

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
ЧЕРНІВЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ  
ІМЕНІ ЮРІЯ ФЕДЬКОВИЧА**

**Факультет історії, політології та міжнародних відносин  
Кафедра міжнародних відносин та суспільних комунікацій**

**СОЦІАЛЬНІ МЕДІА ЯК ІНСТРУМЕНТ ВПЛИВУ  
В ДІЯЛЬНОСТІ ТЕРОРИСТИЧНИХ ОРГАНІЗАЦІЙ:  
ЗАГРОЗИ ТА ВИКЛИКИ СУЧАСНІЙ МІЖНАРОДНІЙ БЕЗПЕЦІ**

**Кваліфікаційна робота**

**Рівень вищої освіти – другий (магістерський)**

***Виконав:***

*студент 6 курсу, групи 604*

**Кувік Степан Володимирович**

***Керівник:***

*Кандидат історичних наук,*

**доцент Звоздецька О. Я.**

*До захисту допущено  
на засіданні кафедри  
протокол № \_\_\_\_\_ від \_\_\_\_\_ 2022 р.  
Зав. кафедри \_\_\_\_\_ проф. Фісанов В. П.*

**Чернівці – 2022**

### *Анотація*

**Кувік С. В. Соціальні медіа як інструмент впливу в діяльності терористичних організацій: загрози та виклики сучасній міжнародній безпеці.**

*Наукова робота присвячена дослідженню питання соціальних медіа як інструменту впливу в діяльності терористичних організацій в контексті загроз та викликів сучасній міжнародній безпеці. Зокрема, досліджено сутність понять «соціальні медіа» та «медіатероризм», проаналізовано трансформаційні процеси медіатероризму, продемонстровано діяльність в медіапросторі терористичних організацій «Ісламська держава» та Аль-Каїда, розглянуто розроблені в міжнародних організаціях ООН, ЄС, ОБСЄ механізми протидії медіатероризму. Зроблено висновок про необхідність поглибленого розуміння ролі Інтернет-технологій у діяльності терористичних організацій, розробки більш дієвих механізмів протидії медіатероризму.*

**Ключові слова:** соціальні медіа, медіатероризм, медіаконтент, комунікативний вплив, «Ісламська держава», Аль-Каїда.

### *Annotation*

**Kuvik S. Social media as a tool of influence in the activities of terrorist organizations: threats and challenges to modern international security.**

*The scientific work is devoted to researching the issue of social media as a tool of influence in the activities of terrorist organizations in the context of threats and challenges to modern international security. In particular, the essence of the concepts of “social media” and “media terrorism” was investigated, the transformational processes of media terrorism were analyzed, and the activities of terrorist groups in the media space were demonstrated.*

*Organizations "Islamic State" and Al-Qaeda, the mechanisms for countering media terrorism developed in the international organizations of the UN, the EU, and the OSCE were considered. A conclusion was made about the need for a deeper understanding of the role of Internet technologies in the activities of terrorist*

*organizations and the development of more effective mechanisms for countering media terrorism.*

**Keywords:** *social media, media terrorism, media content, communicative influence, "Islamic State", Al-Qaeda.*

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів наукових досліджень інших авторів мають посилання на відповідне джерело.

\_\_\_\_\_ С. Кувік

## ЗМІСТ

	<b>С.</b>
<b>ВСТУП</b> .....	5
<b>РОЗДІЛ 1. КОНЦЕПТУАЛЬНО-ТЕОРЕТИЧНИЙ АСПЕКТ ДОСЛІДЖЕННЯ</b> .....	9
1.1. Сутність і зміст понять «соціальні медіа», «медіатероризм».....	9
1.2. Стан джерельної бази дослідження .....	17
<b>РОЗДІЛ 2. МЕДІАТЕРОРИЗМ: ЗАГРОЗИ ТА ВИКЛИКИ СВІТОВОМУ СПІВТОВАРИСТВУ</b> .....	26
2.1. Трансформаційні процеси медіатероризму на початку ХХІ століття...	26
2.2. Зростання медіатероризму як глобальної загрози міжнародної інформаційної безпеки .....	36
<b>РОЗДІЛ 3. СОЦІАЛЬНІ МЕДІА ЯК ІНФОРМАЦІЙНА ЗБРОЯ ТЕРОРИСТИЧНИХ ОРГАНІЗАЦІЙ</b> .....	48
3.1. Медіаконтент «Ісламської держави»: зміст, види та форми.....	48
3.2. Діяльність Аль-Каїди в Інтернет-просторі: форми, види та інструменти.....	58
3.3. Механізми протидії медіатероризму міжнародними організаціями: ООН, ЄС, ОБСЄ .....	65
<b>ВИСНОВКИ</b> .....	84
<b>СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ</b> .....	88
<b>SUMMARY</b> .....	115

