.gov.ua/laws/show/685/2021#Text. (дата звернення : 03.11.2022)

53. Пропаганда vs контрпропаганда у медіа просторі : минуле, сучасне, майбутнє // матеріали міжнародної науково-практичної конференції (Запоріжжя, 12 лютого 2018 р.) Запоріжжя : Інтер-М, 2018. 406 с.

54. Резнікова О.О., Місюра А.О., Дрьомов С.В., Войтовський К.Є. Актуальні питання протидії тероризму у світі та в Україні // аналітична доповідь. Київ : НІСД, 2017. 60 с.

55. Рибчановська Н. Протидія пропаганді і поширенню ідеології тероризму в Україні (психолого-правовий аспект) // зб. наук. пр. «Сучасний вимір держави та права» ; за ред. В.І. Терентьєва, О.В. Козаченка. Миколаїв : Іліон, 2008. С. 406 – 407.

56. Рижов І. М. Базові концепти антитерористичної безпеки // монографія. Київ : Нац. акад. СБУ, 2016. 328 с.

57. Рижов І. М. Основи антитерористичної безпеки соціальних систем // монографія. Київ : Кафедра, 2017. 212 с.

58. Рудник Л.І. Соціальні мережі як засіб здійснення терористичних актів. URL ГОСЛ: https : //goal-int.org/socialni-merezhi-yak-zasib-zdijsnennya-teroristichnixaktiv. (дата звернення : 07.11.2022)

59. Рюміна В.І. Інформаційний тероризм як інструмент зовнішньої політики держави на сучасному етапі. Україна в системі глобального інформаційного обміну : теоретико-методологічні аспекти дослідження і підготовки фахівців // матеріали Всеукраїнської науково-практичної конференції, м. Львів, 27 травня 2011 р. Львів : Видавництво Львівської політехніки, 2011. С. 267–269.

60. Саган О. В. Протидія медіа-інформаційному тероризму як питання національної безпеки України // Дис. канд. політ. наук за спеціальністю 21.01.01 основи національної безпеки держави (політичні науки). Національний інститут стратегічних досліджень. Київ. 2021. 224 с.

61. Саприкін О. Інформаційна експансія, інформаційна війна та інформаційна атака у засобах масової інформації на прикладі Євро-2012 // Вісник Книжкової палати. 2013. № 1. С. 40 – 43.

62. Чайковський Д.З. Втягнення у вчинення терористичного акту. Актуальні проблеми правового регулювання в Україні та країнах ближнього зарубіжжя // Матеріали X міжнародної науково-практичної Інтернет конференції (Львів, 28 грудня 2020 року) : тези доповідей / Відп. ред. П.О. Куцик. Львів : Львівський торговельно-економічний університет. 2020. С.217 – 220.

63. 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.

64. Arquilla J. Information – Age Terrorism. Current History. 2000 // PDF file. URL : https : //core.ac.uk/download/pdf/36728897.pdf. (data of access : 07.11.2022)

65. Dorothy E. Denning. Information Operations and Terrorism. 2005 // Cyberloop. URL : https : //www.cyberloop.org/files/a484999.pdf (data of access : 03.11.2022)

66. Forest J. F. Countering Terrorism and Insurgency in the 21st Century : Strategic and Tactical Considerations. Greenwood Publishing Group, 2007. 696 p.

67. Jerrold M. From Car Bombs to Logic Bombs // The Growing Threat from Information Terrorism. Terrorism and Political Violence. 2007. P. 97–122.

68. Robinson P. The CNN Effect : Can the News Media Drive Foreign Policy? // Review of International Studies. № 25(2). 1999. P. 301–309. URL http : //www.jstor.org/stable/20097596. (data of access : 07.11.2022)

69. The use of the Internet for terrorist purposes. United Nations Office on Drugs and Crime. New York, 2012 // Unodc. URL : www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf (data of access : 07.11.2022)

70. Webb K. Information Terrorism in the New Security Environment // Journal of Information Warfare, vol. 6, no. 2, 2007, pp. 15–24. URL : https : //www.jstor.org/stable/26503475. (data of access : 07.11.2022)