ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

БХ – Боко-Харам

ЗМІ – Засоби масової інформації

ІД – Ісламська Держава

ІДІЛ – Ісламська держава Іраку та Леванту

ІКТ – Інформаційно-комунікаційні технології

ІРА – Ірландська республіканська армія

ЛеТ – Лашкар-е-Тайба

СМ – Соціальні мережі

США – Сполучені штати Америки

ТО – терористичні організації

ФРН – Федеративна Республіка Німеччина

ВСТУП

Актуальність теми. Тероризм є однією з ключових проблем не тільки національного рівня, а й регіонального та міжнародного. Діяльність терористичних організацій досить швидко розвивається в сучасному онлайн просторі. На початку XXI століття тероризм став одним з найнебезпечніших явищ, які важко піддаються прогнозуванню, а його види швидко змінюються та адаптуються під нові умови.

На сучасному етапі, міжнародна безпека знаходиться в складній ситуації, що мотивує до пошуку нових рішень та напрацювання більш дієвих контртерористичних заходів як всередині країни, так і на глобальному рівні. Даний процес є нелегким і вимагає відмови від закоренілих стереотипних підходів в оцінці суспільної небезпеки тероризму, а також актуалізує наукові дослідження з цієї проблематики, що мають велике значення на перспективу.

В епоху інформаційного суспільства, коли соціальні мережі стали частиною щоденного життя людини, присутність в інформаційному просторі є надзвичайно важливою складовою для будь-якого суб'єкта, який має на меті пошук своєї аудиторії, поширення власних ідей та їх популяризацію. Стрімкий розвиток інформаційно-комунікаційних технологій створив такий вид тероризму як інформаційний. Також існує психологічний тероризм, який не використовує засоби фізичного впливу на противника і розрахований на вплив інформацією, маніпулюванням та пропагандою, які призводять до ефекту залякування. Збільшення кількості видів тероризму, стрімкий розвиток та зміна інструментів терористичних організацій дають підставу до розгляду даної теми а також пошук, формулювання шляхів її вирішення.

Терористичні організації обрали для себе ідеальний майданчик в цифровому просторі – соціальні мережі. Такі платформи поряд з позитивними якостями мають негативні сторони, які й послугували поштовхом у виборі терористами онлайн-інструментів. До негативних ознак

можна віднести їх дешевизну, вільний доступ, недостатня захищеність даних та їх шифрування, а також використання фейкових облікових записів.

Тому дослідження ролі соціальних мереж в діяльності терористичних організацій та аналіз особливостей сучасного тероризму є актуальним та потребує детального дослідження.

Метою дослідження є аналіз особливостей використання соціальних мереж сучасними терористичними організаціями, та на основі цих даних – формулювання шляхів протидії сучасному інформаційному тероризму.

Завдання:

– проаналізувати та опрацювати наукові літературні джерела по обраній темі;

– дослідити основні види тероризму та виділити їх характерні особливості;

– виявити головні особливості діяльності терористичних організацій в онлайновому просторі;

– здійснити порівняльний аналіз терористичних угрупувань в соціальних мережах;

– створити SWOT-аналіз соціальних мереж з позиції інформаційної безпеки;

– окреслити систему заходів запобігання тероризму, шляхи покращення протидії використанню інформаційно-комунікаційних технологій терористичними угрупуваннями.

Об’єкт дослідження – інформаційний тероризм на сучасному етапі розвитку міжнародних відносин.

Предмет дослідження – використання сучасних соціальних мереж як інструменту терористичних організацій в онлайн просторі.

Методи дослідження. В ході роботи було використано комплекс загальнонаукових і спеціальних методів, включаючи моніторинг, контент-аналіз, історичний метод, логічний, дедукція, порівняльний, а також SWOT-

аналіз. Саме застосовані методи дали комплексну оцінку та результати, які були отримані під час дослідження даної проблеми

Наукова новизна одержаних результатів. Автором був виконаний детальний порівняльний аналіз особливостей діяльності Ісламської Держави й Аль-Каїди в соціальних мережах, виявлені головні відмінні та подібні ознаки, на основі чого створені головні фактори, на яких слід зосередитися при розробці стратегії безпеки в онлайн просторі. Також був здійснений SWOT-аналіз, через призму інформаційної безпеки, окреслені головні можливості подолання тероризму за допомогою соціальних мереж, та можливі загрози. На основі результатів аналізу сформульовані висновки та рекомендації.

Практичне значення одержаних результатів полягає в подальшому використанні результатів дослідження при вивченні особливостей сучасних соціальних мереж, онлайн платформ та інформаційно-комунікаційних технологій в контексті вивчення тероризму; особливостей діяльності терористичних організацій в мережі Інтернет. Висновки по даному дослідженню можуть стати підґрунтям та теоретичною базою для подальшого дослідження проблеми тероризму та боротьби з ним.

Апробація отриманих результатів. Результати дослідження були представлені на:

– XXI Міжнародній науково-практичній конференції здобувачів вищої освіти і молодих учених «Політ. Сучасні проблеми науки»;

– міжнародній науково-практичній конференції «Сучасні міжнародні відносини: актуальні проблеми теорії і практики»;

– Всеукраїнській конференції «Дипломатія в міжнародних відносинах: ретроспекція і перспективи».

Літературна база. В дослідженні проаналізовано роботи таких авторів: Авдєєва Т. [1], Артамонов І.І. [4], Банк Р.О. [6], Бойченко О.В. [9;10], Бугера О. [11], Вахула Б.Я. [14], Гармашов І. [21], Коршунов В.О. [44], Лисенко

А.М. [48], Ліпкан В.А. [49;50;51], Луцький М.Г. [53], Місюра А.О. [60], Требін М.П. [84], Турчин А.В. [85], Хоффман Б. [89], Шульман О. [90], Яцик Т.П. [91], та інші.

Структура роботи. Робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи 94 сторінки (з них 80 ст. основного тексту). Список використаних джерел містить 125 позицій.

РОЗДІЛ 1. ТЕОРЕТИЧНО-КОНЦЕПТУАЛЬНІ ЗАСАДИ ТЕРОРИСТИЧНОЇ ДІЯЛЬНОСТІ.

1.1. Підходи до визначення терміну «тероризм». Проблема класифікації сучасного тероризму.

Зростаюча динаміка терористичних дій на міжнародній арені змушує серйозно замислитися над проблемою сучасного тероризму. Складність даного поняття, різновид трактувань та велика кількість його проявів зумовлюють необхідність в глибокому аналізі та вивченні саме сутності тероризму на різних рівнях: психологічному, технічному, інформаційному, тощо. Крім того, сучасний тероризм є настільки динамічним, різноплановим та «гнучким», що постійно виникає потреба в розумінні даного явища на теоретичному рівні.

Дослідженню поняття «тероризм» присвятили свої праці такі науковці як Кожушко Є. [41] , Петрищев В. [63] , Горовий В.М. [75] , Хоффман Б. [89], Яцик Т.П. [91], Требін М.П. [84] , Грищук В.К. [81], Петрищев В.Є. [63], Матула М.М. [56], Леонов Б.Д. [47], та інші. В контексті міжнародного права та криміналістики дане явище вивчали: Ліпкан В. [49-51], Артамонов І.І. [4], Авдєєва Т. [1], Бабенко Ю. [5], та інші.

Як соціальне явище, тероризм являє собою певну політику, вид ідеології та соціальну практику суспільних суб'єктів (індивидів, груп, інститутів), які зорієнтовані на нелегальній насильницькій формі зміни державного устрою, політичної системи держави та суспільного устрою. За думкою Канціра В., це «несиметрична реакція, яка з'являється в разі незмоги слабшої сторони подолати сильнішу звичайними методами».

Існують певні розбіжності в тлумаченні даного терміну, науковці виділяють його поняття через призму завдання фізичної шкоди, психологічної, через використання спеціальних інструментів, методів та зброї, тощо. Так, наприклад, в словнику В.І. Даля [26] тероризм визначається як певні погрози в фізичному насильстві та знищенні, катуванні та смерті. Академічний тлумачний словник української мови [2] визначає термін тероризм як вид боротьби з політичними та класовими ворогами з використанням фізичного насильства. Словник іноземних слів прирівнює терміни «терор» і «тероризм» і тлумачить їх як певну політику залякування, яка має на меті здійснення насильницьких актів (вбивства, підпали, вибухи, захоплення заручників, тощо). [73;76]

Термін тероризм застосовувався також для опису політичних явищ. Так, ще при Людовіку XVI в Франції термін «тероро» використовувався жирондистами та якобінцями під час народного повстання і повалення кабінету міністрів за допомогою залякування та приведення всіх у жах. Спочатку, терор був звичайним фізичним явищем, націленим на знищення свого супротивника, яке спочатку не передбачало психологічного впливу на опонентів, а лише фізичний. [63]

Появу масового терору пов’язують з Великою Французькою революцією (1789–1795 рр.), під час якої відбувалися жорстокі розправи бурзуазією своїх противників. Робесп’єр визначив тероризм як внутрішню політику, що направлена на знищення класу аристократії.

З появою опозиційних груп, вже в XIX столітті поняття «терор» і «тероризм» перестають поширюватися лише на воєнні дії, та починають розглядатись як окремий вид політичної боротьби. Під «тероризмом» почали розуміти саме політичні вбивства, а поняття «терор» закріпилось як репресивні дії держави.

Варто зауважити, що існують певні розбіжності між поняттями «терор» та «тероризм», серед них можна виділити наступні:

– Зазвичай, тероризм є разовою дією, або серією таких дій, терор в свою чергу характеризується безперервним процес та масовістю;

– Суб'єктом тероризму є не владні структури, терор є прерогативою держави або органів та інститутів;

– суб'єктом терору є суспільно-політичні структури та утворення, а суб'єктами тероризму – окремі фізичні особи;

– суб'єкти терору здійснюють свої дії з метою залякування населення, задля реалізації ними певної поведінки, а ось субєкти тероризму виконуючи злочини, розраховують на певну поведінку представників міжнародних організацій, державної влади та суспільства в цілому;

– терор – це окремий особливий вид здійснення політичної влади, а тероризм в свою чергу – протиправна, злочинна дія, яка переслідується відповідно до внутрішньодержавного та міжнародного права. [62]

Розглядаючи тероризм в контексті сучасного розвитку міжнародних відносин та міжнародної ситуації, слід виділити його головні особливості:

– Здійснення глобальної небезпеки;

– Демонстративний та радикальний характер;

– Свідоме створення напруженої обстановки, напруженості з метою залякування;

– Психологічний та фізичний вплив на окремих людей, або коло людей для задоволення власних цілей;

– Застосування відразу декількох різних каналів та інструментів терористичної діяльності, тощо.

Слід також розглянути погляди різних вчених та науковців щодо проблеми тлумачення поняття «тероризм». Так, кримінолог І.І. Артамонов [4] розуміє під тероризмом будь-який акт насильства або загрозу його скоєння (ушкодження матеріальних об'єктів, захоплення заручників, вбивство, тощо) з метою залякування населення, вплив на прийняття

політичних рішень органами державної влади, створений навмисно різними способами.

Цікаве формулювання запропонував професор В.Петрищев, [63] він пояснював: «Тероризм – це постійне, систематичне явище, яке має політичну, релігійну, соціальну мотивацію та здійснюється з актами насильства, або з погрозою застосування такого, через залякування фізичних осіб та пропаганду власних ідей».

Професор Є.Кожушко, [41] в свою чергу, тлумачить даний термін так: «Тероризм – це тактика політичної боротьби, яка застосовується зі систематичним використанням ідеологічно вмотивованого насильства та проявляється у формі вбивств, саботажах, викраденнях, та інших діях, які становлять загрозу життю та безпеці людей».

Звичайно, варто згадати офіційне визначення, яке наведено у Законі України «Про боротьбу з тероризмом» (від 31 травня 2005 р. Відомості Верховної Ради України). [64] Тут даний термін обґрунтовується так: «Тероризм – це суспільно небезпечна діяльність; свідоме, цілеспрямоване здійснення насильства шляхом вбивств, підпалів, залякування людей, або загрози застосуванні насильства з метою досягнення власних цілей».

Низка тлумачень поняття тероризм запропонована також закордонними вченими. Так, Б. Гано [103] пропонує визначення тероризму наступне: «Тероризм це застосування або загроза застосування насильства, націлений на цивільне населення, або об’єкти з метою досягнення політичної мети».

В даних визначеннях поєднуються три головні ознаки тероризму, без яких він не може бути названий тероризмом, а саме:

– Здійснення насильницьких дій, або погроза ними (психологічний тиск, тощо);
– Мета має політичний характер;
– Об’єктом тероризму є цивільні особи.

Б. Хофман [89] засвідчує, що «фактично, будь-який відкритий прояв насильства вважається антисоціальним явищем, і не має різниці, ким він був здійснений: чи то урядом, чи дисидентами проти уряду, або ж злочинними організаціями та групами, називається тероризмом».

Відомий американський спеціаліст з міжнародного права професор Фальк пропонує два визначення:

– «Тероризм –це будь-який прояв політичного насильства, який неможливо виправдати з адекватної моральної та юридичної точки зору, неважливо, ким він був здійснений – революційною групою, чи урядом»;

– «Тероризм – політичний екстремізм, що здійснюється без розбору, або направлений на невинних осіб». [16]

Аналіз наукової літератури дає змогу виділити наступні істотні ознаки тероризму:

– Насильницький спосіб досягнення мети;

– Подвійний характер об’єкта тероризму (прямий вплив саме на об’єкт впливу, та на кінцевий – стратегічний об’єкт);

– Створення психологічної напруги та підтримка обстановки страху через залякування;

– Відкритість та публічність терористичних дій;

– Висока соціальна небезпека через прямий вплив на випадкових осіб та їх заохочення до терористичних дій.

Тож, сьогодні тероризм є методом злочинного, протиправного протистояння, насильства, який вже втратив свій індивідуальний характер, та націлений на велику кількість жертв. Він відноситься до однієї з глобальних проблем людства, яка підриває безпеку всього міжнародного товариства.

Проблемою вивчення даного явища також є різноманіття форм, проявів та видів тероризму, тож варто також розглянути погляди науковців щодо класифікації тероризму. В першу чергу, потрібно проаналізувати досить

широку класифікацію В.А. Ліпкана за різними ознаками. В першу чергу, вчений виділяє наступні види тероризму, що класифікуються за своїм територіальним впливом:

– Міжнародний (транснаціональний) – здійснення терористичний дій злочинними угрупуваннями, що но обмежуються державними кордонами, а держава не є суб'єктом.

Міжнародний тероризм можна характеризувати наступними ознаками: будь-який вид підтримки (матеріальний, технічний, організаційний) надходить з-за кордону; терористичні організації мають на мети здійснювати вплив більш ніж на одну державу, а шкоду від тероризму нанесено різним міжнародним організаціям та країнам.

У ст.1 Закону України «Про боротьбу з тероризмом» міжнародний тероризм визначається як небезпечні діяння виконані терористичними угрупуваннями, організаціями з метою вбивства, викрадення, захоплення невинних людей, зруйнування важливих державних об'єктів, систем комунікацій, життєзабезпечення; застосуванням чи загрозою застосування ядерної, біологічної, хімічної, та іншої зброї масового ураження в світовому чи регіональному масштабі. [2]

Наступним видом тероризму за територіальною ознакою є внутрішній або тотальний тероризм. Його дія розповсюджується по всій території країни. Така ситуація може відбуватися в разі слабкої державної влади, або коли держава перебуває в стані латентної війни й терористичні акти створюють небезпечну обстановку та підривають безпеку держави загалом.

Тобто, до внутрішнього тероризму відносять політично мотивовані вбивства громадських або державних діячів даної держави, посягання на її конституційні основи та створення незаконних угрупувань. Яскравим прикладом внутрішнього тероризму є «червоні бригади», які діяли на території Італії в 70-80-х рр. XX ст., здійснюючи близько 2000 терористичних актів щорічно.

Селективний тероризм розповсюджується на певній території/частині держави. Прикладом може бути діяльність Ірландської республіканської армії (ІРА), внаслідок якої загинуло близько 3000 осіб під час конфлікту в Північній Ірландії (більшість терористичних актів ІРА здійснювала в таких районах як: Белфасті, Лондонферрі та у прикордонні з Ірландською республікою).

Локальний тероризм націлений на невелику територію, або на певному окремому об'єкті/визначена категорія осіб. Але попри обмежену націленість, даний вид тероризму має на меті вплив на більше коло осіб, на яке він намагається залякати власними діями, викликати резонанс, тощо. Як приклад можна назвати серію вибухів в м.Житомир 1998р., які були вчинені проти комерційної фірми з метою усунення конкурента, при цьому інші об'єкти, окрім даної фірми, не постраждали.

Наступна група буде класифікуватися за елементами прояву тероризму, а саме: за мотивами та цілями, засобами та методами, суб'єктами, об'єктами, змістом діяльності та характером наслідків.

За суб'єктами розрізняють:

– Терористичні акти, які вчинені підготовленими особами, що перебувають на державній службі;

– Акти тероризму, здійснені етнічними меншинами;

– Вчинені релігійними фанатиками;

– Терористичні акти визвольних рухів в країнах «третього світу» (наприклад партизанська війна в країнах Латинської Америки).

В.А. Ліпкан [49;50] розрізняє наступні мотиви здійснення актів тероризму: політичні, націоналістичні, релігійні, мотиви помсти, прагнення до самоствердження.

За цілями терористичні акти можна поділити на:

– Підрив – придушення ворога з метою отримання поступок (наприклад звільнення засуджених терористів);

– Провокування до певних дій, або навпаки до бездіяльності з метою зміни

встановленої політики;

– Демонстративність з метою привернення уваги громади до терористичних дій. [81]

На мій погляд, найбільш вдалу класифікацію вказав М.П. Требін в своїй праці «Тероризм у XXI столітті». [84] Вона є досить лаконічною та повною: за сферою дії автор виділяє вже згаданий міжнародний та внутрішньодержавний тероризм; за суб'єктами терористичної діяльності – державний та недержавний, головною відмінністю яких є те, що державний тероризм є відкритим насильством з боку владної еліти, а недержавні угрупування не беруть безпосередньої участі в діяльності державних органів. Наприклад, метою терористичних дій японської секти «Аум Синрікьо» (Вища істина Аум) було повалення діючого уряду і висунення свого «керівника» Секо Асахару імператором Японії. Основною зброєю недержавного тероризму є терористичні акти, а державного – репресії.

Якщо брати саме ідентичність суб'єктів терористичної діяльності як ознаку для класифікації, то Требін виділяє етнічний так релігійний тероризм. Етнічний тероризм має на меті зміну форм державного устрою, становище етнічних утворень та створення самостійної держави. Об'єктами зазвичай становляться державні діячі, чиновники, бізнесмени, тощо.

Релігійний тероризм є досить частим явищем, що виникає внаслідок дискримінації будь-якої релігійної групи. Поділ суспільства за релігійною ознакою зумовлює наявність можливого напряму у взаєминах між людьми та віросповіданням.

За соціально-політичною спрямованістю М.П. Требін [84] виділяє лівий (революційний) та правий (контрреволюційний) тероризм. Лівий тероризм орієнтується на ліві соціально-політичні доктрини (ленінізм, марксизм, анархізм, тощо) та націлений на діячів державної влади, співробітників

органів безпеки, бізнесменів і тд. Правий тероризм ґрунтується на традиційних політичних доктринах і цінностях, а його мішенню зазвичай виступають ліві та ліберальні політики й активісти профспілкового руху. Найактивніші праві терористичні угрупування існували під час революції 1905-1907 рр. в Росії («чорні сотні», Союз Михайла Архангела), в Європі після Другої світової війни у формі неофашистських груп, а в Латинській Америці — ескадронів смерті.

За способом дії на об'єкт тероризм поділяється на інструментальний та демонстративний. Останній привертає увагу до певної проблеми, драматизує її та на має на меті викликати емоційну реакцію у політичних опонентів, які є об'єктами терористичних актів. Такою проблемою може бути, наприклад, захист довкілля.

Інструментальний тероризм ставить психологічний ефект своєї діяльності на другий план. Головною метою є досягнення власної мети та здійснення реальних змін у владних відносинах шляхом нанесення фізичних втрат та жертв.