## ВСТУП

**Актуальність теми дослідження.** Сплеск терористичних актів на початку ХХІ століття засвідчив, що саме тероризм став основною загрозою миру та безпеки у світі. Глобальний масштаб, постійне нарощування терористичного потенціалу, активне використання терористами інформаційно-комунікативних технологій (далі - ІКТ) і, як результат, демократизація («використання таких досягнень ІКТ, як Інтернет та смартфон, за допомогою яких сьогодні можна виготовити зброю та організувати терористичний акт, знизили бар'єри для участі у терористичній діяльності» [82]) – ось основні характеристики сучасного тероризму та екстремізму.

Особливого значення у контексті діяльності терористичних організацій набувають соціальні медіа як інформаційна зброя. У порівнянні з традиційними засобами масової інформації (далі – ЗМІ), які терористи використовували, головним чином, для інформування про власну діяльність, соціальні медіа мають низку переваг: зручність у використанні (найменші фінансові та фізичні затрати), доступність (не обмежені ні в часі, ні в просторі), значне охоплення цільової та вікової аудиторії (широка доступність до Інтернет-мережі різних вікових груп), наявність комунікативного зв'язку (взаємне спілкування) тощо. А отже, як бачимо, є доволі багато причин, що сприятимуть широкому використанню терористами соціальних медіа як інструментів впливу у своїй діяльності, як засобів для досягнення власних цілей та намірів.

Поширення соціальних медіа та дешевих цифрових технологій сприяли зміні напрямку та механізмів взаємодії терористичних організацій (далі – ТО) із ЗМІ. Сьогодні терористи активно використовують соціальні медіа (соціальні мережі, Інтернет, онлайн-платформи, месенджери тощо) не тільки як засіб інформування та комунікації, але й як інструмент для розповсюдження насильницької пропаганди та екстремістських настроїв (і як результат - поширення серед населення відчуття страху та паніки), привернення максимальної уваги світу, як джерело вербування та навчання прибічників, фінансування власних організацій (при чому доволі значні фінанси

витрачаються не тільки на підготовку та здійснення терористичних актів, але й на створення та підтримку медійної складової ТО), самореклами тощо. Як бачимо, активне використання ТО соціальних медіа забезпечило активізацію та поширення насильницької пропаганди, просування екстремістських поглядів та ідей при найменших витратах та ризиках.

У зазначеному контексті слід звернути увагу на площину взаємовідносин ТО – МЕДІА: терористи, головним чином, зацікавлені в соціальних медіа у плані забезпечення висвітлення власної діяльності, поширенні страху і паніки серед мас, розповсюдженні власного впливу, а представники медіа – в оперативному та сенсаційному оприлюдненні інформації, що, у свою чергу, створює нову дилему – гонитва за такими сенсаційними матеріалами та, відповідно, рейтингами може переважити над поданням об'єктивної інформації або над етичними аспектами, що полягають у дотриманні принципів приватності та захисту особистого життя. Як влучно зауважили у своїй публікації експерти міжнародної некомерційної організації «Міжнародна підтримка ЗМІ» (International Media Support (IMS) Гульнара Ахундова (Gulnara Akhundova) та Емма Лігнеруд Боберг (Emma Iygnrud Boberg), «журналістам потрібне співчуття, щоб повідомляти про акти тероризму інформативно, також з повагою до жертв події» [105]. У той же час, в законодавчих документах міжнародних організацій ООН та Ради Безпеки чітко прописана пріоритетність приватності та поваги до особистого життя жертв тероризму.

Як бачимо, сьогодні на порядку денному перебуває питання протидії медіатероризму - особливому виду інформаційно-психологічного терору, зміст якого полягає у спланованому використанні соціальних медіа з метою забезпечення психологічного тиску на свідомість мас, що провокує поширення відчуття небезпеки, страху та паніки, нестабільності, невдоволення мас щодо діяльності державних та правоохоронних органів тощо.

Отже, в умовах активного розвитку ІКТ та всеохоплюючих процесів діджиталізації питання використання терористами соціальних мереж та онлайн-платформ набуває значної актуальності та потребує поглибленого дослідження,

а особливо – для визначення ролі соціальних медіа в діяльності терористичних організацій з метою розробки механізмів та засобів протидії медіатероризму. Водночас, у зазначеному контексті важливим є той фактор, що соціальні медіа можна використовувати й як інструмент для боротьби з самим тероризмом.

Таким чином, в умовах активного використання ТО соціальних медіа як своєрідної зброї, яка становить загрозу міжнародній інформаційній безпеці, актуальності набувають питання розробки механізмів з упередження поширення в соціальних медіа терористичного контенту. Важливе значення мають досвід та вжиті заходи міжнародними організаціями ООН, ЄС, ОБСЄ у напрямку боротьби з обмеженням поширення терористичного контенту та вжиття упереджувальних заходів: від створення дискусійних онлайн-платформ, сприяння співпраці державного, правоохоронного, громадського та приватного секторів до розробки міжнародно-правової бази та законодавчих ініціатив тощо. При цьому у центрі уваги залишаються питання забезпечення невторчання у приватне життя, свободу думки, збереження вільного та безпечного обміну інформацією у мережі.

**Мета дослідження:** на підставі аналізу стану використання у своїй діяльності терористичними та екстремістськими організаціями соціальних медіа виявити та проаналізувати виклики і загрози міжнародній безпеці, сформулювати можливі шляхи попередження та поширення медіатероризму.

Досягнення мети дослідження вимагає постановки та розв'язання **наступних завдань:**

- дослідити теоретичні та концептуальні засади понять «соціальні медіа», «медіатероризм»;
- проаналізувати трансформаційні процеси медіатероризму на початку XXI століття;
- з'ясувати фактори впливу на зростання медіатероризму як глобальної загрози міжнародної інформаційної безпеки;
- дослідити зміст, види та форми медіа контенту ІД, а також форми, види та інструменти діяльності Аль-Каїди в Інтернет-просторі;

- розкрити механізми протидії медіатероризму міжнародними організаціями ООН, ЄС, ОБСЄ.

**Об'єктом дослідження** є медатероризм як глобальна загроза міжнародній інформаційній безпеці.

**Предметом дослідження** - соціальні медіа як інструмент впливу у діяльності терористичних організацій.

**Методи дослідження:** Для розкриття предмету дослідження магістерської роботи автором використано певні загальнонаукові та спеціальні методи, зокрема: порівняльний та історичний методи, метод аналізу, індукції та дедукції, метод узагальнення.

**Структура роботи** зумовлена метою, об'єктом, предметом та завданням дослідження. Вона складається із вступу, трьох розділів, висновків та списку використаних джерел (183 найменування). Загальний обсяг 113 сторінок.



## РОЗДІЛ 1. КОНЦЕПТУАЛЬНО-ТЕОРЕТИЧНИЙ АСПЕКТ ДОСЛІДЖЕННЯ

### 1.1. Сутність і зміст понять «соціальні медіа», «медіатероризм»

Події ХХІ століття засвідчили, що саме тероризм став глобальною загрозою сучасній міжнародній безпеці. Сьогодні ТО вбачають першочергове та актуальне завданням у забезпеченні своєї максимальної присутності не тільки у практичній сфері (відбулось значне зростання кількості та впливовості терористичних актів у світі), а й у світовому інформаційному просторі (активізація діяльності терористів у напрямку забезпечення власного комунікативного впливу). Саме з цією метою ТО активно використовують соціальні медіа, які стали не тільки майданчиком для онлайн-комунікування терористів, але й справжньою зброєю у досягненні ними власних намірів та цілей. У той же час, у будь-якому цивілізованому суспільстві саме ЗМІ несуть основну відповідальність за формування та демонстрацію громадської думки.

При дослідженні питання соціальних медіа як інструментів впливу в діяльності ТО, власне поняття «тероризму» розглядатиметься нами не тільки, як дія, але й як комунікативний акт, метою якого є прагнення та наміри терористів за допомогою соціальних медіа поширити серед масової аудиторії пропаганду залякування та насилля, забезпечити вербування та навчання своїх прихильників, розширення фінансової бази тощо. Як зауважив американський дослідник Брайан Дженкінс (Brian Jenkins), «тероризм спрямований на людей, які спостерігають за ним, як глядачі в театрі» [78, с. 11]. Отже, соціальні медіа в діяльності ТО є своєрідними інструментами, які створюють можливості та умови для здійснення терористичного акту на території будь-якої держави, у будь-який час.