Наступний поділ за засобами, які використовуються під час терористичних актів. Існують звичайні засоби, наприклад, холодна та вогнепальна зброя, літаки, танки, вибухові пристрої, ракетні установки, і тд; та зброя масового ураження (біологічна, хімічна, ядерна, тощо).

За місцем здійснення терористичних актів розрізняють наземний, морський, повітряний, космічний і комп'ютерний тероризм. [15;22]

Я хочу зупинитися саме на комп'ютерному тероризмі та згадати про тероризм інформаційний. На перший погляд, інформаційний тероризм є не таким небезпечним, на відміну від звичайного. Але насправді, інформаційний тероризм – це не тільки кібер-злочин, а також пропаганда, маніпуляції, викривлення інформації задля налякування населення. Доступність, простота та дешевизна сучасних інформаційних технологій істотно збільшує ризики інформаційного тероризму.

Пропаганда є основним інструментом інформаційного тероризму, що впливає на формування думок та поглядів суспільства. Під пропагандою мається на увазі форма комунікації, яка включає в себе поширення інформації, чуток, та інших даних з метою впливу на суспільну думку, позицію громадян, зміну її стану в інтересах суб'єкта, який саме здійснює дану пропаганду. В широкому значенні, пропаганда є поширенням будь-яких соціально-політичних, природно-наукових та інших знань задля втілення їх в суспільну свідомість.

Ґарт Йовет та Вікторія О'Доннел [104] запропонували своє коротке визначення даного терміну. За їхніми словами, «пропаганда – це навмисні, постійні спроби змінити розуміння, сприйняття, маніпулювати пізнанням та направляти поведінку й дії людей задля досягнення потрібних дій та реакцій, потрібних для самого пропагандиста».

Російський дослідник Д.О. Лучкін вважає, що пропаганда – це спеціальний засіб здійснення політичної комунікації і організації змісту політичного діалогу/дискурсу. Отже, терористичні угрупування ведуть пропаганду тероризму, в першу чергу, через психологічний вплив на суспільство. [9]

Тероризм, який відбувається в інформаційному просторі, можна поділити на:

– Інформаційно-психологічний тероризм, який впливає саме на психологічному рівні (контроль ЗМІ з метою дезинформації, поширення власної могутності, обговорення ідей та намірів терористичних організацій). Його також можна назвати медіа-тероризмом або «медіа-кілерством». Це певне зловживання каналами ЗМІ, онлайн платформами задля здійснення майбутніх терористичних дій та акцій;

– Інформаційно-технічний тероризм (або кібертероризм), який пошкоджує технічні системи та механізми ворогів. Він завдає шкоди технічному середовищу супротивника через руйнування баз даних, систем

зв’язку, і т.д. Кібер-тероризм включає в себе інформаційні атаки на комп’ютери, засоби передачі даних, обчислювальні системи, тощо. Він перехоплює управління систем, перериває обмін інформацією та перехоплює її. Його небезпека полягає в тому, що він не має фізичних меж, а отже може здійснюватися будь-де та з будь-якої точки планети. Кібер-атаки можуть завдати шкоди на локальному, державному та навіть міжнародному рівні.

Т.П. Яцик [91] вважає, що сучасний інформаційний тероризм є множиною інформаційних війн та спецоперацій, пов’язаних зі спецслужбами та транснаціональними кримінальними структурами.

Міжнародні фахівці в сфері боротьби з інформаційними загрозами вважають, що інформаційний тероризм є поєднанням фізичного насильства з одночасним використанням інформаційних систем, а також навмисне зловживання інформаційно-комунікаційними технологіями, мережами та цифровими системами з метою здійснення терористичних актів. Також, інформаційний тероризм визначають як психологічне залякування населення й органів влади з метою досягнення своїх злочинних цілей.

В.О. Коршунов [44] під інформаційним тероризмом розуміє сучасний вид терористичної діяльності, націлений на використання різноманітних методів та інструментів тимчасового або повного виведення з ладу елементів інформаційної інфраструктури держави, що створює небезпечні наслідки для життєдіяльності суспільства в цілому, держави, і окремих осіб. [6]

На думку Леонова Б.Д. та Лихової С.Я., [47] кібертероризм – це атака на певні об’єкти в інформаційному просторі, з метою порушення державної безпеки, залякування суспільства та провокації конфлікту. До кібертероризму автори також включають будь-які політично вмотивовані дії, які створюють серйозну шкоду економічному сектору, наприклад зупинку водопостачання, енергопостачання, тощо.

Стаття 1 Закону України «Про основні засади забезпечення кібербезпеки України» від 2017р. [65] визначає кібертероризм як терористичні дії, реалізовані за допомогою кіберпростору, або в ньому.

В своїй праці «Протидія комп'ютерній злочинності в Україні (системно структурний аналіз) Бутузов В.М. [12] визначив термін кібертероризм наступним чином: «це здійснення комп'ютерних атак, націлені на елементи інформаційної інфраструктури, з метою проникнення в цифрові системи ворога, перехоплення управління комп'ютерами, порушення роботи засобів комп'ютерного та інформаційного обміну, здійснювати інші види деструктивного впливу, що провокує серйозні наслідки.

Кібертероризм має такі головні ознаки: можливість віддаленого доступу, анонімність, дешевизна та доступ до технологій, велике охоплення аудиторії. Дії в інформаційному просторі часто є лише частиною майбутніх терористичних операцій на фізичному полі.

Для кібертероризму характерним є використання комп'ютерних технологій, інших видів девайсів, які мають доступ до мережі Інтернет; об'єкт злочину, що перебуває в інформаційному просторі; орієнтування саме на такі своєрідні об'єкти як локальні та глобальні мережі, комп'ютери, програми, та в особливості – інформація.

Отже, аналіз наукової літератури показав, що тероризм має чотири основні ознаки: по-перше, тероризм включає в себе виконання насильницьких та протиправних дій; тероризм націлений на переважаючих за силою державних меншин; він має власні цілі та мотивацію, політичні погляди, які переслідує; для тероризму є характерним активне залучення великої кількості людей до своїх рядів, та відсутність цінності людського життя.

Тероризм досліджується як явище досліджується під призмою соціальної поведінки, соціально-правової, соціально-психологічної, як різновид злочинної діяльності та тип політичної поведінки. Методологія

аналізу включає в себе визначення самого феномена тероризму, соціального та правового походження, соціально-психологічної направленості.

Специфіка даного аналізу полягає в тому, що існують різноманітні форми, види та прояви тероризму, різні підходи до визначення та аналізу даного явища, що перешкоджає формулюванню, створенню єдиної прийнятої парадигми його розуміння. Тому, з розвитком даного явища тероризму, воно варто уваги та подільшого дослідження. З розвитком цифрових та інформаційно-комунікаційних технологій, тероризм перейшов з фізичного поля в онлайн, тим самим змінилися основні інструменти та методи терористичної діяльності, а інформаційний тероризм сьогодні є вже звичайним явищем. Тому, на сучасному етапі, варто детально досліджувати нові тенденції в розвитку інформаційних інструментів терористичних організацій.

1.2. Терористична організація як головний суб'єкт здійснення терористичної діяльності.

Вивчення особливостей терористичних груп, а також видів терористичної злочинності допоможе в подальшому пошуку ефективних інструментів протидії злочинам та покращенню діяльності держав в сфері безпеки. Такі науковці, як Ліпкан В.А. [39;40;41] , Рустамова Л.Р. [36], Руденко М.М. [41; 49], Лисенко А.М. [48], Іванов С.М. [27], Луцький М.Г. [54] , та інші вивчали особливості терористичних організацій та розглядали окремі аспекти їх діяльності.

Так, А.О. Данилевський вважає, що терміни терористична організація та група потрібно об'єднати з термінами «організована злочинна група» та «злочинна організація», взявши до уваги положення міжнародних нормативно-правових актів. Такої позиції дотримуються й інші науковці, та

на їхню думку варто замінити термін «терористична група» на «організована терористична група».

Деякі вчені погоджуються з даним визначенням, та зазначають : «терористична організація поєднує в собі всі ознаки, характерні для організованих злочинних угрупувань: наявність лідера, чіткий розподіл функцій між членами організації, конспірація, дотримання неформальних норм поведінки, наявність фінансування та грошового фонду підтримки».

Семикін М.В. також визначає, що «терористична організаціє налічує в собі ті ж ознаки, що й організована група, але також включає ще додаткові ознаки, зумовлені особливостями терористичної діяльності». [84]

Згідно з положеннями ст.28 Кримінального кодексу України, однією з найважливіших відмінних характеристик злочинної організації та організованого угрупування від інших видів співучасті є попередня змова/кооперація трьох чи більше осіб (злочинна організація – від п’яти осіб), яка має на меті скоєння злочинів, що потребує попередньої підготовки. З цим погоджуються дослідники Ліпкан В.А., Антипенко В.Ф., та деякі інші, що займаються проблемами визначення тероризму через кримінально-правову призму. [80]

Вчинення певного виду злочину, зокрема створення терористичної організації, можливе лише зі складної взаємодії декількох суб’єктів, адже в формі простої співучасті, створення подібного угрупування неможливе з наступних причин:

– Злочин, здійснений групою осіб, має наступні характеристики: два або більше учасників; відсутність попередньої змови, тобто не відбувалося попереднього обговорення щодо скоєння злочину, його деталей, розподілу ролей, тощо. Тобто, без попередніх домовленостей створити терористичне угрупування неможливо, адже термін «створення» має на увазі здійснення конкретних операцій, в результаті яких була створена терористична група. Також, під цим терміном мається на увазі пошук

суб'єктів, які будуть брати участь в терористичній діяльності, об'єднання їхніх дій, розподіл обов'язків, складання плану, визначення інструментів та порядок дій, що ніяк не може бути здійснено без попередньої змови.

– У статті 2583 Кримінального кодексу України говориться також про «керівництво терористичною організацією». Так, керівництво відрізняється від попередньої змови в першу чергу тим, що керівництво передбачає управління вже створеної групи/організації, контролю над її функціонуванням в період деякого часу і властивий саме організованим угрупуванням, тоді як «змова» має на меті саме домовленість про вчинення злочину, яке може відбутися хоч за хвилину/годину до здійснення цього самого злочину.

Отже, злочин визнається здійсненим терористичною групою, якщо в його організації брала участь група людей з трьох або більше осіб, які мали попередню змову щодо згрупування, розподілу функцій, та всі учасники організації були проінформовані щодо плану здійснення терористичної діяльності.

Терористична діяльність – це протиправна, незаконна діяльність, вчинена задля порушення міжнародної та громадської безпеки/ правопорядку, шляхом насильницького примусу органів державної влади з метою досягнення терористами власних політичних цілей.

Зокрема, ст.1 Закону України «Про боротьбу з тероризмом» [64] , терористична діяльність поряд з іншими видами діянь включає в себе також пропаганду та розповсюдження власної терористичної ідеології. Частина перша даної статті трактує терористичну діяльність як:

– сукупність дій, що поєднують планування, організацію, підготовку та вчинення терористичних актів;

– підбурювання та заохочення до здійснення терористичних дій, і сама участь в цих актах;

– організація незаконних збройних угрупувань;

– поширення ідеології тероризму, пропаганда власних поглядів;

– фінансування тероризму та інші прояви його сприяння, тощо.

В.А. Ліпкан [51] відокремлює внутрішню та зовнішню (в навколишньому світі) діяльність терористичних організацій. Зовнішня діяльність націлена на:

– Державу, сюди можна віднести посягання або загроза посягання на життя і здоров'я: представників посадових органів, вищих посадових осіб та осіб нижчого рангу, лідерів громадських об'єднань, релігійних організацій, партійних рухів; посягання на державні об'єкти, такі як МЗС, підприємства, і т.д.; недержавні об'єкти;

– Певні групи, організації – шляхом посягання на життя та здоров'я її членів (зазвичай, злочинні дії направлені на керівництво організації); посягання на власність організації; на об'єкти, які безпосередньо не належать організації (комунікації, транспорт, і т.д.); посягання на здоров'я та життя людей, які не є членами організації, наприклад випадкові відвідувачі;

– Індивіда шляхом посягання на його життя та здоров'я та його близьких, та на майно, яке є їхньою власністю.

В разі здійснення внутрішньої терористичної діяльності, терористичні групи здійснюють наступне:

– Інформаційно-аналітична діяльність, яка полягає у вивченні інформації про об'єкт тероризму, аналіз маршрутів, розробка плану, поширення інформації щодо захоплення заручників, попередження про теракти, тощо;

– Матеріальна складова підготовки терористичних актів: пошук транспортних засобів, виготовлення необхідних знарядь, купівля техніки, утримання викрадених осіб;

– Контррозвідка та охоронне забезпечення діяльності (охорона баз, утримання заручників, вербування, тощо);

– Набір нових членів організації, їх навчання перепідготовка, ознайомлення зі своїм досвідом;

– Становлення та підтримка зв’язку з іншими терористичними організаціями. [81]

Варто наголосити, що терористична діяльність може бути реалізована не тільки терористичними організаціями, групами, а й окремими злочинцями та бойовиками. Звичайно, в першому випадку, виникає більша соціальна небезпека, адже є можливість здійснення відразу декількох терактів одночасно, або з невеликими проміжками часу в різних місцях, що, відповідно, збільшує число жертв, економічної шкоди та збитків. Отже, терористичні організації мають такі основні ознаки, що дозволяють їм здійснювати велику кількість злочинів: наявність єдиного плану, кооперація, попередня змова та підготовка, розподіл функцій між учасниками.

Так, ряд дослідників зазначають, що тероризм не може існувати без організації своєї діяльності. Також, важливою ознакою, які вирізняють їх від інших, є якісний склад групи. Так, керівники організованих та терористичних організацій, зазвичай, професіонали, які мають достатньо досвіду та отримують дохід зі злочинної діяльності протягом тривалого часу. Вони мають знання та навички щодо організації та здійснення злочинів, володіють спеціальними прийомами та мають високий авторитет в злочинному колі.[81]

Теоретично під загрозою міжнародного тероризму може опинитися будь-яка людина, незалежно від місця її перебування, однак слід зазначити, що рівень такої загрози для країн є неоднаковим. На думку авторів аналітичної доповіді «Актуальні питання протидії тероризму у світі та в Україні» , можна умовно виділити групи країн, за якими спостерігається підвищена активність міжнародних терористичних організацій (передусім джихадистських):

Перша група включає в себе ті країни, на території яких постійно знаходяться лідери та керівництво терористичних організацій, розміщені

їхні осередки, табори, та країни, в яких зацікавлені терористи в тому, чи іншому плані (Афганістан, Ірак, Сирія, Лівія, Нігерія, Камерун, Ємен, Пакистан та інші). [90]

Дані країни характеризуються слабким та неефективним державним правлінням та інституціями, зокрема в сфері оборони та безпеки. Ці та інші негативні чинники провокують те, що терористичні організації здатні контролювати великі території, здійснювати захоплення районів, населених пунктів та крупних об'єктів, та відповідно мати доступ до ресурсів (людських, матеріальних тощо). Діяльність міжнародних терористичних організацій у зазначених регіонах, як і відповідні антитерористичні заходи, несуть загрози життю і здоров'ю не лише громадянам цих країн, а й громадянам інших держав, які перебувають на цій території. Терористична активність у вказаних країнах має такі характерні прояви: [63]

– напади на представників урядових та силових структур (державних та коаліційних), міжнародних гуманітарних місій;

– використання важкої зброї та техніки в районах бойових дій з урядовими та міжнародними силами, застосування безпілотних літальних апаратів, використання цивільного населення як «живого щита»; [81]

– здійснення заходів починаючи з підготовки партизанської війни, до її ведення на звільнених урядовими силами територіях (зокрема, проникнення бойовиків до підконтрольних уряду населених пунктів під виглядом біженців);

– активна діяльність терористів-смертників, особливо в місцях масового скупчення людей, використання при цьому жінок, підлітків та навіть дітей;

– здійснення як показових страт (в тому числі й масових), так і їх інсценування. За результатами терористичної активності такі країни несуть значні людські та матеріальні втрати. Крім того, там зазнають втрат і сили міжнародної антитерористичної коаліції. [48]

Друга група включає в себе країни, які ведуть активну боротьбу з міжнародними терористичними організаціями (США, Канада, Велика Британія, Франція, Туреччина, ФРН, Ізраїль тощо). [81;67]

Метою терористів є вимушення урядів даних країн відмовитися від боротьби з міжнародним тероризмом за межами держави. Такі вимоги, зокрема відбуваються шляхом залякування населення, яке, в свою чергу, тисне на уряди, а також відволікання зусиль спеціальних служб, правоохоронних органів, спеціальних служб, збройних сил і ресурсів держави на подолання наслідків таких терактів та проведення відповідної профілактичної роботи всередині держави.

Для реалізації та досягнення своїх цілей у країнах другої групи, які мають у своєму розпорядженні потужні сили безпеки та оборони, терористи вдаються до таких заходів:

– створення та забезпечення функціонування терористичних осередків у країнах розташування потенційних об’єктів терористичних атак (у т. ч. з числа іммігрантів, найманців тощо);

– активна інформаційно діяльність з використанням пропаганди: психологічне маніпулювання послідовниками терористичної ідеології та саморадикалізованими особами в даних країнах (терористичними організаціями використовуються різні методи впливу, націлені на конкретну аудиторію);

– під час вибору цілі майбутніх терористичних нападів, в першу чергу, перевага надається об’єктам, на яких неможливе постійне забезпечення високого рівня захисту, насамперед, місцям масового скупчення людей: стадіонам, ринкам, ярмаркам, кафе, театрам тощо;

– звернення до своїх послідовників щодо використання найпростіших та дієвих методів, інструментів, способів та засобів здійснення терористичних атак: використання транспортних засобів, холодної зброї,

терористів-смертників тощо. При цьому злочинці використовують також вибухові пристрої та стрілецьку зброю.

Остання, третя група країн – країни, які міжнародні терористичні організації використовують як «транзитні».

Такі країни терористичні організації не розглядають як потенційні цілі, а використовують лише для транзиту, перепочинку, лікування, вербування нових членів – тобто для забезпечення своєї діяльності. До цієї категорії, можна віднести й Україну. Варто зазначити, що факти використання міжнародними терористами транзитного потенціалу нашої держави знаходять підтвердження за результатами діяльності Служби безпеки України.

Аналізуючи діяльність терористичних організацій на міжнародній арені, варто розглянути їхні види та особливості, так американський фахівець з питань тероризму Дж. Мотлі запропонував модель класифікації терористичних організацій, за якою вони поділяються на дві групи: ліві та праві. Ліві групи мають на меті кардинальну зміну існуючого соціального ладу або ж політичної системи використовуючи для цього революційні ідеї. Представниками таких груп можна назвати організацію «Червоні бригади» (Італія), РАФ (ФРН) та подібні, що поширюють свою діяльність майже у всіх регіонах світу. Останнім часом, уряди деяких країн та міжнародне товариство стурбоване діями саме «правих» терористичних груп, в першу чергу фашистської орієнтації в Європі, які мають більш радикальні цілі, як, наприклад, возз’єднання Північної Ірландії з Ірландією, проголошення незалежності від США Пуерто-Ріко тощо. Американські спеціалісті також виділяють третю групу, яка пов’язана з виробництвом, перевезенням та продажом на внутрішньому ринку США наркотиків з країн Латинської Америки, Близького і Середнього Сходу, Південно-Східної Азії. Так званий «наркотероризм» став небезпечною проблемою для міжнародної безпеки, зокрема для індустріально розвинутих країн. [66; 67]

Підсумовуючи вищезгадану інформацію, можна зробити висновок, що організація вважається терористичною, якщо хоча б один із підрозділів займається терористичною діяльністю, та хоча б один із керівників проінформованих щодо цих дій. Терористичні організації є різновидом форм організованої злочинності, що мають схожу структуру, організацію процесів діяльності, механізми реалізації цих процесів. Серед основних відмінностей терористичних груп серед інших видів організованої злочинності варто виокремити їхні мотиви, цілі та мету.

1.3. Соціальні мережі та їх головні особливості

Інформатизація суспільства надзвичайно вплинула на інструменти ведення конфліктів та війн. Сьогодні, інформація є важливим ресурсом та інструментом в руках як організацій, так і державних органів. Соціальні мережі, в свою чергу стали зручним майданчиком для діяльності терористичних організацій, що дають їм увесь інструментарій для реалізації головних завдань та цілей: вербування новобранців, поширення пропаганди, покращення методів фінансування, тощо.