На наш погляд, аргументованим є твердження американського дослідника з питань тероризму Брюса Хоффмана (Bruce Hoffman), який наголошував, що «без висвітлення в засобах масової інформації втрачається будь-який вплив самого акту, що залишається обмеженим безпосередніми жертвами нападу, а не

досягає ширшої аудиторії, на яку власне і спрямоване насильство терористів» [111, с. 174]. Сьогодні терористи спрямовують значні зусилля для забезпечення свого «піар-ефекту» [146].

Серед наукової спільноти відсутнє загальноприйняте та уніфіковане трактування термінів «соціальні медіа» та «медіатероризм». Межі вживання зазначених понять розмиті та трактуються дослідниками різних наукових галузей з власних позицій. А отже необхідність чіткого визначення основних понять нашого дослідження не позбавлена актуальності й сьогодні.

Дослідники та експерти медійної сфери соціальні медіа розглядають переважно для позначення нових форм медіа, які безпосередньо стосуються сфери інтерактивної участі. У контексті дискусій щодо соціальних медіа доволі часто науковці та експерти вживають такі терміни, як електронні ЗМІ, цифрові або онлайн-медіа тощо, що пояснюється наявністю широкого переліку каналів передачі інформації. З метою чіткого визначення сутності соціальних медіа необхідно визначити головні ознаки, за якими вони вирізняються з-поміж цілого масиву визначень. На нашу думку, головною такою ознакою є активна участь користувачів у створенні та обігу контенту, яка полягає у його створенні, подальшому редагуванні, коментуванні, оновленні, можливому вилученні або поширенні. У цьому випадку користувач соціальних медіа виступає не тільки споживачем інформації, а створює її, корегує тощо. А отже, соціальні медіа є не тільки джерелом інформування, але й виступають інструментом процесу комунікування.

Інтернет-ресурси подають наступні трактування поняття «соціальних медіа»:

- як «групи Інтернет-додатків, що базуються на ідеологічних та технологічних засадах Web 2.0 і дозволяють створювати та обмінюватися контентом» [72] (на наш погляд, у зазначеному трактуванні акцент зроблено переважно на технічному аспекті);

- як «вид Інтернет-масмедіа, завдяки яким споживачі контенту одночасно виступають і його співавторами (через свої дописи), одночасно взаємодіючи, співпрацюючи та спілкуючись із іншими користувачами певного сервісу» [71].

Вітчизняні дослідники соціальні медіа розглядають з наступних позицій:

- як «засіб комунікації, за допомогою якого користувачі спілкуються, створюють та розповсюджують, а також споживають інформацію» (зокрема, Ю. О. Алексеєнко [29], Н. О. Піпченко [55]);

- як сукупність технологій: зокрема, під соціальними медіа розуміють «сукупність сервісів та онлайн-платформ, які надають можливість користувачам спілкуватись, створювати та поширювати інформацію тощо» [56]; акцент зроблено саме на каналах поширення інформації (зокрема, З. В. Григорова [33], Г. Г. Почепцов [58], Н. В. Покровська, М. М. Федорович та М. О. Щербина [56]).

У той же час українські дослідники В. О. Каплуненко та С. В. Бондаренко, аналізуючи визначення поняття соціальних медіа, подають чотири підходи, доповнивши вищевказані дві позиції наступними:

- «соціальні медіа як соціальна система у віртуальному просторі» (в основі – соціальні мережі) [39, с. 238];

- «соціальні медіа як сукупність інформаційного контенту на сайтах соціальної мережі» [39, с. 239].

В іноземних джерелах соціальні медіа трактуються, головним чином, у прив'язці до віртуального простору. Зокрема, у Кембриджському словнику (The Cambridge Dictionary) під соціальними медіа розуміють «вебсайти та комп'ютерні програми, за допомогою яких користувачі спілкуються в Інтернеті, використовуючи комп'ютерну техніку чи мобільний телефон» [147]. Британська енциклопедія (Encyclopedia Britannica) трактує соціальні медіа як «комунікації в Інтернеті, за допомогою яких користувачі діляться інформацією, ідеями, особистими повідомленнями та іншим вмістом» [144]. Американська компанія – видавець довідників та лексичних словників Мерріам-Вебстер (Merriam Webster) подає таке тлумачення соціальних медіа: «форми

електронного спілкування (такі як вебсайти для соціальних мереж і мікроблоги), за допомогою яких користувачі створюють онлайн-спільноти для обміну інформацією, ідеями, особистими повідомленнями та іншим вмістом» [145].