А. Каплан та М. Хенлейн [108] під соціальними медіа розуміють «групу Інтернет-додатків, які базуються на технологічній базі Web 2.0, та дозволяють користувачам створювати контент і обмінюватися ним». Також, до соціальних медіа можна віднести соціальні мережі, геосоціальні сервіси, вікі-сервіси, блоги, тощо. Термін Web 2.0 започаткував Тім О'Рейлі у публікації «What is Web 2.0». В ній він поєднував появу великої кількості онлайн-сайтів, їх спільні принципи роботи, разом зі загальною тенденцією розвитку у Інтернет спільноти, і назвав це явище Web 2.0. Автор визначає його як «спосіб проектування систем, які покращуються зі збільшенням користувачів шляхом обміну та взаємодією між ними. Важливою рисою Web 2.0 є принцип залучення користувачів до створення контенту та багаторазового постійного його використання. [77]

Зокрема, Б. Веллман і С. Берковіц [94] під соціальною мережею розуміють множину членів/користувачів суспільної системи, та зв’язки між ними. На думку . Рафаели, Г. Равида, та В. Сороки [117] соціальні мережі являють собою вагомою часткою віртуального соціального капіталу. Вони стверджують, що «реєстрація та діяльність у соціальних мережах/форумах створюють соціальну систему, всі учасники якої, як активні, так і пасивні одержують соціальний капітал шляхом отримання доступу до потрібної інформації, вивчаючи соціальні норми, та знайомлячись з іншими користувачами». [30]

Б.Я. Вахула [14] вважає, що соціальна мережа – це спеціально створена можливість онлайнової взаємодії з метою створення та обміну інформацією, певної тематичної спрямованості з іншими користувачами; інструментарій соціальних мереж вважається ефективним засобом комунікації через можливість спілкування між користувачами з віддалених точок планети.

Термін «соціальна мережа» застосовують також до опису Інтернет-сервісів, а не тільки тематичних товариств, таких як «Facebook», «LiveJournal», «Twitter», тощо. [28]

В мережі Інтернет існує безліч соціальних мереж, які мають різну характеристику та направленість, їх можна класифікувати за різними ознаками. Перша ознака – доступність, за нею можна виділити відкриті, закриті та змішані соціальні мережі. Сьогодні, майже всі сучасні соціальні мережі є відкритими та доступними для всіх користувачів, за винятком окремих бізнес-платформ, які початково створювалися закритого типу. СМ змішаного типу є досить непопулярними серед користувачів, адже мають на меті досягти такого ж рівня популярності, як і у відкритих СМ, але мають різні бар'єри для учасників, чим їх і бентежать, тому вони неохоче до них приєднуються.

За географічним чинником, соціальні мережі можна поділити на СМ світового значення; окремої країни; певної територіальної одиниці; та без регіональної приналежності.

За спрямуванням можна виділити особисті, професійні та тематичні соціальні мережі. Особисті допомагають підтримати комунікацію з іншими користувачами, а також здійснювати пошук нових. Професійні спрямовані на покращення професійних навичок шляхом розвитку, а також допомагають в побудові кар'єри. Тематичні СМ збирають користувачів за певними інтересами: спорт, музика, хобі, спосіб життя, тощо.

Існує також більш детальна класифікація, яка описує види соціальних мереж наступним чином:

– Соціальні мережі для спілкування, до яких можна віднести «Facebook». Саме вони вперше запровадили створення власного «міні-сайту», який зараз більш відомий як профіль користувача;

– Соціальні мережі для обміну фото та відео контентом: «Instagram», «YouTube».

– Соціальні мережі для колективних переговорів з метою обміну знаннями: «Quora», «Reddit».

– Соціальні мережі, які допомагають поширювати власні думки та авторські дописи, сюди також можна віднести блоги: «Blogger», «Twitter».

– Сервіси, за допомогою яких можна зберігати контент в власних бібліотеках (фото, музика, відео, тощо), та мають можливість підписатися на них іншим користувачам. Це такі соціальні мережі, як: «Pinterest», «Flipboard».

– Соціальні мережі за інтересами, де є можливість знайти однодумців, наприклад – «Goodreads», «Friendster». Зрештою, можна сказати, що класифікації є достатньо умовними, адже на них впливає безліч факторів, а поділ на види та категорії триває по сьогодні. [85]

Варто окремо виділити блоги, в особливості Twitter, адже саме вони грають важливу роль у формуванні громадської думки. Важливе визнання блогів та діяльності блогерів у висвітлені світових подій відбулося після рішення низки провідних інформаційних агенцій щодо цитування та посилання на блоги як джерело інформації. Так, агенція Associated Press (AP) доповнила правила щодо цитування, тепер у своїх новинах вони мають можливість посилатися на блоги, якщо ті є першоджерелом інформації. Раніше, посилання були лише на друковані ЗМІ, веб-сайти та телерадіокомпанії. [30]

Сьогодні блогосфера являється альтернативним інформаційним та новинним простором, який на ряду з професійними ЗМІ надають інформаторам завантажувати останні новини, фото та відео. Такі проекти вже є у CNN, the Guardian, Aftonbladet (популярна шведська газета), а BBC відкрили окремий відділ, який займається пошуком, аналізом та перевіркою цікавого контенту в соціальних мережах. Подібні відділити також існують і в інших провідних виданнях західних країн.

Соціальні мережі виконують всі головні функції, які властиві засобам масової комунікації: інформативна функція, регуляторна та культурологічна.

Під інформативною функцією розуміється надання користувачам актуальної інформації щодо різних сфер діяльності людини: політичної, ділової, медичної, науково-технічної, і т.д.

Регуляторна функція полягає в певному впливі на аудиторію, від встановлення певних видів контактів до контроля над суспільством. Масова комунікація впливає на суспільну свідомість особистості та групи, на формування громадської думки та створення соціальних стереотипів. Під цією функцією також може бути прихована можливість маніпулювати й управляти суспільною свідомістю, фактично здійснювати соціальний контроль.

Культурологічна функція, в свою чергу сприяє усвідомленню та розумінню суспільством важливості та необхідності в збереженні культурних традицій. [29]

Згідно з дослідженням Factum Group Ukraine, станом на грудень 2019 р. загальна кількість користувачів мережею Інтернет в Україні складала 71% (тобто 22,96 млн), а 65% мають інтернет вдома. Відбулося збільшення на 7%, і однією з причин є «смартфонізація» населення, адже приблизно 22% аудиторії користуються інтернетом лише за допомогою смартфонів. Найактивнішими користувачами виявилися українці віком від 15 до 24 років - серед них частка користувачів інтернетом становить 97%, люди віком від 25 до 34 років - становлять 96%, віком від 65 років - уже 29% користувачів (в 2018 році було лише 14%). [42]

В контексті інформаційного тероризму, можна виділити головні соціальні мережі, та мету їх використання терористами. Так, наприклад, Facebook не часто використовується для прямого найму й вербування новобранців, адже він має певні механізми відстеження і може визначити як місцеположення користувача, так і конкретний час поширення повідомлення. Натомість, ця СМ частіше використовується саме як децентралізований центр поширення інформації, фото та відео-контенту, або як спосіб пошуку прибічників, однодумців й поширення власної ідеології.

Twitter, як й інші мікроблоги, дає більше переваг для терористичних груп, адже можливість відстеження повідомлень та джерело твітів дещо нижча, що збільшує комунікаційні дії терористів. В своїх твітах, терористи, зазвичай, намагаються взаємодіяти з владою тієї чи іншої держави, або опозицією, в інформаційних зіткненнях, які мобілізують обидві сторони. Також Twitter використовується для поширення провокацій, або намірів терористів.

Крім того, ТО можуть з легкістю коментувати чужий контент, пов'язаний з міжнародними подіями, або інформацію про політиків,

особистостей кількома мовами, таким чином бути активним користувачем та завжди залишатися в центрі подій під час розгортання своїх кампаній.

Популярною платформою серед терористів також є YouTube, що є найліапшим майданчиком для поширення екстремістських відео, незважаючи на посилення конкуренції з боку інших СМ, таких як Dailymotion, Vimeo тощо. Його перевагою, окрім поширення відео, можливості їх коментування та створення каналів, також є можливість поширення відео окремим користувачам, створення спеціальних посилань, через які можна переглянути обмежений контент. Трьома основними причинами створення відеоповідомлень терористами є: звеличення своїх лідерів та мучеників, які служили заради єдиної мети; пропаганда терактів та смертників; та загальна пропаганда своєї ідеології.

Отже, можна зробити висновок, що інформатизація населення, збільшення кількості та якості новітніх технологій та легкий доступ до мережі Інтернет зробили соціальні мережі активним та популярним майданчик для «онлайн-життя» громадян, де є можливість знайти, аналізувати, обговорити певну інформацію; згрупуватися задля вирішення певних питань та проблем, організовувати заходи, знайти людей зі схожими інтересами. Через популяризацію та соціалізацію онлайн мереж, варто обов’язково звертати увагу на їх використання терористичними організаціями, адже саме їхня доступність, відкритість та зручність дає змогу здійснювати незаконні діяння в онлайн просторі.

В СМ є слабкі місця, якими й користуються терористи, та саме на них в першу чергу варто звертати увагу при дослідженні інформаційної безпеки.

РОЗДІЛ 2. ПРАКТИЧНИЙ ДОСВІД ВИКОРИСТАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ ТЕРОРИСТИЧНИМИ ОРГАНІЗАЦІЯМИ.

2.1 Загальна практика і методи використання інформаційних технологій та соціальних мереж терористичними групами.

Соціальні мережі є зручним засобом комунікації, завдяки своїй доступності, дешевизні та простоті. Поряд з позитивними якостями, СМ також мають негативні сторони, якими й користуються терористичні організації, до них можна віднести: створення та ведення необмеженої кількості сторінок користувача, можливість надання неправдивої інформації, створення закритих груп по різним тематикам та інтересам, тощо. Все це дійсно приваблює терористів, в порівнянні з використанням звичайних сайтів. СМ дозволяють напряму взаємодіяти з аудиторією, та підтримувати спілкування, в той час як на сайтах та інших платформах потрібно чекати на читачів та використовувати додаткові інструменти для їх приваблення. В

соціальних мережах є також зручні функції, які дозволять покращувати соціальну взаємодію: можливість коментування контенту, здійснення приватних листувань, поширення чужого контенту, а також нова функція, що дозволяє перекладати іншомовну інформацію на зручну для читача мову, що прибирає мовні бар'єри.

Також, великою перевагою є те, що в соціальних мережах аудиторія набагато більша, ніж в інших видах медіа. Так, наприклад, станом на 2019 рік кількість читачів BBC становила 426 млн, а в Facebook – майже 2,5 млрд. користувачів, що в рази перевищує свого онлайнового «конкурента». [1]

В соціальних мережах існують корисні інструменти, які допомагають в залученні аудиторії, що є також важливим для терористичних угрупувань. Тут можна виділити можливість залучення через вірусний фото, відео контент, фільтрування інформації по інтересам, контекстна реклама, тощо.

Завдяки подіям, що відбувалися в арабських країнах, які називають «арабською весною», ЗМІ перестали бути звичайним інструментом для обміну фотографіями та повідомленнями з друзями, а стали справжнім майданчиком для кооперації громадян та «зустрічей революціонерів». Через групи в Facebook, активісти стали писати про мирні протести, заохочуючи до участі в них. СМ відіграють важливу роль в інтеграції та кооперації населення, вони дозволяють висловлювати особисті погляди та цінності, й є не просто інтструментом для розваг. Також, в мережі з'являються політичні партії, релігійні групи, а використання блогів, веб-сайтів та онлайн-комунікацій перенесли частину політичної дискусії в мережу Інтернет.

Варто окремо згадати про таку особливість СМ, як таргетинг, це показ та націлення контенту на конкретну цільову аудиторію, залежно від обраних параметрів. Facebook, наприклад, має приблизно 29 тисяч характеристик для тергетингу аудиторії. Дана функція дозволяє терористичному контенту бути сфокусованим на аудиторії, а не перебувати «засекреченим» з ціллю уникнення раптового блокування, і з іншої сторони, такий контент перебуває

у великому масиві інформації, що дозволяє йому там перебувати більшу кількість часу, ніж на інший онлайн-майданчиках.

Таргетинг також дозволяє аналізувати та вивчати свою аудиторію. На власних ресурсах, терористичні угрупування повинні діяти «наосліп» та поширювати «універсальну» інформацію, соціальні мережі в свою чергу, дозволяють проаналізувати користувачів по статі, віку, місця проживання та дізнатися популярні тренди в спілкуванні між окремими групами, що дає можливість поширювати власну пропаганду більш ефективно. Таким механізмом й користувались терористи в 2013 році під час поширення ідеї джихаду. [1]

Так, наприклад в Snapchat терористи використовують короткі відео-звернення, або вірусний контент, щоб привернути увагу користувачів; створюють фейкові акаунти відомих співаків, блогерів, акторів, які мають високий вплив на молодь, або ж використовують оригінальні сторінки для популяризації власного контенту. Наприклад, коментуючи першим новий допис, твій коментар побачать усі наступні читачі. Взагалі, пропагандистські матеріали – це основа онлайн-діяльності терористів. Часто, вона може бути «позитивною» в очах глядачів, та не містити негативного посилу. Так, на платформі Youtube, терористи поширюють відео-звернення з їх визнанням відповідальності за терористичні атаки, але без зображення будь-який проявів насильства.

Терористичні організації також використовують соціальні мережі з навчально-освітньою метою, поширюючи спеціальні інструкції, плані дій; інформацію щодо виготовлення вибухівок та інших пристроїв; правила поведінки зі зброєю; організаційна інформація, тощо. Часто, така інформація потрапляє до рук звичайних користувачів, що може призвести до трагічних наслідків, як, наприклад ситуації, що траплялися в Сполучених Штатах, коли радикалізована молодь реалізувала масові обстріли в громадських місцях.

Деякі організації не закінчують свою діяльність на публікації онлайн-контенту в соціальних мережах, а навіть випускають власні онлайн-журнали, де розповідають основну інформацію про угрупування: мета, цілі, завдання; ознайомлюють читачів зі своїми «наставниками», беруть інтерв'ю та інформують про шляхи приєднання, і т.д.

Потрібно також виокремити тенденцію терористичних організацій щодо використання зовсім нових соціальних мереж, які швидко розвиваються та отримують свою популярність. Причиною цьому є ще не вдосконалена, або взагалі майже відсутня політика боротьби з тероризмом. Вдалим прикладом є вже згадана платформа Snapchat, який в перші місяці роботи взагалі не мав власного визначення терміну «тероризм». Такі майданчики, переважно, використовують в короткий період часу, доки мережа не створить надійний механізм виявлення терористичного контенту. Через деякий час, кількість такого контенту зменшується.

Терористи теж використовують дефекти в алгоритмах соціальних мереж. Так, тривалий період часу на Youtube були доступні до перегляду образливі та жорстокі відео-матеріали, які не тільки мали змогу поширюватися й популяризуватися, а й іноді – монетизувалися. [1]

Завдяки соціальним мережам, терористи також здійснюють рекрутинг. Інформаційні відділи терористичних угрупувань завжди активно шукають нових потенційних членів, які охоче б приєдналися до їх організації, а можливість долучатися до будь-яких онлайн-спільнот, спілкуватися з іншими користувачами дозволяють терористам легко взаємодіяти з аудиторією, що робить СМ зручною платформою для вербування нових членів. З розвитком різних функцій соціальних мереж, також сформувалися й нові способи залучення нових учасників до терористичних організацій. До цих дій можна віднести: запит в друзі, підписки на інших користувачів, подальше приватне листування в таких мережах як Facebook, Twitter і WhatsApp. Вербування

здійснюється шляхом укріплення соціальних зв'язків та подальшої радикалізації вразливих груп.

Можна також згадати про важливий спосіб поширення незаконної інформації, яким користуються терористи – це редагування контенту. Тобто, після створення нейтрального допису, його поширення та популяризації, зміст повідомлення редагують, і таким чином терористичний контент потрапляє в тренди. Іншим варіантом є включення посилань на власні групи та сторінки поміж звичайного тексту повідомлень. На жаль, прослідкувати такий вид порушення досить складно, а кількість користувачів, які потрапляють в «терористичні сітки» в такий спосіб – надзвичайно велика.

Інший вид інформації, яку створюють та поширюють терористичні організації – їхні вимоги, залякування та інформування про майбутні можливі атаки. При вчасному реагуванню органами безпеки, низку терактів можна було б уникнути. Одним з перших поширень такої інформації можна назвати повідомлення від 12 травня 2012 року в Twitter, де ісламістські екстремісти закликали членів своїх груп до активних дій та додавали посилання на свої веб-сайти. Даний допис був способом координації терористів і організація майбутніх терактів.

Схожа ситуація сталася в 2013 році, коли член організації Хезболла опублікував відео відразу в трьох соціальних мережах: Facebook, YouTube та Twitter, де демонстрував тренування озброєних терористів та розповідав про їхні майбутні плани. Подібна тактика була також в Аль-Каїди, Хамасу. Метою була не сама пропаганда, а намагання донести до уряду власні вимоги без втрати ресурсів з боку терористів.

Такий спосіб поширення забороненого контенту, спілкування в онлайн-просторі набагато зручніший, ніж використання телефонних дзвінків та повідомлень, адже технічно їх дуже просто моніторити та вчасно призупиняти. Одним з найпопулярніших месенджерів для координації та спілкування терористів є Телеграм. Він не має потрібних інструментів

моніторингу контенту, методів безпеки, та дозволяє зберігати зашифрований характер листування навіть у відкритих групах до 5000 осіб, та публічних каналах до 200 тисяч підписників.

Члени організації Хезболла в період 2013-2015 років здійснювали свою координацію через платформу Twitter, яка дозволяє здійснювати обмін повідомленнями в режимі реального часу. Це дозволило миттєво змінювати та повідомляти членів групи про нові плані здійснення терактів та лишало можливості органів правопорядку вчасно реагувати на дані зміни. Незважаючи на постійні покращення системи безпеки в онлайновому просторі, оновлення політики безпеки Twitter, терористи досі користуються даною платформою для комунікації та кооперації. [1;124]

В контексті вивчення соціальних мереж в руках терористичних організацій, варто обов'язково згадати сайт 8chan, що також відомий як "Infinity chan" («Нескінченний канал», адже перший символ в назві символізує безкінечність). Це така собі «дошка оголошень», де кожен з користувачів може вільно розміщувати будь-який контент, а що саме важливе – повністю анонімно. [70] Анонімний форум був створений в 2013 році Фредеріком Бреннаном, який задумав формування простору без цензури – абсолютно вільну територію, де кожен міг анонімно висловити свою думку, обговорювати з іншими користувачами трендові теми та їхні повідомлення не мали б аналізуватися та модеруватися адміністраторами сайту. [32]

В рейтингу компанії Alexa, 8chan займав (на момент роботи) 4526 місце у світі за відвідуваністю, а за добу на нього заходили десятки тисяч користувачів. Найпопулярніша група тем для обговорення на цьому сайті називається "/pol/", вона присвячена саме "політично некоректним" темам.

Перший терористичний маніфест «Велике заміщення» (The Great Replacement) з'явився в березні 2019 року. Його автором був стрілець Брентон Таррант, який через кілька хвилин після публікації маніфесту здійснив вбивство 51 людини в мечетях Аль-Нур і Лінвуд Масджид в Новій

Зеландії. Він також вів пряму трансляцію з мечеті Аль-Нур в мережі Facebook, прикріпивши до голови камеру та подавав усе, що відбувається онлайн.

Згодом, в квітні 2019 року на сайті 8chan з'явився ще один маніфест від автора Джона Ернеста, який зібрався здійснити обстріл у синагозі в Каліфорнії. Останній маніфест— «незручна правда» (The Inconvenient Truth) був в серпні цього ж року 21-річного Патріка Крузіса, який здійснив стрілянину в американському Ель-Пасо після публікації маніфесту, внаслідок чого загинуло близько 20 людей. [32]

Приблизно через добу сайт став недоступним для користувачів, а сам засновник був дуже пригнічений ситуацією, яка склалася з його «творінням». Фредерік Бренан в газеті New York Times сказав, що це дуже сумно, але сайт варто заблокувати. Все ж, робота 8chan повністю не закінчилась, один з адміністраторів сайту озвучив, що він працює над розширенням доступу до сайту в тіньовому сегменті мережі Інтернет – «даркнет». [70]

Користувачі 8chan заявляють, що спроси заблокувати даний ресурс призведуть до децентралізації цього сегменту інтернету. Кроки в даному напрямку вже робить соціальна мережа під назвою Gab. Вона називає себе платформою, що зберігає свободу слова, та є досить популярною серед радикальних користувачів, сторінки яких вже стали недоступними в мережах Twitter та Facebook. Плюс до того, компанія надала код сайту у відкритий доступ, тому кожен може створити власну версію Gab.

Інформація в подібних сервісах не зберігається на серверах, а розподіляється між комп'ютерами користувачів, тому чисто теоретично, повідомлення в таких мережах не можуть бути видалені ні адміністраторами, ні правоохоронними органами. [70]

Тож, враховуючи популярність, широке використання соціальних мереж по всьому світу, ТО також стали націлюватися на використання даних інструментів в своїй діяльності, тим самим ще більш ефективно поширювати

свою пропаганду та реалізовувати свої цілі. Такий вибір методів, як СМ, дає терористам ряд важливих переваг, поряд з традиційними видами інструментів вербування. Вони можуть охопити набагато ширше коло користувачів, оскільки СМ надають вільний доступ до інформації, можливість контролювати доступ до контенту, яким ви ділитеся та легко спілкуватися з іншими користувачами.

Швидке охоплення інформаційного простору терористами є підставою до подальшого вивчення цієї проблеми, а головне – на основі моніторингу соціальних мереж створення ефективної політики безпеки в інформаційному просторі.

2.2. Особливості діяльності окремих терористичних організацій в онлайн просторі.

За оцінками міжнародних організацій, національних урядів, спецслужб, неурядових організацій та незалежних фахівців наразі найбільшу терористичну загрозу у світі становлять ісламістські або джихадистські організації та групи. Більшість терористичних актів пов’язано саме з активністю таких угруповань. До джихадистського руху належить велика кількість організацій та груп. Вони присягають на вірність більш потужним групам, взаємодіють, змінюють назви, конкурують, відокремлюються одна від одної тощо. Для таких організацій спільним є прагнення знищення світської влади, встановлення халіфату, панування законів шаріату, викорінення західних стандартів демократії, освіти тощо.

Усі терористичні організації мають спільні головні цілі, які вони реалізують використовуючи СМ, але дещо в їхній діяльності все ж відрізняється, наприклад початкова мета, ідеологія, вид кооперації членів

організації, тощо. Всі ці відмінності й вказують на подальшу тенденцію використання СМ, особливості вибору інструментарію та поведінки, тож варто розглянути різні ТО для більш широкого розуміння особливостей діяльності терористів в інформаційному просторі.

– Ісламська держава

Наразі найбільшу глобальну загрозу становить міжнародна терористична організація «Ісламська держава» (раніше – Ісламська держава Іраку та Леванту ІДІЛ або ДАІШ). Це угруповання діє як квазідержава переважно на території Сирії та Іраку, частково контролюючи території «сунітського трикутника». Проте за результатами військових операцій урядових та коаліційних сил організація поступово втрачає контроль над захопленими територіями та населеними пунктами.

Організація має важку зброю, веде активну екстремістську діяльність та бере відповідальність за велику кількість вчинених у всьому світі терористичних актів. Однією з особливостей діяльності ІД є активне вербування до своїх лав іноземців. ІД визнана терористичною організацією Радою Безпеки ООН, Європейським союзом, а також низкою окремих країн. У березні 2015 р. на вірність ІД присягнула організація «Боко Харам». Організація виникла у 2002 р. та діє на території Нігерії, півночі Камеруну, Нігеру та Чаду. Своїм завданням визначає запровадження в Нігерії шаріату та викорінення «західного способу життя», включаючи політичний, соціальний, освітній аспекти. [102;118]

Терористична організація Ісламська держава (далі ІД), або ІДІЛ (Ісламська держава Іраку і Леванту) втілює свої дій в багатьох вимірах та фронтах, в тому числі цифровому. Діяльність в інформаційному просторі вважається такою самою важливою, як і фізичні теракти. Угрупування часто прославляє своїх «медіа героїв», які пожертвували своїм життям заради створення контенту. Як й інші організації, Ісламська держава активно вводить онлайнові майданчики для кооперації членів, їхньої комунікації та

вербуванню нових людей. Головним інструментом терористів онлайн є, звичайно, пропаганда. Будучи переможеними ще в 2019 році в Сирії, бойовики продовжують набирати лави терористів онлайн, з допомогою пропагандистських відео.

Ісламська держава досить рано збагнула всю силу онлайн-медіа, та з розвитком своєї пропаганди, організація перевершила Аль-Каїду в своїх «онлайн-здобутках», активно вивчавши та користувавшись цифровим технологіями. ІД використовувала максимально різноманітні майданчики: Facebook та Twitter, месенджери Telegram та Surespot та інструменти з поширення контенту, такі як JustPaste.it.

Сьогодні, Ісламська держава – це повноцінна медіа-група, яка створює, аналізує та поширює власний контент. Згідно з «Документуванням віртуального халіфату» (звіт Фонду К'юлліам, від жовтня 2015), ІД поширювала 38 різнотипних повідомлень кожного дня: відео, повнометражні документальні фільми, фоторепортажі, брошури, аудіокліпи, тощо. Організацією використовуються вже перевірені інструменти залучення аудиторії, які можна порівняти з діяльністю маркетингових фірм, які шукають та аналізують свою цільову аудиторію. Один з таких методів – це створення спеціального контенту для нішевих груп. Не завжди контент націлений на показ садизму та жорстоких матеріалів, часто розповсюджують метаріали зі зображенням економічного розвитку всередині організації, гарних взаємин, громадських робіт та своїх перемог, які мають на меті показати та підтвердити основний месидж ІД – процвітання та стабільність організації. На відміну від Аль-Каїди, Ісламська держава веде більш відкриту пропаганду, яка дозволяє залучити більше прихильників.[30]

Кожна провінція, або віліят, має свій окремий медіа-офіс з режисерами, операторами, які працюють з потоковим локальним контентом по всім регіонам. В листопаді 2019 року, колишній оператор ІД розповів, що отримував $700 на місяць, що всемеро більше, ніж зарплата звичайного

бійця-джихадиста. Існували також спеціальні «медіа-точки», які були під управлінням офісів, це такі собі кіоски, або вагончики, які поширювали мешканцям завойованих міст матеріали на компактних носіях інформації (USB-флешках або SD-картах). Оскільки ІД суворо обмежує доступ до мережі Інтернет на захоплених територіях, її фото, відео контент став майже єдиним видом доступної онлайн інформації в регіоні.

Для більш переконливої пропаганди, терористи використовують історії звичайних бійців, на відміну від Аль-Каїди, яка, зазвичай, поширювала розповіді про топ-фігур, як Завахірі. Це дозволяло їм бути «ближчими» до майбутніх членів своєї групи.

Медіа-стратегія також дотримується політики прозорості. Якщо раніше угрупування джихадистів створювали лише закриті арабомовні групи та форуми, то сьогодні ІД навпаки зазиває прихильників використовувати відкриті соціальні платформи для збільшення популярності, йдучи на ризики. Така відкритість робить помітними дії терористів в цифровому просторі, та притягує увагу правоохоронних органів, але переваги такої стратегії значно перевищують наявні недоліки. [57]

Тому, відкритість соціальних мереж привернула багато уваги терористів, які намагаються покращити свою онлайн-стратегію та розвиток в цифровому світі. Бойовики, зазвичай, «працюють» в групах Telegram, Twitter, WhatsApp, а також висвітлюють контент на власних YouTube-каналах чи ЗМІ. Вони створюють контент в залежності від вподобань конкретної аудиторії, потім починають спілкування, втираються в довіру та починають свою пропагандистську «кампанію». Тим, хто шукає додатковий заробіток, вони обіцяють хорошу щомісячну зарплату, гарних друзів та дружній табір членів ІДІЛ, де всі стають однією родиною. Використовуються й емоційно-психологічні маніпуляції, не тільки на хлопцях, а й на дівчатах. Якщо жертва вірить даним маніпуляціям та погоджується, організація надсилає їй кошти для подорожі в один із таборів поблизу кордонів Сирії та Іраку. Під час

пандемії, коли подорожувати було складно, кількість «мандрівників» до табору зменшилась, але все ж вони залишалися їхніми прихильниками онлайн, що теж є важливим для подальшого поширення своїх ідей та пропаганди. Все ж таки, кордон з Іраком досить довгий, та є фактично пустелею, тому пройти непоміченим можливість є, чим деякі й скористалися. Показуючи також свою «турботу» до членів організації, ІД публікувала на своїх сторінках поради щодо збереження здоров'я під час пандемії, не забуваючи нагадати про те, що їх врятує лише віра в Алаха. [26]

Попри вже згаданий сайт 8chan, популярною СМ в діяльності ІДІЛ став Telegram, після введення функції «каналу», яка дає можливість трансляції відео необмеженій кількості читачів. Звичайно, активні дії терористів не залишилися без уваги і офіційні канали з часом були всі заблоковані, а в 2015 році після терактів в Парижі, засновник Telegram Павло Дуров почав видаляти також чат-боти, створені ІД та інші публічні канали. Звіти оновлюються шодня, та до цієї боротьби приєднався Facebook, видаляючи пропагандистські ролики, що знаходяться у вільному доступі та записані англійською й арабською мовами. [26]

Але медіа спеціалісти ІД активно почали створювати нові канали, які повторювали весь контент з офіційних. Агентство Nashir News, в компетенцію якого входять дзеркальні канали, закликало своїх послідовників поширювати інформацію через інші СМ, також агентство створювало профілі в Instagram та почало розміщувати контент арабською та англійською мовами. Експерт з Міжнародного центру з вивчення радикалізації та політичного насилля Чарлі Вінтер признає успішну пропаганду, яку здійснила ІД в Telegram, та зазначає, що контртерористичні дії служби обміну повідомленнями виявилися безсистемними та дещо неефективними. [58]

Також, медіа-центр ІДІЛ «Аль-Хаят» створила рубрику під назвою «Вустами ворога», яка цитує американських політиків та показує всі

актуальні події в світі, використовуючи Твіттер, поширюючи також свої організаційні цілі та ідеї. [72]

В цифровому просторі, ІД не лише використовує готові майданчики для власних цілей, а й створює свої окремі програми та мобільні додатки. Так, ІД створила мобільний додаток для Android, який навчає арабському алфавіту, де біля кожної букви зображений малюнок з відповідною асоціацією, але вже з «терористичними мотивами», наприклад: літера «дааль» асоціюється з арабським словом «дабаба» (що означає танк), літера «сад» з «сарух» (ракета), і т.д. Даний додаток можна знайти тільки в приватних групах ісламістів, і він недоступний для завантаження на офіційних платформах типу Google store. Також існує безліч інших додатків, наприклад, радіо «Аль-Баян», яке транслює пропаганду ІД. [37]

Проаналізувавши використані СМ Ісламською державою, можна зробити короткий висновок: прихильники ІД використовують Facebook для обміну контентом та новинами, наприклад поширюють посилання на відео з YouTube серед своєї аудиторії; Twitter – ще одна популярна соціальна мережа для створення облікових записів терористів, де вони, зазвичай, спілкуються, проводять кооперацію з потенційними новобранцями та поширюють всі види контенту; YouTube також використовується для розміщення відео, як на офіційних сторінках ІД, так і відео, створені самими користувачами. Користувачі діляться посиланнями на відео-матеріали на своїх власних акаунтах в інших вже згаданих СМ; люди, які планують поїхати до таборів ІД та долучитися до їх діяльності, іноді використовують платформу Ask.fm, де можна задавати будь-які питання, наприклад: рівень життя джихадистів, про вербування, подорож до осередків, більш детально про ідеологію та головні аспекти/закони, бойові дії, тощо; бойовики та прихильники ІД використовують Instagram, щоб ділитися фотосетами, які часто створюють різні медіа-організації ІД. Вони також використовують Instagram, щоб поширювати фотографії свого життя в осередках, часто

показуючи гарні пейзажі та зображення, які свідчать про те, що вони живуть повним і щасливим життям; Tumblr, сайт для ведення блогів, використовується бійцями для просування власних аргументів щодо безпеки та важливості подорожі до таборів організації. Tumblr користується популярністю серед жінок-прихильниць ІД, які пишуть блоги, присвячені занепокоєнням дівчат щодо подорожей до регіону, наприклад, залишення сімей та особливостей стандартів життя/права жінок, і т.д.; важливим майданчиком для спілкування з новобранцями є різного роду месенджери, такі як WhatsApp, Kik, SureSpot і Viber, Telegram. Такі мережі використовуються, зазвичай, на етапі подорожі до осередків, коли відбувається надання конфіденційної інформації: маршрути, речі, які потрібно брати з собою, контакти особи, яка буде зустрічати, або саме місце зустрічі, тощо. [105]

Також, терористи ІД подбали про збереження всіх своїх наробіток та створили «резервні копії» всього контенту організації онлайн. Після витіснення Демократичними силами Сирії ІД з Ель-Багуза, та вбивства лідера Абу Бакра аль-Багдаді американськими спецслужбами в жовтні 2019 року, ІД архів даних, розташований в хмарному сховищі. Він складається в більш ніж чотирьох тисяч папок, починаючи від «Авіалінії Аль-Каїди» до «Сумка моджахеда». Тут вони зберігають усі інструкції, інформацію та плани щодо виготовлення зброї, навчання новачків, та навіть шкільну програму для молодших, за якою вчилися діти членів ІД. [81]

Саме в жовтні 2019 року заступник директора аналітичного центру боротьби з екстремізмом «Інститут стратегічного діалогу» Мустафа Аяд замітив дивні посилання, які залишали члени та прихильники ІД в своїх акаунтах Twitter. Перейшовши по посиланню, Аяд потрапив власне до архіву з ретельно класифікованим та розподіленим контентом. Спочатку, він нагадував безліч файлів з DropBox, але величезним по розміру. Папки містили близько півтора терабайта тектової інформації, та фото/відео

контенту, презентації в PowerPoint на різних мовах світу: арабською, англійською, французькою, німецькою, російською, іспанською, бенгальською, турецькою, і навіть пушту. Велика частка файлів відображала щоденне життя Ісламської держави, в одній з папок зберігалася шкільна програма, яка включала в себе 6 предметів: арабську мову, англійську мову, фізичне виховання, кораністику, історію та географію, а також предмет із назвою «ідеологія».

Поміж інших файлів було знайдено звіти про здійснені теракти, поразки та успіхи, а також майбутні плани та їх організаційні моменти. Ряд презентацій під назвою «Авіалінії Аль-Каїди» розповідали про етапи викрадення літаків, а до папки «Сумка моджахеда» входили матеріали про створення хімічної, травматичної, холодної зброї, тощо; аспекти здійснення терактів в різних регіонах. Вже в листопаді американські та британські правоохоронці були проінформовані щодо архіву, але він досі існує та розширюється. Мустафа Аяд зі своїми колегами дізналися, що доступ до архіву можна одержати шляхом використання бота в Telegram. Після приєднання до бота, в нового користувача запитують, чи необхідний йому доступ до файлів, якщо так, він формує посилання на матеріали в хмарному сховищі. Перевіряючи ці посилання, дослідники виявили, хто і яким чином розповсюджує терористичний контент ІД та зробили висновок, що зазвичай такі посилання вказують в інформації про профіль (шапка профілю), або ж вставлять її в різні фото та зображення. Такі акаунти, які у відкритий спосіб поширюють пропагандистський контент, працюють близько доби, а після модерації контенту, адміністраторі просто блокують подібні сторінки, та терористів це не зупиняє, і вони створюють велику кількість нових акаунтів, або викрадають чужі. В Facebook, пропаганда ІД розповсюджується через невеликі групи, що також використовують викрадені сторінки користувачів. [82]

Архівовані файли зберігаються за допомогою програмного забезпечення Nextcloud, яке можна встановити на приватні сервери. Воно також є безкоштовним та дає змогу здійснювати синхронізацію матеріалів з уникненням будь-якого контролю та централізованого хостингу. Цим програмним забезпеченням користується безліч людей, як політики, так і активісти, але програма потрапила також в руки терористів, і завдяки своїй доступності та відсутності контролю являється дуже популярною серед них. Компанія-розробник Nextcloud не несе відповідальності за збережений контент, тому, окрім ІД, сервісом компанії також користуються «Аль-Каїда» та група сомалійських ісламістів «Харакат аш-Шабаб».

Поряд зі сторінками в соціальних мережах, закритими групами та каналами в месенджерах, існують також окремі сайти, як наприклад «Netflix для джихадистів», який транслює жорстокий терористичний контент. На іншому сайті, Muslim News, концентрується весь офіційний контент: актуальні новини та повідомлення, виступи та промови лідерів, їхні звернення, тощо. [82]

Ісламська держава досить активно позиціонує себе в онлайн просторі, та користується всіма перевагами цифрових технологій, використовуючи їх в своїх цілях. Попри свою надмірну відкритість, організація ефективно створює та поширює контент, створюючи нові профілі й акаунти в соціальних мережах, та не даючи правоохоронним органам повністю «закрити» доступ до їхньої діяльності в мережі Інтернет.

– Талібан

Для багатьох видається дивним той факт, що терористична організація Талібан, яка колись наклала повну заборону та цензуру щодо будь-яких видів розваг, сьогодні є активним користувачем соціальних мереж та онлайн платформ, з метою збільшити власний вплив.

Дослідник аналітичного центру Королівського інституту об'єднаних служб з питань оборони та безпеки Рафаело Пантуччі в інтерв'ю видання Vice заявив, що сучасні методи талібів в мережі Інтернет розвиваються та покращуються. Вони оволоділи мистецтвом піару, та вдало просувають свої ідеї в соціальних мережах, зокрема публікують контент в Twitter, Facebook та спілкуються, поширюючи повідомлення в месенджері WhatsApp. Варто звернути увагу на те, що месенджер WhatsApp шифрує повідомлення користувачів, впевнюючи їх в безпеці обміну інформацією, тим самим ускладнюючи роботу модераторів, адміністраторів та військових в перехоплені незаконної інформації та попереджені протиправної діяльності онлайн. Тому, таліби користуються даним месенджером з метою кооперації бойовиків, нових найманців зі своїми керівниками, підтримуючи постійний зв'язок. Діяльність не обмежується єдиними месенджерами, за словами виконавчого директора Intel Group (організація, що займається аналізом та відстежує онлайн-діяльність джихадистських організацій) Ріти Кац, Талібан активно піарить власну організацію та ідеологію на міжнародній арені, використовуючи завчасно підготовлену пропаганду. Вони активно використовують цифрові технології, щоб показати всьому світу свої зміни, наміри та покращують імідж, поширюючи лже обіцянки.

Експерти зазначають, що таліби вже понад 10 років активно використовують соціальні мережі, а також власний сайт «Голос джихаду», а в 2019 році представник Талібану заявив, що члени організації не проти використання цифрових та онлайн технологій, і їх використання не суперечить принципам шаріату. [39]

The Washington Post вказує на те, що таліби досить вдало та грамотно поширюють контент в соціальних мережах, намагаючись не виходити за рамки правил політики безпеки, за якою контролюється діяльність користувачів СМ.

Їхня тактика в онлайновому просторі вважається досить високого рівня та аналітики вважають, що хоча б одна фірма, яка спеціалізується в зв'язках з громадськістю консультує талібів, та допомагає їм в побудові грамотної онлайн-стратегії, допомагає просувати ключові теми, збільшувати вплив на різних онлайн-майданчиках та платформах, та зокрема створювати ті самі ключові вірусні зображення й відеоматеріали. [79]

В Twitter, на відміну від Facebook або YouTube, таліби мають більше свободи дій, адже тут акаунти, створені організацією не видаляються. На думку одного з дослідників Центру медіакриміналістики Університету Клемсона Даррена Лінвілла, по іншу сторону акаунту в СМ, сидять не бойовики або лідери Талібану, а люди, що мають відношення до роботи в СМ та веб-сайтів, та які мають гарне володіння англійською мовою.

Популярні меседжі талібів включають в себе дезінформацію щодо власних доброзичливих дій, в тому числі повідомлення про помилування людей, позитивні наміри, тощо. Тому, американські аналітики закликають користувачів ставитися до будь-яких подібних повідомлень дуже прискіпливо та не довіряти їм. [79]

Ситуація в Афганістані дуже турбує міжнародне співтовариство. Згідно з даними Світового банку за 2017 рік, лише 11,4% населення Афганістану користувалися Інтернетом, що є дуже малим показником, але він різко збільшився з 0%, коли Талібан був при владі. Це також свідчить про те, що аудиторія талібів знаходиться в різних країнах світу. Тим часом, міське населення підпадає під вплив пропаганди терористів, через нерозвинену інфраструктура медіа в країні, що ускладнює місцевим журналістам вести ефективну протидію дезінформаційним заявам терористів. Більше того, експерти наголошують на тому, що низька інтернет-грамотність в країні збільшує ризик сприйняття населенням пропаганди як факту. [122]

– Аль-Каїда

Аль-Каїда також швидко охопила сучасні технології, незважаючи на її спроби уникнули небезпеки модернізації та глобалізації. Лідер Аль-Каїди Усама бен Ладен зазначив, що «90% підготовки до війни – це ефективне використання ЗМІ, та онлайн-технологій. Аль-Каїда довгий час виступала за активні інформаційні операції та електронну війну. [111; 124]

Через онлайн-канали, організація надає відео та фотоконтент, створює дошки оголошень, онлайн-чати, розсилку по електронній пошті, листівки, які можна завантажити. Всього за один рік, з 2005го по 2006 рр. вона збільшила виробництво відео в чотири рази та використовувала близько 4500 веб-сайтів для поширення своїх повідомлень.

Крім того, онлайн-матеріал дублується різними мовами: англійською, французькою, тощо, особливо інформація щодо вербування, щоб з легкістю залучати прихильників із західних країн до своїх лав. Загалом, інформаційні онлайн дії організації були ефективними, і вона успішно долучила багато звичайних користувачів на своїх бійців.

На відміну від ІД, яка активно поширює власний контент з поля бою, історії бійців, та промови лідерів, Аль-Каїда в своїй онлайн діяльності робить акцент на координації своїх центрів, їх кооперації та контролі осередків, що зменшило ефективність вербування, порівняно з ІД. Крім того, організація приділяє увагу саме закритим каналам, прихованим форумам та онлайн-платформам, де вони б могли повністю контролювати доступ користувачів до певного кола питань, пов’язаного з їх джихадистським рухом. Це призвело одночасно до дійсно більш безпечної та глибокої взаємодії з прихильниками Аль-Каїди, та з іншого боку зменшило вплив на населення. Тим не менш, організація приділяє увагу на розповсюдження контенту соціальними мережами, що робить розгляд даної проблеми актуальним для подальшого її вивчення та формулювання прогнозів на майбутнє.

Що стосується окремих СМ, то Аль-Каїда, наприклад, не є таким активним користувачем Telegram, як ІД через постійні видалення профілів.

Так, організація знайшла іншу альтернативу для поширення своєї пропаганди. Rocket Chat виявився більш найдійним варіантом для терористів, через платформу Geo News, яка містить в одному місці безліч багатомовних медіа-каналів з різних філій організації. Дана платформа не була видалена з моменту її створення в кінці 2019 року. [117]

Вона побудована на основі відкритого коду, що включає в себе захищений інтерфейс та, наразі, налічує близько 2200 активних користувачів. Платформа включає в себе як канали для спілкування та поширення думок, так і інформаційно-навчальних груп, яка забезпечує постійний доступ до матеріалів терористів по всьому світу.

Хоча члени групи, звісно, присутні в таких месенджерах як Telegram, WhatsApp, Riot і Minds, кількість користувачів на даних платформах становить лише частку від кількості Rocket Chat. [116]

Запуск, пов'язаний з інформаційним агенством Аль-Каїди – Табат/або Ель-Табат, який поширює інформацію про діяльність організації по всьому світу, стало важливим етапом в період цифрової трансформації Аль-Каїди. Деяким чином, Табат, який служить майданчиком новин організації, імітує роботу інформаційного агенства ІД Nashir.

Табат використовує боти в Telegram, які звітують про роботу різних осередків та філій організації. Окрім цього, агенство також використовує безкоштовні «конструктори» для створення сайтів для поширення пропаганди, та сайт Yola для розповсюдження щотижневого бюлетеня. Окрім цих інструментів, організація активно користується багатофункціональним мобільним додатком для Android як єдиний канал для поширення новин, статичних даних, публікацій, доповідей, та інших статей. [116]

Комунікаційну онлайн-стратегію Аль-Каїди можна умовно розділити на три гілки, де:

– Провідні лідери обмінюються повідомленнями через захищені та закриті платформи;

– Інші діячі обговорюють нагальні питання, стратегії та наявні проблеми на спеціальних закритих форумах, доступ до яких вони можуть надавати іншим користувачам, за бажанням. Вони мають більш відкритий доступ для майбутніх новобранців;

– Остання гілка включає в себе відкриті та незалежні веб-сайти, які дозволяють терористам та майбутнім членам організації спілкуватися, кооперуватися та вирішувати питання.

Однак, деякі аналітики вважають таку стратегію провальною, що не отримала такий самий успіх в порівнянні з ІД. Це пояснюється цілями та ідеологічними мотивами організації, ворог якої знаходиться на відстані (Захід), тому вона швидше залучає «пасивних» членів, які будуть працювати онлайн та поширювати пропаганду, чутки, дезінформацію, ніж активних, які мають бажання «подорожувати» заради терактів. [118]

На мою думку, вважати таку стратегію невдалою, або ж провальною – недоречно, адже інформаційна складова в будь-якій війні/конфлікті/боротьбі є важливим етапом підготовки, контролю та кооперації фізичних дій, тому тероризм в онлайн середовищі, навіть якщо він поки що не провокує активні дії на справжньому полі бою, є небезпечним, адже всі дії, створені терористами в мережі Інтернет, мають свої цілі та мотиви, які також варті уваги.

Уряди країн, політики, лідери думок використовують СМ для поширення власних ідей, та впливу, спілкуються зі своїми прихильниками, так само й ТО користуються соціальними мережами з подібними цілями. Аль-Каїда, наприклад, використовує PalTalk і створює спеціальні чати для спілкування, та відкриті форуми, де будь-хто може приєднатися та бути завербованим або підпасти під вплив терористів. [121]

– Лашкар-е-Тайба

Лашкар-е-Тайба (далі ЛеТ) мають за мету поширення ідей радикального ісламу на території всієї Індії, розширення масштабів впливу в державах Центральної Азії, та інших частин світу, де переважає мусульманське населення, наприклад в Північному Кавказі.

Першим завданням в своїй онлайн-стратегії, організація визначила вербування молодих чоловіків в свої лави. Група також організовує безліч онлайн-семінарів та зустрічей через СМ, які інформують новобранців спочатку про базу використання інтернет-технологій з метою поширення ідеології ЛеТ та її цілей, і по-друге, включає в себе прямі способи впливу на молодь задля участі їх в протестах та терактах організації. [118]

Цими завданнями займаються політичний підрозділ Jamaat-ud-Dawah (JuD) та підрозділ, що займається кібер питаннями, та інформаційною стратегією організації – JuD Cyber Team.

Ще в 2008 році, під час атаки в Мумбаї, ЛеТ використовувала канали соціальних мереж, та інші технології під час терактів. Так, терористи використовували технології VoIP (Voice over Internet Protocol), тобто технологія передачі медіа данних через системи зв’язку IP-телефонії, які кодують звуковий сигнал в цифрову форму та передають його цифровими каналами іншому абоненту, з метою отримання інформації в режимі реального часу. Вони також використовували технології та пристрої глобальної системи позиціонування (GPS), супутнікові телефони/зображення, щоб мати змогу спостерігати за розгортанням подій, вчасно та швидко приймати рішення.

Терористи також стежили за активністю громадян в соціальних мережах, які поширювали повідомлення в Twitter про дії поліції та їх пересування, що й дозволило ЛеТ знизити ефективність планів правоохоронних органів. [118]

Громадяни також поширювали свої думки в СМ, місцезнаходження, щоб повідомим друзям та родичам про свій стан, чим терористи також користувалися, переглядаючи цю інформацію.

ЛеТ також розробила власну програму під назвою Ipotel, яка є зашифрованим спеціальним додатком для зв'язку VoIP. Це позиціонує групу не тільки як користувача СМ та онлайн-технологій, а й демонструє її вміння розробляти нові продукти, тим самим підкреслюючи рівень загрози. [124]

– Боко-Харам

Боко-Харам (далі БХ) – це радикальна ісламістська організація, яка була заснована у 2002 році Мохамедом Юсуфом, спочатку вона позиціонувала себе як релігійно-навчальний комплекс, хоча насправді здійснювала відбір потенційних бійців. Головним осередком діяльності організації стали райони Нігерії на північному заході, де БХ мала за мету втілити закони шаріату. Ці завдання мали бути втілені шляхом відмови від способу життя західного світу та їх цінностей. В інтерв'ю для ВВС, Юсуф назвав західну освіту такою, що перечить ісламу, а також під забороною був традиційний виборчий процес. Однією з характерних методів діяльності БХ стали регулярні захоплення заручників. [43]

Головною метою організації є повалення чинної влади, євро-християнської культури, науки та освіти, і виступає за створення ісламської держави. Члени угрупування також виступають за відновлення справедливості, в їхньому розумінні, через руйнування соціальної та економічної нерівності, корупції, що звичайно привертає увагу молоді, при правильній подачі інформації та повідомлень. Частиною даного ісламського руху є також організація Аш-Шабаб. [25]

В березні 2015 р. Боко-Харам присягнула на вірність ІДІЛ, а пізніше почала називати себе Західноафриканською провінцією Ісламської держави. З самого початку своєї діяльності, БХ взагалі не використовувала привілегії соціальних мереж, але згодом стала активно поширювати пропагандистські матеріали в мережі Інтернет, включаючи відеоконтент, що також може слугувати деяким доказом впливу ІДІЛ.

Станом на 2017 рік, Нігерія була лідером по кількості користувачів інтернетом, завдяки чому доступ до контенту СМ був ще простішим та доступнішим, а кількість користувачів в 2018 р. зросла до 98 млн, в порівнянні з 82 млн у 2015 р. [115;61]

Доступність онлайн-мереж автоматично збільшили залучення та використання додатків таких як Facebook, 2go, WhatsApp, Twitter, Instagram, Snapchat, Telegram та інших. Це покращило соціальний, економічний та політичний ландшафт Нігерії.

Ще до появи онлайн-додатків, БХ поширювала свої ідеологічні та пропагандистські матеріали через відео, брошури та проповіді свого лідера на широкі верстви населення. Організація також координувала дії бойовиків під час атак завдяки мобільним гаджетам. [101]

Можливість постійного контролю, висока інтерактивність, зручність та простота з поширенням візуального контенту «змусили» бійців почати використання СМ.

Через проблему низької інтернет-грамотності населення, бійці надають перевагу залученню нових членів організації особисто, на відміну від Аль-Каїди, але все ще використовують СМ для різних заходів, наприклад:

– Взяття на себе відповідальності за скоєні теракти, тобто терористи поширювали відео з наслідками жорстоких дій, та зізнавалися в тому, що це їх рук справа. Це створювалося з метою розповіді про причини атак, їх цілі та, в деяких випадках майбутні наміри, тобто певний вид попередження. Ці відео були записані з використанням регалій, та членів БХ: прапори на задньому плані, джихадисти, одягнені у військовий камуфляж, зброя, тощо. Доказом таких нападів були полонені солдати, їх зброя, або транспорт, який також потрапляв на фото та відео терористів. БХ також періодично проводить прямі трансляції їхніх нападів, детальні відео про захоплення баз, територій, або інших об’єктів, їх пограбування або руйнація.

– Комунікація з бійцями, або прихильниками організації. У своїх відео, під час нападу на військову базу Гіва (2014 р.), Абубакар Шекау (лідер організації) говорить: «Брати, де б ви не були, я молюся за вас, усе буде добре. Йдіть вперед, будь-то вас двоє, чи троє, візьміть свою зброю та почніть стріляти… всіх тих, хто відмовляється від Аллаха». [92]

– Поширення пропаганди. З метою передання атмосфери «звичайного життя», терористи поширюють відео на YouTube і Facebook з обличчями дружин та дітей, які займаються «повсякденними справами», показують також наявність дотримання правил шаріату на захоплених територіях. З іншого боку, бійці поширюють страшні матеріали задля залякування населення та демонстрування домінування БХ.

В 2015 р. БХ створила власний медіа-офіс, який поширив та зробив більш ефективним використання таких мереж, як YouTube і Twitter (наприклад, створивши власний обліковий запис @Al Urwah al-Wuthqa), що покращило якість матеріалів, розповсюджених на цих платформах. [92]

Організація використовує пропагандистські відео для залякування місцевого населення через платформи YouTube, Twitter, служби новин, тощо. Головними темами для таких відео стали:

- БХ – сильна та могутня організація;
- БХ – багата та успішна;
- БХ – це успішна військова група (а не армія повстанців);
- БХ – це чесна, щира та дружня організація;
- Зневажливе ставлення членів БХ до лідерів Нігерії та західного світу;
- Слабкість уряду Нігерії;
- Боязгливість та некомпетентність Нігерійських солдатів.

На відміну від ІД, відео якої зроблені професійно, гарної якості з метою привернути увагу та надихнути мусульманську молодь в Європі та Північній Америці приєднатися до лав терористів, відео БХ є досить непрофесійні та погано зроблені. Проте, така зйомка теж може бути певною технікою

передачі повідомлень, де грубість, простота відео, без певних сценаріїв мають показати реальні дії терористів, їх серйозність намірів та вселяти страх в того, хто його переглядає. [117]

БХ в своїх повідомленнях в СМ, зазвичай, акцентує не на своїй могутності, та не націлюється на новобранців, а навпаки – зневажає місцеву владу та всяко її дискредитує, демонструючи її неспроможність захистити своїх громадян, її слабкість, та свою зневагу в сторону уряду. Вони використовували СМ для інформаційного впливу на громадян, розвовсюджуючи інформацію про уряд, та свою могутність, непереможність.

Так, терористи показували негативну та різку реакцію уряду, твердження про те, що уряд Нігерії говорить неправду своїм громадянам, та їх незмогу завадити діям терористів в терміни, встановлені самим урядом, і в кінцевому підсумку, підтвердили свою непереможність. Здатність БХ використовувати інформацію проти свого ворога, високий рівень корупції, пов'язаний із закупівлею зброї для боротьби з терористами, все це сприяло успіху БХ у висвітленні уряду як невмілого та неосвіченого.

Соціальні мережі зіграли також негативну роль для БХ. Бійці організації ділилися своїм досвідом з родичами, друзями та навіть ЗМІ через власні акаунти в Facebook, Twitter та Instagram, надсилаючи зображення та відео боротьби з повстанцями. Ці матеріали дали змогу показати справжню ситуацію життя «всередині». Бійці розповідали про відсутність належних умов життя, відпусток та постійне перебування в терористичних таборах, невиплату заробітної плати, та жорстоке поводження старших бійців. [125]

Такий аспект використання цифрових технологій є небезпечним для терористичних організацій, адже є шанс розкриття секретної інформації, поширення негативного контенту про угрупування та скарг, що підриває її позицію та «статус». Бійці також стверджували, що була поширена інформація про майбутні операції, що ставило під загрозу життя терористів. [111; 114]

В червні 2016 року найбільні СМ: Facebook, YouTube, Microsoft і Twitter домовилися про створення спільної бази даних для виявлення терористичної пропаганди, та для загальної перевірки контенту. Цей крок був підтвердженням збільшення терористичного впливу в інформаційному просторі, та небезпеки, яка випливає з цього.

Отже, можна зробити короткий висновок щодо основних характерних особливостей діяльності терористів в СМ. В першу чергу, це їх бажання до кооперації й вербування, в незалежності чи передбачає воно подальший переїзд новобранців до табору, чи це просто «онлайн вербування» з метою поширення власних ідей і пропаганди. Поширення каналів фінансування також часто зустрічається серед головних завдань використання СМ терористами. Тож, в період інформаційного суспільства, коли СМ є невід'ємною частиною життя сучасної людини, а інформація – важливим ресурсом країн світу, соціальні мережі варті подальшого вивчення, а інформаційний тероризм – посиленої уваги з боку держав, міжнародних організацій, та окремих користувачів.

РОЗДІЛ 3. ПРАКТИЧНЕ ДОСЛІДЖЕННЯ СУЧАСНОГО ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ

3.1. Порівняльний аналіз діяльності Ісламської держави та Аль-Каїди в соціальних мережах.

Порівняльний аналіз двох терористичних організацій допоможе виявити різні підходи та варіанти використання соціальних мереж, а також окреслить головні особливості та види контенту, який поширюють ТО.

Даний розділ також допоможе краще окреслити та сформулювати стратегії боротьби з інформаційним тероризмом.

Ісламська держава та Аль-Каїда, на мою думку мають більше відмінних характеристик онлайн-діяльності, ніж подібних. Це пояснюється, зокрема, початковою метою терористів, яку вони намагаються реалізувати, тому і суть онлайн-повідомлень, а також головні завдання дуже відрізняються.

Так, відмінними аспектами можна назвати:

– Ідеологія та цілі організації, що впливають на контекст поширюваної інформації, та територіальне охоплення;

– Цільова аудиторія;

– Сам зміст повідомлень ;

– Методи та канали поширення інформації.

Подібними характеристиками можна назвати:

– Використання закритих каналів комунікації;

– Велике територіальне охоплення;

– Створення власних онлайн-журналів з пропагандистським контентом;

Можна почати з того, що організації мають досить різну організаційну структуру, ідеологію та головні цілі. Ісламська держава, наприклад, має за мету побудування єдиного халіфату, стійкої та сильної організації, використовуючи стратегії, спрямовані на охоплення всього мусульманського світу, що й впливає на бажання організації переконати людину саме до міграції в свої табори та їх майбутній захист від західних сил. Аль-Каїда, в свою чергу, надає пріоритет «віддаленим» атакам на західного ворога (США), надаючи всі сучасні дистанційні цифрові інструменти та інші види зброї для здійснення атак, та поширення пропаганди, незалежно від перебування читача, тим самим збільшуючи число прибічників по всьому світу. Саме тому можна пояснити, що ІД в соціальних мережах, зазвичай, намагається здійснювати вербування нових учасників організації, проводить

досить успішну пропаганду щодо сильного духу, дружнього «колективу», сильної та успішної організації, яка дотримується своїх цілей та йде до мети.

Аль-Каїда, в свою чергу прагне протидіяти поширенню присутності та впливу західних країн, особливо США, як у регіоні, так і по всьому світу, вважаючи саму західну цивілізацію розбещеною та неправильною. Аль-Каїда прагне вигнати збройні сили США з території Перської затоки, зокрема Саудівської Аравії. Окремо варто відзначити її прагнення знищити Ізраїль. Головною ціллю є повалення світського правління в ісламських державах. Тож, Аль-Каїда прагне поширювати свій рух по всьому світу, здійснюючи напади на території різних держав, та не зосереджуватися в одному місці щоб не бути атакованими опонентами, як це сталося з ІД. Це й пояснює її активну участь в онлайн-навчанні своїх послідовників та надання їм усіх потрібних інструментів для здійснення терактів, або ж проведення пропагандистських кампаній. Після теракту 11 вересня 2001го року, лідери Аль-Каїди зрозуміли, що територіально обмежену організацію легше знищити, порівняно з глобальним рухом.

Медіа-підрозділи ІД використовують канали СМ для створення образу справжнього мусульманина, веде живі репортажі з місця бою, розповідає про життя звичайних бійців та відносини в середині Халіфату. ІД намагається створити власну державу та залучити до цього процесу якомога більше прибічників, в той час як Аль-Каїда прагне навпаки дестабілізувати інші держави також за допомогою «онлайн-підтримки» в обличчях звичайних громадян по всьому світу.

Щодо наповнення самих повідомлень, то ІД показувала майже все, включаючи криваві та жахливі кадри вбивств, страт, і т.д., що показувало рішучість лідерів. Це, можливо, й стало однією з причин такого вдалого залучення великої кількості бійців, які теж мали бажання брати участь в створенні власної держави.

Ідеологія Аль-Каїди була спрямована саме на висвітлення всіх, на її думку, негативних та слабких сторін заходу, і в кількох випусках свого електронного журналу Inspire, вона навіть висміювала те, що для паніки в США знадобилося всього 4200 доларів (мова йдеться про ситуацію, коли Аль-Каїда переправляла картриджі для принтерів, які були наповнені вибухівкою через рейс UPS (United Parcel Service). В цьому ж журналі, терористи поширюють інформацію та плітки щодо західних країн, які порушують права мусульман. Так, вони критикують Францію, де існує заборона на носіння паранджі, що сприймається як напад на мусульманських жінок, та говорить про загальну «ісламофобію» в Сполучених штатах.

В своєму бажанні дестабілізувати держави західного світу, Аль-Каїда також зосереджується на їх економічному становищі. Так, в журналі Inspire, згадується ситуація з картриджами, за якою послідували великі витрати в мільярди доларів США для поліпшення та оновлення системи заходів безпеки. Також, згадується теракт 11 вересня 2001р., після якого держава зазнала великих економічних збитків, та інші ситуації, а також майбутні плани щодо дестабілізації та руйнування економіки країн. Впродовж багатьох років, угрупування закріпляла свою антиамериканську точку зору та позицію щодо західних держав.

Отже, ідеологія ІД має фізичне існування, тобто передбачає створення Халіфату, використовуючи сучасні засоби, зброю, соціальні мережі та онлайн-пропаганду, а ось Аль-Каїда позбавлена кінцевої «фізичної» цілі, та має на меті саме збереження та поширення існування ідей та цілей в свідомості своїх послідовників. Вона націлена на окремих осіб, та заохочує їх здійснювати напади там, де вони проживають. Таким чином, Аль-Каїда є не лише терористичною організацією в фізичному світі, а й ідеологією, яка поширюється серед своїх прибічників. Аль-Каїда дещо відстала від ІД у сприйнятті та використанні соціальних мереж, та тим не менш, поява онлайн-комунікацій та цифрових технологій однозначно допомогла Аль-Каїді

охопити більшу територіальну підтримку серед своїх послідовників і потенційних новобранців. ІД, в свою чергу, побудувала свою діяльність вже в існуючому онлайн середовищі, з аудиторією, яка активно користується сучасними інтернет-технологіями.

Для створення ефективної контрстратегії важливо уважно вивчати всі види повідомлень терористів, вчасно на них реагувати, та ще важливим кроком є зосередження та вивчення каналів поширення пропагандистської інформації.

ІД використовує всі наявні онлайн-інструменти для реалізації своїх цілей, та на мою думку, є більш успішною в цьому аспекті, ніж Аль-Каїда. Окремо слід виділити підхід до створення контенту, наявність професійних інструментів для зйомок, відео та фото високої якості, а також контент-план соціальних мереж, журналів, який завчасно будує «сценарій» та цікаву сторінку для читачів. Окрім YouTube, Twitter, Instagram, Facebook, угрупування також користується месенджерами. Так, наприклад, в Telegram, в закритих каналах, ІД ділиться інструкціями, планами та навіть своїми онлайн-магазинами, наприклад LUCKP47 SHOP (найкраща зброя в даркнеті).Крім цього, також існує безліч програм для перегляду сайтів в даркнет, таких як Tor, що також ускладнює виявлення та визначення фактичної IP-адреси.

Щодо контенту, то на відміну від Аль-Каїди, яка спирається на змістовний текст, інколи з фото доповненням, ІД пропонує читачеві різноманітну інформацію, починаючи від добірок «десяти найкращих відео для перегляду» на YouTube, до спеціальних програм для навчання дітей алфавіту, звичайно в стилі терористів. Якщо порівнювати електронні журнали організацій, то ІД має також більш вдалу реалізацію даного виду поширення інформації. Її журнали, це справжні електронні сховища даних, які включають в себе масиви інформації, і що саме цікаве – текст включає в себе посилання, які ведуть читача до інших відео, сайтів, або ж аудіо-

контенту (подібні інструменти можна зустріти на багатьох сайтах, наприклад Вікіпедії, де можна, використовуючи спеціальні посилання, перейти до нової сторінки). Така мультимедійність дозволяє переходити від одної інформації до іншої, рухаючись по певній траєкторії всередині нескінченної спіралі контенту, яка «затягує» читача та врешті-решт може залишити його як майбутнього захисника поглядів терористів та учасника радикальних рухів.

Наступною відмінною ознакою є аудиторія. ІД приваблює молоду аудиторію на глобальному та місцевому рівні, яка добре володіє сучасними цифровими онлайн-технологіями, незалежно від їх віку, статі, тощо. Терористи відкрито говорять про те, що однією з груп населення, здатних до поширення ідей ІД є є мусульманська спільнота з великою часткою безробітної молоді, яка не має особливих життєвих перспектив. Такі групи спроможні реалізовувати в життя радикальні ідеї та швидко зацікавлюються процесом.

Така аудиторія любить ефектно подану інформацію, любить бути «в центрі подій» та залучається до візуальних форм спілкування за допомогою інфографіки та відео високої якості, в порівнянні з журналом Аль-Каїди Inspire, де інформація подається «прісною» – простий текст та зображення низької якості.

Цільовою аудиторією Аль-Каїди є особи на глобальному рівні, тобто по всьому світу, з вищим віковим показником, аудиторія спирається саме на зміст повідомлень, робить висновки та приймає рішення вже в залежності від нього. Вона добре розуміється у світових процесах та підтримує боротьбу Аль-Каїди проти США через втручання останніх в регіон Близького Сходу.

Крім того, організації відрізняються також методом поширення контенту та онлайн-каналами. ІД використовує безліч інструментів: відео-трансляції, репортажі з місця подій, промови лідерів, віртуальні ігри, програми для навчання, електронні журнали, тощо. У випадку Аль-Каїди, онлайн-діяльність є більш функціональною з точки зору спеціальних

посібників, навчальних матеріалів та ноу-хау інструментів, адже вона робить акцент саме на цьому, щоб навчити прибічників по всьому світу дистанційно та залучити їх до терористичної боротьби.

Тож, загалом, ІД акцентує увагу читачів саме на візуальному контенті для поширення своїх екстремістських поглядів, в порівнянні з Аль-Каїдою, яка покладається саме на текстові повідомлення та зображення, що є більш звичним для її аудиторії.

Спільні риси вже були коротко описані вище, перша – це наявність власних онлайн-журналів, у випадку ІД – можна назвати журнал Rumiyah (який , замінює Dabiq, Dar al-Islam та інші журнали, що виходили до середини 2016 року). Аль-Каїда має свій всесвітньо відомий електронний журнал – Inspire. Подача їхнього контенту дещо відрізняється, але сам факт наявності такого виду ресурсу в обох організацій дає підставу віднести його до спільних характеристик.

Також, спільним є використання закритих каналів, сторінок та сайтів, що є повністю логічною поведінкою будь-якої терористичної організації в онлайн-просторі. Якою б відкритою не була інформаційна політика угрупування, все одно існує засекречена інформація, яка має поширюватися лише на обмежене коло аудиторії, або взагалі серед лідерів та головних бійців організації. Використовуються як початково закриті соціальні мережі з можливістю шифрування даних, такі як Telegram, наприклад, так і створюються закриті групи/канали в інших СМ, куди поступово додаються нові учасники.

Спільною рисою також є широке інформаційно-територіальне охоплення аудиторії, що пояснюється бажанням організацій розширювати свої лави та збільшувати могутність. У випадку Аль-Каїди така територіальна ознака пояснюється здебільшого онлайн-діяльністю організації, та дистанційного навчання бойовиків. ІД, зі свого боку, шукає бійців зі всього світу, та направляє їх до своїх таборів, забезпечуючи їх усім необхідним,

починаючи від коштів на дорогу, закінчуючи кураторами, які працюють з ними протягом всього маршруту.

Отже, аналіз показав, що початкова мета терористичної організації може значно вплинути на її подальшу онлайн-стратегію, на обрані інструменти та методи діяльності, а також на інші ознаки, що характеризують її в інформаційному просторі. Така різниця дає нам зрозуміти, що увага органів безпеки має бути зосереджена на різних етапах поширення пропаганди, та вчасно реагувати на можливі незаконні загрози. Щоб протистояти ідеологічним проявам ТО, варто також добре орієнтуватися в каналах поширення інформації, та вміти правильно взаємодіяти з інструментами цих каналів, щоб протистояти будь-якому ідеологічному наступу з боку ТО. Адже, незважаючи на знищення осередку ІД в Сирії та Іраку, ідеологія все ж продовжує існувати та поширюватися, і так як ІД мала свій медіа-центр, він просто перетворився з фізичного «офісу» в цифровий на деякий час, що нагадує ситуацію з Аль-Каїдою.

Сучасні ТО користуються великою кількістю інтернет-платформ, онлайн-інструментів, а отже мають доступ до незліченної кількості пристроїв, що допоможе завербувати більшу кількість потенційних послідовників. Інструкції зі застосування певних видів зброї, та її створення, навчальні посібники терористів, та інше знаходиться в мережі Інтернет, та може потрапити до рук будь-якого користувача мережею, тож ця проблема є дуже важливою для ретельного вивчення та потребує негайного вирішення.

Одним із основних завдань також має бути обмеження обігу такого контенту, який циркулює через платформи соціальних мереж, та протидія каналам поширення. Такий феномен інформаційного тероризму, який швидко розвивається та видозмінюється, можна подолати, якщо розробити міцну та стабільну нормативну базу в сфері інформаційної безпеки, яка обов’язково буде розглядати соціальні мережі як окремий онлайн-інструмент, та відповідно розробляти стратегію боротьби з тероризмом

відповідно до особливостей, які притаманні СМ, а не загальні характерні ознаки будь-яких цифрових технологій.

3.2. SWOT-аналіз соціальних мереж.

Соціальні мережі відкрили багато можливостей поширення власних думок, ідей, кооперації користувачів у вирішенні спільних питань та проблем, а також звичайному спілкування з цікавою за інтересами аудиторією. Зі зміною інструментарію СМ, їх розвитком, варто також змінювати шляхи протидії інформаційному тероризму, SWOT-аналіз СМ зможе виділити головні аспекти, на які потрібно звернути увагу задля покращення політики безпеки в СМ та запобігання збільшення терористичної діяльності в інформаційному просторі.

SWOT-аналіз є видом планування покращення певної проблеми, на основі вивчення та аналізу внутрішніх та зовнішніх чинників, які впливають на цю проблему.

SWOT розшифровується як:

- Strengths (сильні сторони);
- Weaknesses (слабкі сторони);
- Opportunities (можливості);
- Threats (загрози).

Сильні та слабкі сторони відносяться до внутрішніх чинників, а можливості й загрози до зовнішніх.

Тож, вивчивши всі особливості незаконної діяльності в СМ, можна виділити наступні характеристики:

Strengths (сильні сторони)	**Weaknesses (слабкі сторони)**
– Відкритий доступ до	– Відсутність належної

інформації, що дає змогу легко прослідкувати за повідомленнями терористів; – Надання доступу до геолокації; – Можливість миттєво отримувати актуальну інформацію, бути присутнім в колі подій; – Дешевизна та легкий доступ до технологій	відповідальності за скоєння незаконних дій (лише блокування акаунту); – Шифрування інформації та повідомлень, створення закритих каналів та груп; – Створення облікових записів без введення правдивої інформації про користувача/створення фейкових сторінок; – Відсутність адаптивної політики безпеки, яка б вчасно реагувала на нові атаки;
Opportunities (можливості)	**Threats (загрози)**
– Вчасне реагування органів безпеки на можливі теракти; – Здійснення моніторингу та аналізу контенту й поведінки користувачів; – Підвищення рівня обізнаності в питаннях онлайн-безпеки; – Збереження масивів даних та важливої інформації про користувачів;	– Прискорення радикалізації серед користувачів через велике охоплення аудиторії; – Недостатня захищеність користувачів як в технічному, так і психологічному плані; – Створення системи фінансування злочинних угрупувань; – Створення нових соціальних мереж без стабільної безпекової системи, чим можуть скористуватися терористичні організації

(табл.1 SWOT-аналіз)

До сильних сторін можна віднести легкий доступ до технологій, їх простоту у використанні та доступну інформацію. Терористи, зазвичай, ведуть змішану інформаційну політику, яка включає в себе як закриті дії,

доступні для окремого кола користувачів, так і відкриту пропаганду, націлену на широку аудиторію, і саме це дає змогу вислідкувати терористичний контент, вчасно відреагувати на повідомлення, та за змоги – попередити можливі атаки. Доступ до геолокації дає змогу вислідкувати, хоча б приблизне місце, з якого було відправлене те, чи інше повідомлення, часто користувачі самі вказують геопозицію під час поширення фото або відео на своїх сторінках. Також, така відкритість дає змогу самим користувачам, до рук яких потрапив небажаний або жорстокий контент, поскаржитись на сторінку або групу, що призводить до обов'язкової перевірки акаунту модераторами та адміністраторами, які аналізують діяльність даної сторінки, її повідомлення та дописи.

Все це допомагає органам безпеки та самим користувачам СМ виявляти незаконний контент, та вчасно на нього реагувати, але на мою думку, в контексті розгляду СМ як платформи для терористичної діяльності та її рівня безпеки, вона має більше слабких сторін, ніж сильних, що й проявляється в активному використанні ТО соціальних мереж.

До слабких сторін я віднесла, по-перше відсутність належної відповідальності за скоєння незаконних дій, і як на мене, це також пов'язано з наступною негативною характеристикою СМ, а саме – створення облікових записів без введення правдивої інформації про користувача/створення фейкових сторінок. Після виявлення користувачами, або модераторами поширення забороненого контенту, відбувається блокування акаунту/групи, без подальших дій або розслідування, окрім певних випадків. Більшість популярних СМ потребують лише вашу поштову скриньку при реєстрації облікового запису, інколи навіть номер мобільного телефону, що ніяк не ідентифікує вас як особу, або громадянина певної країни, тобто СМ дають можливість реалізовувати свою діяльність під чужим ім'ям, з фейковою інформацією, і т.д.

Також, проблемою є етап аналізу інформації модераторами, що включає в себе виявлення незаконного контенту та негайне його видалення. Перша сходинка цього аналізу є автоматизована, яка ще на етапі створення контенту та його поширення, відразу аналізує його та блокує в разі невідповідності до політики користування СМ. Такий автоматичний фільтр націлений лише на окремі слова та словосполучення, які він виявляє, та вважає за небезпечні, але часто інформація може бути подана у вигляді зображення, або завуальованого тексту, який може зрозуміти лише окрема аудиторія, що ускладнює перевірку контенту. Це і є ще одною слабкою ознакою СМ, яка не дає змогу здійснити якісну перевірку та пропускає багато забороненого контенту у вільний доступ.

СМ дають нам можливість збереження даних про користувачів, їх діяльність та можуть бути використані для запобігання злочинності та проведення аналітичних досліджень. Наприклад, аналіз СМ дає змогу військовим, органам безпеки, урядам країн дослідити будь-яку інформацію, тенденції розвитку проблеми, наприклад ставлення громадян до того чи іншого питання, світогляд та позиція широкого кола осіб. Так, контент-аналіз можна використати з метою пошуку та виявлення користувачів у процесі радикалізації, оцінити ступінь підтримки екстремістських поглядів у певній групі. Дописи, що містять дані про геолокацію допоможуть покращити аналіз та надати оцінку географії поширення певних груп чи ідей. Завдяки аналізу соціальних мереж можна сприяти, або, навпаки, протидіяти поширенню окремих ідей або інформації. Аналіз постів та дописів в СМ може виявити лідерів суспільної думки. Алгоритми класифікації фото, відео-контенту, а також інших зображень допомагають дізнатись, які види контенту популярні в СМ, а разом із даними про локацію та місцевість – відстежити зміну вподобань та ставлення населення до різних речей в тих чи інших країнах.

Загрози включають в себе відсутність стабільної та ефективної політики безпеки в нових СМ, що є також «Ахіллесовою п’ятою», якою

можуть скористатися терористи. Вже згадані слабкі характеристики СМ можуть завдати шкоди та стати загрозою до подальшої радикалізації користувачів, залучення їх до лав терористів та продовження існування небезпечної атмосфери в онлайн просторі.

Наступним кроком в SWOT-аналізі є побудова матриці, яка поділяє нашу інформацію за наступними групами:

– SO – лінія, де вивчаються сильні сторони і можливості з метою покращення ситуації

– WO – використання наявних можливостей для певного «придушення» слабких сторін задля поліпшення ситуації;

– ST – лінія захисту, що показує як переваги можуть захистити від неконтрольованих зовнішніх чинників, тобто загроз. Допоможе визначити, чи зможемо ми в нашій ситуації боротися з загрозами при наявних позитивних рис.

– WT – лінія попередження показує нам, які заходи варто реалізувати для попередження майбутніх ризиків.

В подальшому дослідженні дані стратегії так і будуть називатися: SO, WO, ST, WT.

Тобто, можна виділити наступні стратегії:

- Стратегія «покращення ситуації» (SO);
- Стратегія «вчасного реагування» (WO);
- Стратегія «захисту від загроз» (ST);
- Стратегія «попереджувальних заходів» (WT).

Зовнішнє середовище			
		Можливості	Загрози

Внутрішнє середовище	Сильні сторони	Використання наявних сильних сторін соціальних мереж в контексті боротьби з інформаційним тероризмом з метою реалізації всіх можливостей	Стратегія показує чи досить ефективними є наші сильні сторони при боротьби з зовнішніми загрозами
	Слабкі сторони	Реалізація можливостей для вчасного попередження атак та перекриття тим самим слабких сторін	Стратегія дає нам змогу зрозуміти, які на які заходи потрібно в першу чергу звернути уваги та виправити їх, щоб вчасно попереджувати можливі загрози

В стратегії покращення ситуації, модератори мають змогу використовувати свій наявний доступ до даних користувачів, їх листування, що дасть змогу здійснити більш детальний аналіз як самих користувачів, так і аналіз контенту, який вони поширюють для подальшого вчасного виявлення радикально налаштованих осіб, та вчасного блокування їх дописів, або ж сторінки/групи. Користувачі, в свою чергу, та ЗМІ, що мають доступ до загальної інформації в СМ, або які потрапили до закритих груп терористів, та мають на меті викорінити дану проблему, мають можливість здійснювати аналіз контенту терористів, їх настрої та виявити на короткостроковій перспективі головні тенденції діяльності ТО, та їх можливі подальші дії, що дасть змогу органам безпеки вчасно попередити можливі теракти в фізичному світі, або кібертерористичні напади в цифровому вимірі. Так само й державні органи, що мають доступ до більших масивів даних, та за

допомогою соціальних мереж мають змогу аналізувати поведінку терористів, аудиторію, на яку вони зазвичай націлені, та на основі вже перевіреної інформації – попереджувати можливе скоєння злочинів у майбутньому.

Тут варто зауважити також про важливість взаємодії державних/правоохоронних органів та адміністрацією соціальних мереж. Часто органи безпеки можуть прослуховувати чи переглядати інформацію підозрюваних осіб в соціальних мережах, що може допомогти попередити скоєння злочину на будь-якому його етапі: обговорення, підготовки, або ж безпосередня реалізація.

Щодо аналізу другої стратегії, то наявні можливості не дають змогу повністю прибрати слабкі сторони нашої проблеми, адже для створення адаптивної політики, надання належної відповідальності за скоєння терористичних дій в інформаційному просторі СМ, варто створити спеціальне нормативно-правове регулювання такої діяльності взагалі, та визначити головні шляхи покарання осіб, які ведуть терористичну діяльність. Тут можна привести в приклад уряд США, який використовує інформацію з соціальних мереж для перевірки іноземців, що приїжджають в країну, та отримують візу. Так, обов'язковим етапом є перевірка всіх соціальних мереж, поштових скриньок, минулі та наявні імена користувача, його попередні реєстрації в будь-яких СМ та номери телефонів. Все це допомагає скласти більш конкретну картину про особу, та зрозуміти рівень її небезпеки для держави. Якщо раніше такі дії застосовувалися тільки для осіб під підозрою, то зараз цю перевірку проходять усі громадяни.

Стратегія «захисту від загроз» передбачає використання вільного доступу до інформації користувачів, їх контенту; швидкісного поширення повідомлень і взагалі доступності СМ, в ході боротьби з недостатньою захищеністю користувачів в онлайн просторі та інших загроз. Вже згадані шляхи аналізу контенту, можуть допомогти в ході попередження деяких негативних зовнішніх впливів, але тут варто виділити загрозу, що потребує

окремого вирішення – це створення нових соціальних мереж, та використання терористами ще недоопрацьованої або відсутньої політики безпеки. Нажаль, багато нових СМ в перший період свого існування працюють в тестовому режимі, лише перевіряючи справність інструментарію, та виправляючи наявні проблеми в роботі програми. В цей період, коли користувачі лише тестують нову СМ, терористи встигають провести свою пропагандистську політику.

Тому, на мою думку, на етапі тестування СМ, можна взяти за приклад тестування деяких відеоігор, які проходять альфа та бета-тестування лише для закритого кола користувачів (тобто осіб, що мають вплив в цій сфері, або осіб, які займаються технічною складовою даних програм). Тож, таку практику можна реалізовувати і з соціальними мережами, надаючи доступ в період тестування обмеженій аудиторії, що дає змогу виправити всі помилки в роботі програми, та допрацювати всі інші складові, включаючи інформаційну безпеку, не піддаючи небезпеці самих користувачів.

Остання стратегія включає в себе систему «попереджувальних заходів» (тобто на що саме варто звернути увагу, та виправити в першу чергу, щоб попередити якомога більше можливих загроз). На мою думку, наявні загрози вже були проаналізовані вище, а саме відповідальність за скоєння злочину онлайн, відсутність належної політики безпеки, тому я б хотіла зупинитися, напевно, на одному з початкових етапів залучення користувача в світ соціальних мереж, а саме – етап реєстрації.

Великою проблемою, як на мене, є можливість створення облікового запису користувача, що займає лічені хвилини, і не потребує використання будь-яких даних, які могли б ідентифікувати користувача. Також, сюди можна віднести купівлю мобільних номерів, які частіше всього використовуються при реєстрації будь-яких сторінок, чи то в інтернет-магазині, чи в СМ. Це дає змогу особам, що вчиняють протизаконні дії здійснювати незліченну кількість купівель номерів, та їх постійну заміну.

Станом на 2019 рік, понад 150 країн запровадили реєстрацію та активацію SIM-карти лише за наявності документа, що посвідчує особу, низка країн теж спробували запровадити обов'язкову реєстрацію карток у такий спосіб, але вирішили все ж таки відмовитися. Уряд Великої Британії, експерти з безпеки, приставники спецслужб, та провайдери після теракту в Лондоні в 2005 р. розглянули та детально вивчили дане питання, але в кінцевому результаті вирішили не реалізовувати дану ініціативу, адже вирішили, що це не дасть нових переваг, а лише відштовхне користувачів від бажання проходити самостійну реєстрацію.

Тому, ці дії варто запроваджувати не на етапі реєстрації SIM-карти, а на етапі її купівлі, що вже успішно реалізується в Норвегії, Польщі, Франції, Російській Федерації, Бразилії, та інших державах. Уряд України, в свою чергу, також розглядав законопроект про запровадження продажу SIM-карток за паспортом, який не увінчався успіхом, мовляв це порушує приватне життя громадян. [13]

На додаток до відсутності ідентифікаційних можливостей користувача на момент реєстрації, в СМ є також усі можливості надавати фейкову інформацію безпосередньо в своєму профілі. Тож, всі ці аспекти, впливають на збільшення незаконних дій в онлайн просторі та існування великої кількості фейкових сторінок на просторах інтернету.

Отже, незважаючи на те, що соціальні мережі дають широкі можливості соціалізуватися сучасній людині в онлайн просторі, знайти близьких за інтересами людей, здійснювати кооперацію та отримати безліч корисної інформації, СМ також є небезпечним середовищем поширення терористичної пропаганди. На сучасному етапі розвитку інформаційно-комунікаційних технологій, є необхідним постійний моніторинг контенту в СМ, та аналіз тенденцій поведінки користувачів, їх вподобання, тощо. Розумним буде не блокування ресурсів, а їх більш глибоке вивчення, усунення проблем, що допоможе в подальшому покращити обізнаність в

даній сфері та побудову відповідних висновків та рекомендацій. Органи безпеки вже використовують СМ для виявлення, розслідування та попередження злочинів. Здійснюється також моніторинг закритих чатів, груп, блогів та сайтів задля отримання потрібної важливої інформації.

Якщо говорити про короткочасну перспективу, включаючи стан проблеми сьогодні, загрози можуть якщо не залишатися на місці, то збільшуватися. Тож, варто в першу чергу звернути увагу на згадані слабкі сторони СМ, й на додаток збільшити залучення правоохоронних органів до використання СМ при розкритті злочинів, створення ефективної системи протидії інформаційному тероризму та створення безпечного онлайн середовища для користувачів шляхом постійного моніторингу контенту.

Міжнародне співтовариство активно веде боротьбу з інформаційним та кібертероризмом, але ці дії мають бути систематизовані у всіх країнах, що користуються тією чи іншою СМ, тобто повинна бути створена загальна політика безпеки в інформаційному просторі, та відповідно обов’язкове її дотримання.

На завершення, можна підсумувати всі аспекти, на які варто звернути увагу та в першу чергу їх вирішити:

– Ідентифікація користувачів під час реєстрації шляхом використання документу, що посвідчує особу;

– Створення загальної політики безпеки країнами світу;

– Постійний моніторинг контенту правоохоронними органами;

– Початкові етапи тестування соціальних мереж та програм – для закритого кола користувачів;

– Створення окремого виду відповідальності за здійснення інформаційного тероризму.

ВИСНОВКИ

В ході дослідження, були виконані головні завдання, а також здійснена мета, а саме: була проаналізована наукова література, виявлені головні особливості діяльності терористичних організацій в онлайн просторі та використання ними інформаційно-комунікаційних технологій, зокрема соціальних мереж, також був досліджений міжнародних досвід в сфері протидії тероризму.

В першому розділі були проаналізовані підходи до тлумачення термінів «тероризм», «терор», «терористична організація», «організована злочинна група», «соціальна мережа», а також види терористичної діяльності. З розвитком технологій, та збільшенням цифрових інструментів, з'явився інформаційних та кібертероризм. Головною відмінністю є те, що інформаційний тероризм охоплює психологічну ланку, а кібертероризм – технічну, або цифрову. Тобто, під інформаційним тероризмом розуміється саме використання фейкового контенту/ дезінформації, поширення пропаганди, залякування громадян в онлайн просторі, тощо. Кібертероризм, в свою чергу, націлений на технічну складову цифрових технологій, тобто до нього можна віднести наступні дії: інформаційні атаки на комп'ютери, обчислювальні системи, руйнування баз даних, злом приватних ресурсів, та здійснення несанкціонованого доступу. Цей вид тероризму є небезпечним, адже він не має фізичних меж та може бути здійснений з будь-якої точки планети.

В другому розділі було проаналізовано «онлайнову діяльність» терористичних організацій, таких як Ісламська держава, Аль-Каїда, Боко-Харам і Талібан, а також загальну практику використання соціальних мереж терористами, виділені головні особливостію

В третьому розділі був здійснений порівняльний аналіз діяльносіт Аль-Каїди та Ісламської держави в інформаційному просторі з використанням соціальних мереж; виділені спільні та відмінні риси, на основі яких були зроблені висновки. Головною початковою відмінністю цих угрупувань стала

їх ідеологія, яка і вплинула на подальші особливості діяльності. Вона вплинула як на методи вербування, так і загалом на діяльність терористичних організацій на міжнародній арені. Ісламська держава веде відкриту політику в соціальних мережах, роблячи акцент на свою всеосяжність та щоденне спілкування зі своїми послідовниками. Незважаючи на великі ризики такої неприхованої діяльності, ІД успішно продовжує реалізовувати свої наміри та цілі. Головними завданнями терористичних організацій в цифровому вимірі є: вербування нових членів угрупування; створення інформаційного, навчального, пропагандистського та інших видів контенту; забезпечення шляхів фінансування терористичних дій; масовий вплив на аудиторію, поширення маніпулятивних повідомлень; нав'язування своєї ідеології.

Аль-Каїда, в свою чергу, має більшу сконцентрованість саме на «дистанційному навчанні» своїх послідовників, які знаходяться в різних країнах світу, та не збирає їх в одному осередку. Тим самим вона поширює свої ідеї на глобальному рівні, та здійснює теракти по всьому світу.

Порівняльний аналіз показав, що саме початкова мета може значно вплинути на подальшу стратегію терористичної організації в інформаційному просторі, методи реалізації своїх цілей, обрані інструменти та канали комунікації. Такі відмінності інформаційної політики ТО дають нам зрозуміти важливість вивчення як самих тенденцій розвитку терористичної онлайн діяльності, так і початкові цілі терористів. Варто також вчасно реагувати на повідомлення, які поширюються ТО, та вміти правильно взаємодіяти з цифровими інструментами, щоб протистояти будь-якому ідеологічному наступу з боку ТО.

Також, в останньому розділі був виконаний SWOT-аналіз соціальних мереж в контексті їх безпеки, виділені основні сильні та слабкі сторони, а також наявні можливості та загрози. Аналіз показав, що головними аспектами, на яких слід зосередитися в першу чергу є:

– Відсутність ідентифікації користувачів;

- Неналежне тестування соціальних мереж;
- Недостатньо ефективна фільтрація контенту.

Тож, підсумовуючи, можна сказати, що на сьогодні, досвід у вивченні теми сучасного тероризму, його форм, видів та інструментів – достатній, а ось аналіз соціальних мереж все ще потребує покращення. Соціальні мережі –занадто відкритий інструмент, безпека якого під питанням, деякі сервіси взагалі не мають модераторів та адміністраторів, в компетенції яких була б перевірка вмісту контенту та повідомлень користувачів.

З активним розвитком технологій збільшується присутність терористичних організацій в онлайн просторі, та розвиваються інструменти інформаційно-пропагандистської роботи. На сьогодні, рівень терористичної загрози у світі досить високий, від неї потерпають як країни, де тривають збройні конфлікти (передусім на Близькому Сході та в Африці), так і країни Заходу, що до останнього часу вважалися цілком безпечними з огляду на розвинену систему правоохоронних органів і спецслужб. Протидіяти цій загрозі стає дедалі важче. Сучасний тероризм – це явище, що не має географічних кордонів і не лише становить небезпеку для окремих країн, а й ставить під сумнів стійкість міжнародного правопорядку та спроможність протистояти викликам з боку міжнародних терористичних організацій і квазідержавних утворень, які претендують на самостійну роль у системі міжнародних відносин.

Сучасні інформаційні технології мають безліч переваг, які допомагають громадянам вести повноцінне онлайн життя в інформаційному просторі: створювати, поширювати та обговорювати інформацію, знаходити подібних за інтересами людей. Соціальні мережі дають змогу спілкуватися, кооперуватися, тощо. Завдяки своїм зручним інструментам, онлайн мережами користуються сучасні політичних діячів, новинні канали, засоби масової інформації, державні структури, та ін., з метою поліпшення власного

іміджу, поширення ідей, формування суспільної думки, привернення уваги до нагальних проблем, тощо.

Поряд з перевагами, соціальні мережі мають серйозні недоліки, якими й користуються терористичні організації. До них можна віднести: можливість створення закритих та приватних акаунтів/груп, недостатній контроль над користувачами, відкритість мережі та її «вседозволеність», що призводить до активнішої кооперації та діяльності злочинних угрупувань та шахраїв, викрадення персональних даних та розповсюдження забороненого контенту, дезінформація населення та пропаганда, тощо. Соціальні мережі активно використовуються задля власних цілей, в тому числі й в інформаційному протиборстві.

У сучасному світі, де відбувається активна глобалізація, терористичні дії часто виходять за рамки однієї країни та мають міжнародний характер. За цих обставин, національні уряди країн мають вирішувати одразу два завдання: забезпечення національної безпеки і сприяння розв'язанню глобальної проблеми. Тож, міжнародне співробітництво у сфері протидії тероризму набуває нині особливого значення, в тому числі й у контексті забезпечення національної стійкості.

Вагомим компонентом у системі протидії терористичній діяльності організацій є поширення та укріплення співробітництва та взаємодії з іноземними правоохоронними органами, спецслужбами, а також міжнародними організаціями у сфері боротьби з тероризмом.

Багато країн світу активно запровадили та користуються базами даних осіб, груп та організацій, стосовно яких було введено низку санкцій. Також здійснюється жорсткий фінансовий моніторинг з метою недопущення надання ними матеріальної, фінансової або іншої допомоги терористичним організаціям. Відповідно до світової практики визнання організацій терористичними може здійснюватись у судовому або позасудовому порядку.

На національному рівні держави мають вживати додаткових заходів, спрямованих на профілактику тероризму, вдосконалювати антитерористичне законодавство, розширювати повноваження силових структур, надаючи їм додаткові інструменти, покращювати взаємодію та обмін інформацією між уповноваженими органами, створювати нові координуючі органи по боротьбі з тероризмом, та посилювати відповідальність за участь у терористичній діяльності, особливо в інформаційному просторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авдєєва Т. Вибуховий контент онлайн. Частина 1: веб-сайт. URL: https://cedem.org.ua/analytics/vybuhovyj-kontent-onlajn/.
2. Академічний тлумачний словник української мови: веб-сайт. URL: http://sum.in.ua/
3. Актуальні питання протидії тероризму у світі та в Україні: аналіт. Доповідь / Резнікова О.О., Місюра А.О., Дрьомов С.В., Войтовський К.Є.; за заг. ред. О.О. Резнікової. – К.: НІСД, 2017. – 60 с.
4. Артамонов И.И. Терроризм: способы предотвращения, методика рассладования. – М.:Изд-во И.И. Шумилова, 2002. –с.29-33.
5. Бабенко Ю. Інформаційний тероризм: Електронний ресурс. – URL: http://www.aratta-ukraine.com/text_ua.php?id=149.
6. Банк Р. О. Інформаційний тероризм як загроза національній безпеці України: теоретико-правовий аспект. *Інформація і право*. 2016. № 1 (16). С. 110–116.
7. Битяк Ю. П., Калиновський Ю.Ю. Деструктивний вплив соціальних мереж на інформаційну безпеку людини й суспільства. Науковий семінар ХНУ ПС ім. І.Кожедуба. 2020. С. 1-7.
8. Біленчук П.Д., Кофанов А.В., Кобилянський О.Л. Міжнародний тероризм: консолідований аналіз забезпечення безпеки. – Навчальний посібник. – Київ: ННІПСК КНУВС, 2009. – 72с.
9. Бойченко О. В. Медіа-тероризм: особливості сучасних ознак інформаційній безпеці / Інтегровані інтелектуальні робото технічні комплекси (ПРТК-2009): Друга міжнародна наук.-практ. конф. (25–28 травня 2009 р.). – К.: НАУ, 2009. – С. 230–232.
10. Бойченко О. В., Ончурова О.О.Кібертероризм у складі сучасних проблем національної безпеки. *Форум права.* – 2010. – № 2. – С. 57–62.
11. Бугера О. Використання соціальних Інтернет-мереж для запобігання злочинності. Підприємництво, господарство і право. Сер. Кримінологія. 2018. Вип. 5. С. 238-241.

12. Бутузов В. М. Системно-структурний аналіз як метод дослідження протидії комп'ютерній злочинності / *Правова інформатика*. - 2011. - № 1. - С. 67-71. – Електронний ресурс. URL: http://nbuv.gov.ua/UJRN/Pinform_2011_1_13
13. В яких країнах неможливо придбати SIM-картку без документів та реєстрації. *Аналітичний портал «Слово і діло»*. – 2019: веб-сайт. URL: https://ru.slovoidilo.ua/2019/11/27/infografika/obshhestvo/kakix-stranax-nevozmozhno-kupit-sim-kartu-dokumentov-i-registracii.
14. Вахула Б. Я. Соціальні інтернет-мережі, їхні функції та роль у формуванні громадянського суспільства / Вісник Львівського університету. — Львів : [б. в.], 2012. — Вип. 6. — С. 312, 313.
15. Види тероризму. *Lib-Net.com:* веб-сайт. URL: http://lib-net.com/content/9312_Vidi_terorizmy.html
16. Визначення поняття тероризм та його генезис / І. Р Серкевич. Часопис Київського університету права. - 2011. - № 4. - С. 331-335. Електронний ресурс. Режим доступу: http://nbuv.gov.ua/UJRN/Chkup_2011_4_82
17. Використання соціальних мереж: посібник з питань використання соціальних мереж, розроблений Департаментом преси і публічної інформації Консультативної місії ЄС в Україні: Київ, 2020. 46 ст.
18. Волошин Ю.О. Legal globalization and interstate integration as a leading factor of the formation of state security and sovereignty. Atlantic Press. 2nd International Conference on Social, Economic and Academic Leadership . – 2018, № 11. – P. 351-358
19. Волошин Ю.О., Замула А.Ю.The State as the Leader in Fighting International Terrorism in the Globalized World. International Conference “Entrepreneurial and Sustainable Academic Leadership” . –2018. – P. 491-501.
20. Гаркуша Ю.О. Тероризм як окремий вид суспільно небезпечної діяльності, вчинений з використанням соціальних мереж. Право і суспільство. 2016. Вип. 4. С. 174-180.

21. Гармашов І. Актуальні питання класифікації сучасного тероризму: веб-сайт. – URL: http://www. politik.org.ua (дата звернення 12.11.2021)
22. Геніческий фаховий коледж Херсонського державного університету: 2015: Веб-сайт. URL: http://gmu.ks.ua/problematyka-teroryzmu/ (дата звернення: 12.11.2021).
23. Герасименко К. С. Сучасні ознаки загроз інформаційного тероризму. *Форум права.* – 2009. – № 3. – С. 162-166.
24. Глазов О. В. Міжнародний інформаційний тероризм в контексті загроз національній безпеці України / О. В. Глазов: Електронний ресурс. URL: http://lib.chdu.edu.ua/pdf/naukpraci/politics/2012/197-185-15.pdf.
25. Глобальні трансформаційні процеси в країнах світової периферії (регіон Субсахарської Африки): виклики та можливості для України: матеріали міжнар. наук. конф.; вид. укр. та англ. мов.: доповн. та уточ. / НАН України, ДУ «Інститут всесвітньої історії НАН України» ; Відп. наук. ред. О.І. Лукаш. – К., 2017. – С. 59 – 68
26. Громлюк І. Пандемія та ІДІЛ. Як Йорданія бореться з бойовиками, які вербують молодь через Facebook і Telegram. ms.detector.media: веб-сайт. URL: https://ms.detector.media/trendi/post/25126/2020-07-24-pandemiya-ta-idil-yak-yordaniya-boretsya-z-boyovykamy-yaki-verbuyut-molod-cherez-facebook-i-telegram/
27. Группировки радикальных исламистов как угроза региональной и международной безопасности / С.М. Иванов. *Дипломатическая служба.* – 2016. – № 5 (68). – С. 38 – 47.
28. Губанов Д. А. Социальные сети: модели информационного влияния, управления и противоборства / Д. А. Губанов, Д. А. Новиков, А. Г. Чхартишвили. — М. : *Физматлит*, 2010. — С. 84—86
29. Динник І. Соціальні мережі як засіб суспільного розвитку. *Ефективність державного управління.* 2017. – № 1. С. 64-69.

30. Довгань О. Д. Соціальні мережі як чинник впливу на інформаційну безпеку. Правова інформатика. 2015. – № 2. С. 25-31.
31. Закон України від 05.10.2017 № 2163-VIII «Про основні засади забезпечення кібербезпеки України».
32. Иванов С. Как сайт 8chan стал главной информационной площадкой для террористов: Хайтек – Медиа: веб-сайт. URL: https://hightech.fm/2019/11/14/8chan
33. Исламское государство - угроза мировой безопасности / С.М. Иванов. Зарубежное военное обозрение. – 2015. – № 12 (825). – С. 52 – 55.
34. Исламское государство как передовой отряд международного терроризма. В сб. 70-летие Первой ассамблеи ООН и современные вызовы международной безопасности. М.: Институт Европы РАН. – 2015, с. 52-58
35. Исламское государство как угроза региональной и международной безопасности / С.М. Иванов. Ежегодник СИПРИ «Вооружения, разоружение и международная безопасность» со Специальным приложением ИМЭМО РАН: пер. с англ. Редкол.: А.А. Дынкин, А.Г. Арбатов, В.Г. Барановский и др. М.: ИМЭМО РАН, 2015. - С. 716-723
36. Использование информационных методов борьбы террористической организацией ИГИЛ / Л. Р. Рустамова. *Международная жизнь.* – 2019. – № 5. – С. 112-119.
37. ІДІЛ випустив мобільний додаток для дітей. *Texty.org.ua:* веб-сайт.URL: https://texty.org.ua/fragments/67504/IDIL_vypustyv_mobilnyj_dodatok_dla_ditej-67504/
38. Ілія Куса. Інформаційний аспект тероризму та переговорний процес із терористами. 2014: Електронний ресурс. URL: http://mskod.com/informatsiyniy-aspekt-terorizmu-ta-peregovorniyprotses-iz-teroristami

39. Как социальные сети помогли талибам взять под контроль Афганистан: веб-сайт. URL: https://www.maximonline.ru/guide/kak-socialnye-seti-pomogli-talibam-vzyat-pod-kontrol-afganistan-id675060/
40. Катренко А. Особливості інформаційної безпеки за міжнародними стандартами. *Альманах економічної безпеки*. – 1999. – № 2. – С. 15-17.
41. Кикоть В.Я. Современный терроризм: анализ основных направлений / В.Я. Кикоть, Е.П. Кожушко. – Минск, 2000. –77 с.
42. Кількість користувачів інтернетом в Україні виросла на 7% - дослідження. Економічна правда: Веб-сайт. 2019. URL: https://www.epravda.com.ua/news/2019/10/11/652498/ (дата звернення: 23.10.2021).
43. Коли західне – це харам! Аналітичний центр ADASTRA: веб-сайт. URL: https://adastra.org.ua/blog/koli-zahidne-ce-haram
44. Коршунов В. О. Політичний тероризм: інформаційні методи боротьби : автореф. дис. на здобуття наук. ступеня канд. політ. наук : спец. 23.00.02 «Політичні інститути та процеси» / В.О. Коршунов. – Дніпропетровськ, 2008. – 18 с.
45. Кубишкін О. В. Міжнародно-правові проблеми забезпечення інформаційної безпеки держави.: Електроний ресурс. URL: http://pravolib.pp.ua/ informatsionnyiyterrorizm-15103.html.
46. Лабенко Л. В. Інформаційний тероризм: поняття та ознаки. Міжнародні читання присвячені пам'яті професора Імператорського Новоросійського університету П. Є. Казанського: матеріали Міжнародної конференції (м. Одеса, 22-23 жовтня 2010 року). – Одеса : Фенікс, 2010. - С. 195-198.
47. 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. № 2(59). С. 170–176.

48. Лисенко А. М. Особливості терористичних груп та організацій як форм організованої злочинності / А. М. Лисенко. *Форум права.* – 2010. – № 4. – С. 576–580: Електронний ресурс. URL: http://www.nbuv.gov.ua/e-journals/FP/2010-4/10lamfoz.pdf
49. Ліпкан В. Щодо поняття тероризму / Право України. – 2000. – № 7. – С. 66–69.
50. Ліпкан В.А. Боротьба з тероризмом / В.А. Ліпкан, Д.Й. Никифорчук, М.М. Руденко. – К.: Знання України, 2002. – 254 с.
51. Ліпкан В.А. Тероризм і національна безпека України / В.А. Ліпкан. – К.: Знання, 2000. – 184 с. 40.
52. Лобода С.М., Матвійчук-Юдіна О.В. Метод проектів у формуванні компетентності з інфографіки у майбутніх бакалаврів з кібербезпеки. Проблеми інженерно-педагогічної освіти: зб. наук, праць. 2017. № 54–55. С. 269–277.
53. Луцкий М.Г. Исследование программных средств анализа и оценки риска информационной безопасности/ Луцкий М.Г., Корченко А.Г., Иванченко Е.В., Казмирчук С.В. Захист інформації. – 2011. – №3. – С. 97-108.
54. Луцкий М.Г., Иванченко Е.В., Казмирчук С.В. Базовые понятия управления риском в сфере информационной безопасности. *Захист інформації*. – 2011. – №2. – С. 86-94.
55. Луцкий М.Г., Иванченко Е.В., Корченко А.Г., Казмирчук С.В., Охрименко А.А. Современные средства управления информационными рисками. Защита информации – 2012. – № 1. – С. 5-16.
56. Матула М. М. Феномен інформаційного тероризму як загрози національній та міжнародній безпеці / М. М. Матула. Науковий блог НАУ Острозька Академія Електронний ресурс. URL: http://naub.oa.edu.ua/2014/fenomen-informatsijnoho-teroryzmu-yakzahrozy-natsionalnij-ta-mizhnarodnij-bezpetsi/].

57. Медіа-імперія ІДІЛ. Як терористи виграють війну в соціальних медіа. Дослідження. Texty.org.ua: веб-сайт. URL: https://texty.org.ua/articles/67603/Mediaimperija_IDIL_Jak_terorysty_vygrajut_vijnu_v-67603/
58. Медіатероризм: ІДІЛ обирає Telegram. Mind.ua: веб-сайт. URL: https://mind.ua/news/20172618-mediaterorizm-idil-obirae-telegram
59. Мірошниченко Б. Чому ІДІЛ продовжує існування: терористи будують медіаімпері: веб-сайт – 2020. – URL: https://24tv.ua/idil-teroristi-zalyakuyut-svit-cherez-media-ta-sotsmerezhi_n1429314.
60. Місюра А.О. Іноземний досвід протидії тероризму: висновки для України. Аналітична записка. веб-сайт. URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/inozemniy-dosvid-protidii-terorizmu-visnovki-dlya-ukraini (дата звернення : 03.09.2021)
61. Мобільна революція і епоха бездротового Інтернету в країнах Африки. Все про Африку: веб-сайт. URL: https://africaners.com/uk/afrikans-kij-pobut/mobil-na-revolyutsiya-i-epoha-bezdrotovogo-internetu-v-krayinah-afriki/bezdrotovogo-internetu-v-krayinah-afriki/
62. Перспективы «Исламского государства»/ В.В. Евсеев, Ю.Н. Зинин. *Обозреватель -Observer*. – 2015. – № 2 (301). – С. 43 – 56.
63. Петрищев В.Е. Заметки о терроризме. В.Е.Петрищев – М.: Эдиториал УРСС, 2001. – С.11.
64. Про боротьбу з тероризмом: Закон України від 31 травня 2005 р. Відомості Верховної Ради України. 2005. № 25. Ст. 335. (зі змінами 17.06.2020 №720-9, №47, ст.408): Електронний ресурс. URL: https://zakon.rada.gov.ua/laws/show/en/2600-15/ed20110519#Text
65. Про основні засади забезпечення кібербезпеки України : Закон України № № 2163-VIII від 05.10.2017 р. Відомості Верховної Ради (ВВР). 2017. № 45. Ст. 403. Електронний ресурс. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

66. Проблемы и особенности борьбы с террористической группировкой Исламское государство. Зарубежное военное обозрение. – 2016. – № 6 (831). – С. 3 – 13.
67. Проблемы и особенности борьбы с террористической группировкой Исламское государство. Зарубежное военное обозрение. – 2016. – № 6 (831). – С. 3 – 13.
68. Ризики тероризму та сепаратизму. Державна служба фінансового моніторингу України: 2017. 84 ст.
69. Румія (журнал) - Rumiyah (magazine) – 2021: веб-сайт. – URL: https://uk.wikihol.ru/wiki/rumiyah(magazine).
70. Сайт 8chan, популярный у экстремистов, отправили в нокдаун. Куда уходят пользователи? - BBC News Русская служба: веб-сайт. URL: https://www.bbc.com/russian/features-49267635
71. Сапсай А. П. Участь ЄС у врегулюванні конфліктів на африканському континенті / А. П. Сапсай, М. К. Манташян. Гілея: науковий вісник. - 2013. - № 72. - С. 921-927. URL: http://nbuv.gov.ua/UJRN/gileya_2013_72_180.
72. Сім речей, про які я дізнався, прочитавши всі випуски журналу Ісламської держави. Texty.org.ua: веб-сайт. URL: https://texty.org.ua/articles/63491/7_rechej_pro_jaki_ja_diznavsa_prochytavshy-63491/
73. Словник іншомовних слів / За ред. О.С. Мельничука. – К.: Головна редакція Української енциклопедії АН УРСР, 1975. – 775 с.
74. Социальные сети: новые возможности или угрозы? / Н.П. Ромашкина, Т.И. Фоминых. Информационные войны. – 2017. – № 3 (43). – С. 16-27.
75. Соціальні мережі як інструмент взаємовпливу влади та громадянського суспільства / О. С. Онищенко, В. М. Горовий, В. І. Попик та ін.; НАН України, Нац. б-ка України ім. В. І. Вернадського. – К., 2014. – 295 с.

76. Сучаний словник іншомовних слів: Близько 20 тис. слів і словосполучань / Уклад : О.І. Скопенко, Т.В. Цимбалюк.-К.: Довіра,2006.-789 с
77. Сучасний навчально-методичний інструментарій. Сервіси Web 2.0 в побудові ефективного уроку. Електронний ресурс. URL: http://dvpub.dp.ua/content/load_files/141.pdf
78. Схеми: Використання збору коштів для фінансування тероризму із застосуванням соціальних мереж. Академія соціального моніторингу: веб-сайт. URL: https://finmonitoring.in.ua/vikoristannya-zboru-koshtiv-dlya-finansuvannya-terorizmu-iz-zastosuvannyam-socialnix-merezh/ (дата звернення : 03.09.2021)
79. Тёрнер Дж. Мастерство SMM-кампании талибов* в социальных сетяхпоразило аналитиков США. REGNUM: веб-сайт. URL: https://regnum.ru/news/polit/3347751.html.
80. Тероризм: кримінологічна детермінація і кримінально-правова протидія: монографія / В. В. Середа, І. Р.Серкевич; за заг. ред. В. С. Канціра. – Львів: ЛьвДУВС, 2016. – 188 с.
81. Тероризм: теоретико-прикладні аспекти: навчальний посібник / кол. авторів; за заг. ред. проф. В.К. Грищука. – Львів: ЛьвДУВС, 2011. – 328 с.
82. Терористи «Ісламської держави» на випадок відродження створили «резервну копію» ІДІЛ. У архіві чотири тисячі папок з інструкціями, як робити бомби та викрадати літаки – переказуємо матеріал Wired: веб-сайт. URL: https://babel.ua/texts/50898-teroristi-islamskoji-derzhavi-na-vipadok-vidrodzhennya-stvorili-rezervnu-kopiyu-idil-u-arhivi-chotiri-tisyachi-papok-z-instrukciyami-yak-robiti-bombi-ta-vikradati-litaki-perekazuyemo-material-wired
83. Террористический халифат как квазигосударство: проблема концептуализации. Полития: Анализ. Хроника. Прогноз. 2020. № 2 (97). С. 87-103.
84. Требин М.П. Терроризм в XXI веке. Мн.: Харвест, 2004. 665 с.

85. Турчин А. В. Класифікація соціальних мереж. Матеріали всеукраїнської наук.-практ. конференції. Кіровоградський національний технічний університет. м. Кропивницький, 2016. – 206 с.
86. Указ Президента України від 7 червня 2016 року № 242 «Про Національний координаційний центр кібербезпеки» (зі зміною, внесеною Указом від 19 червня 2019 року № 415): Електронний ресурс. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text
87. Указ Президента України Про рішення Ради національної безпеки і оборони України Від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Електронний ресурс. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text
88. Фейсбук заявляє, що видалятиме пов'язаний з талібами контент. веб-сайт. URL: https://www.ukrinform.ua/rubric-world/3298979-facebook-zaavlae-so-vidalatime-povazanij-z-talibami-kontent.html (дата звернення : 03.09.2021)
89. Хоффман Б. Терроризм: взгляд изнутри / Брюс Хоффман. М.: Ультра; Культура, 2003. С. 640
90. Чеканова П.В. Соціальна платформа Twitter як інструмент сучасної інформаційної війни: Зб.мат. міжнародної наук.-практ. конф. «Сучасні міжнародні відносини: актуальні проблеми теорії і практики». ФМВ НАУ; за загальною редакцією Ю. О. Волошина: Київ, 2021. С. 193-198.
91. Шульман О. Соціальні мережі як зброя. Соціальні мережі: веб-сайт. URL: https://armyinform.com.ua/2020/03/soczialni-merezhi-yak-zbroya/ (дата звернення : 03.09.2021)
92. 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

English:

93. Abidemi. Olabode S., «A Preliminary Overview of ICT Use in the Boko Haram conflict: A Cyberconflict Perspective», Contemporary Voices 1 no. 1 (2018): p.43.
94. Archetti, C. (2015). Terrorism, Communication and New Media: Explaining Radicalization in the Digital Age.
95. Berkowitz S.D. Social structures: a Network approach / S.D. Berkowitz, B. Wellman. – Cambrige : Cambrige University Press, 1988. – 513 p.
96. Carley, Kathleen. (2017). Social Influence, Bots, and Fake News. Presentation to the Security, Networks, and Social Computing Working Group.
97. Chekanova P.V. Social networks as tool of political manipulation and propaganda: Polit. Challenges of science today. International relations: Kyiv, 2021. Editorial board Lutskyi M. [and others]. — K: NAU, 2021. – p 103-105.
98. Cohen, K., Johansson, F., Kaati, L., & Mork, J. C. (2014). Detecting Linguistic Markers for Radical Violence in Social Media. Terrorism and Political Violence, 26(1), 246–256. URL: https://doi.org/10.1080/09546553.2014.849948
99. Conway, M. (2017). Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research. Studies in Conflict & Terrorism, 40(1), 77–98. URL: https://doi.org/10.1080/1057610X.2016.1157408
100. Cox. Kate, Marcellino. Williams, Bellasio. Jacopo and Ward. Antonia, «Social media in Africa, a Double-edged Sword for Security and Development Research» UNDP 23, URL: //www.undp.org/content/dam/rba/docs/Reports/UNDP-RAND-Social-Media-Africa-Research-Report_final_3%20Oct.pd

101. Ette. Mercy and Joe. Sarah, «Rival Visions of Reality»: An analysis of the framing of Boko Haram in Nigerian Newspapers and Twitter, War & Conflict 11 no. 4 (2018): 394 p.

102. Farwell, J. P. (2014). The Media Strategy of ISIS. Survival, 56(6), 49–55. URL: https://doi.org/10.1080/00396338.2014.985436

103. Ganor B. Defining Terrorism: Is One Man's Terrorist Another Man's Freedom Fighter? / B. Ganor. IST Papers on Terrorism. Jerusalem, Israel: The International Polisy Instutute for Counter-Terrorism, The Interdisciplinary Center, Herzliya, Israel. 2002. P. 910.

104. Garth Jowett and Victoria O'Donnell, Propaganda and Persuasion, 4th ed. Sage Publications, 2005. 448 p.

105. How social media is used to encourage travel to Syria and Iraq briefing note for schools. Department for Education and Home Office. 2015. P. 1–5.

106. Jerrold M. From Car Bombs to Logic Bombs : The Growing Threat from Information Terrorism / M. Jerrold. NATO Library at : Terrorism and political violence, vol. 12, no. 2, Summer 2000. – p. 97-122.

107. Jerrold M. From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism / M. Jerrold. NATO Library at: TERRORISM_AND_POLITICAL_VIOLENCE, vol. 12, no. 2, Summer 2000, p. 97-122.

108. Kaplan, A.M. Users of the world, unite! The challenges and opportunities of Social Media / A.M. Kaplan, M. Haenlein. Business Horizons. – 2010. – Vol. 53 (1). – P. 59–68. URL: http://www.michaelhaenlein.eu/Publications/Kaplan,%20Andreas%20-%20Users%20of%20the%20world,%20unite.pdf/

109. Klausen J. Role of Social Networks in the Evolution of Al Qaeda-Inspired Violent Extremism in the United States, 1990-2015. – Brandeis University, 2016. – 71p.

110. Klausen, J. (2015). Tweeting the jihad: social media networks of Western foreign fighters in Syria and Iraq. Studies in Conflict & Terrorism, 38(1), 1–22.

111. Maeghin Alarid. (2015). Recruitment and Radicalization: The Role of Social Media and New Technology. Impunity: Countering Illicit Power in War and Transition, pp. 313–329. Retrieved from http://cco.ndu.edu/Publications/Books/Impunity/tabid/21393/Article/780274

112. Maina Maina. Boko Haram: Buratai Blames Social Media for Endless War. Daily Post, August 17, 2017. URL: https://dailypost.ng/2017/08/17/boko-haram-buratai-blames-social-media-endless-war/

113. Medinat Abdulazeez Malefakis. Social Media Dynamics in Boko Haram's Terrorist Insurgence. Toda Peace Institute. 2019. Policy Brief No. 50. P. 1–15.

114. Molly Kilete. Boko Haram: Again, Army Cautions Troops on Indiscriminate Use of Social Media. Sun News Online, August 26, 2018. URL: https://www.sunnewsonline.com/boko-haram-again-army-cautions-troops-on-indiscriminate-use-of-social-media/

115. Nigeria Internet Users. Internet Live Stats - Internet Usage & Social Media Statistics. URL: https://www.internetlivestats.com/internet-users/nigeria/

116. Nsaibia H. The Digital Transformations of Al-Qaeda and Islamic State in the Battle Against Online Propaganda / H. Nsaibia, R. Lyammouri. Global Network on Extremism & Technology. – 2021. – URL: https://gnet-research.org/2021/05/19/the-digital-transformations-of-al-qaeda-and-islamic-state-in-the-battle-against-online-propaganda/.

117. Ogbondah C.W., Agbese P.O. (2018) Terrorists and Social Media Messages: A Critical Analysis of Boko Haram's Messages and Messaging Techniques. In: Mutsvairo B. (eds) The Palgrave Handbook of Media and Communication Research in Africa. Palgrave Macmillan, Cham.

118. Perspectives on Terrorism 9(1). URL: http://www.terrorismanalysts.com/pt/index.php/pot/article/view/401

119. Rafaeli, S., Ravid, G., Soroka, V. De-lurking in virtual communities : a social communication network approach to measuring the effects of social and cultural capital. URL: http://csdl.computer.org/comp/proceedings/hicss/2004/2056/07/205670203.pdf; http://sheizaf.rafaeli. net/publications/ RRSHICSS37DeLurking1.pdf

120. Social Media Strategies and Online Narratives of Terrorist Organizations; Case studies of Al-Qaeda, ISIS, Taliban and Lashkar-e-Taiba. European Foundation for South Asian Studies. 2020. P. 1–24.

121. Thevenet C. Cyber-terrorisme, mythe ou réalité? / C. Thevenet. Série Mémoires et Thèse. – Université de Marne-La-Vallée. – 2005. – 57 p

122. Thompson, Robin L.. Radicalization and the Use of Social Media. Journal of Strategic Security 4, no. 4 (2012) : 167-190.

123. Thorbecke C. How the Taliban uses social media to seek legitimacy in the West, sow chaos at home. ABC News. URL: https://abcnews.go.com/Technology/taliban-social-media-seek-legitimacy-west-sow-chaos/story?id=79500632.

124. Van Den Ende, B. (2016). Understanding and combatting terrorist networks: Coupling social media mining with social network analysis. In Johnstone, M. (Ed.). (2016). The Proceedings of 14th Australian Information Security Management Conference, 5-6 December, 2016, Edith Cowan University, Perth, Western Australia. (pp.48-51).

125. Van Den Ende, B. Understanding and combatting terrorist networks: Coupling social media mining with social network analysis. In Johnstone, M. (Ed.). *The Proceedings of 14th Australian Information Security Management Conference. – 2016*, pp.48-51.