Зарубіжні науковці, експерти та дослідники у своїх дослідженнях аналогічно акцентують увагу на факті інтерактивної участі. Так, зокрема, під час медіаконференції «Від традиційних до онлайн-медіа: найкращі практики та перспективи», що відбулась у 2012 році у Тбілісі (Грузія) експерт офісу представника ОБСЄ з питань свободи ЗМІ Крістіан Меллер (Khristian Möller) зауважив, що термін «соціальні медіа» відноситься до «використання мобільних та Інтернет-технологій для перетворення комунікації в інтерактивний діалог» [174, с. 21]. Німецький дослідник Штефан Примбс (Stefan Primbs) поняття «соціальні медіа» трактує як «онлайн-сервіси, за допомогою яких користувачі обмінюються інформацією чи думками або ж спільно їх напрацьовують» [59, с. 14]. Американський консультант з питань SEO-контенту в Search Engine Journal Шеллі Волш (Shelley Walsh) зауважує, що соціальні медіа – це «цифрові платформи, які дозволяють взаємодіяти з користувачем і ділитися створеним ним вмістом через онлайн-програму для мережових цілей» [139]. Як бачимо, зарубіжні дослідники розглядають соціальні медіа у контексті цифрових платформ, які забезпечують взаємодію (обмін інформацією) користувачів онлайн-сервісів.

Узагальнюючи все вищезазначене, констатуємо, що соціальні медіа – це цифрові інструменти, які дозволяють створювати та поширювати, оновлювати та корегувати інформацію, документи, зображення та відео, при одночасному активному використанні ІКТ та соціальної взаємодії. До соціальних медіа належать вебсайти, онлайн-платформи, соціальні мережі, блоги, підкасти тощо. Отже, на відміну від звичайних ЗМІ, соціальні медіа поєднують цифрові платформи та Інтернет-комунікацію, забезпечують онлайн-зв'язок автора контенту з його споживачем.

В умовах активного розвитку ІКТ, всеохоплюючого процесу діджиталізації актуальність та роль соціальних медіа зростає. За даними Глобальної статистики соціальних медіа, станом на 2022 рік у всьому світі нараховувалось 4,95 мільярда користувачів соціальних мереж (що становить 58,4% загального населення світу), а рівень проникнення в Інтернет становить 62,5% від загальної кількості населення світу [140]. У той же час, встановлено, що у середньому типовий користувач Інтернету зараз проводить понад 40 % свого життя, використовуючи підключені пристрої та служби [141]. Як бачимо, глобальна мережа Інтернет сьогодні є найбільш затребуваною, розповсюджуваною платформою серед населення. До того ж користувачі соціальних мереж, як правило, молодого віку, які достатньо обізнані із ІКТ: майже 90% осіб у віці від 18 до 29 років [127]. Аналогічна ситуація склалась й в Україні. Зокрема, за результатами презентованого 5 жовтня 2021 року дослідження «Медіаспоживання та аналіз аудиторії в Україні», що провів Фонд Томсон Рейтер (Thomson Reuters Foundation) – благодійна організація канадського новинного конгломерату «Thomson Reuters» у партнерстві з BBC Media Action, встановлено, що найпопулярнішими джерелами новин та інформації в Україні є пошукові системи (щодня їх використовують 80% респондентів) та соціальні медіа (72%) [68].

В інформаційному суспільстві соціальні медіа розвиваються та вдосконалюються. З'являються нові додатки та мережі, що, у свою чергу, створює умови для розширення інформаційних можливостей користувачів соціальних мереж та веб-сайтів.

У контексті зростання впливовості соціальних медіа актуальності набувають питання їх активного використання ТО. Так, доцільно виокремити наступні характерні особливості соціальних медіа у цьому контексті:

- 1) соціальні медіа формують інформаційний блок про діяльність ТО (оприлюднюють інформацію різного походження (авторства) щодо діяльності терористів; функція інформування);

2) соціальні медіа – один з інструментів формування громадської думки щодо ТО (потік інформації про діяльність ТО, їх характеристики та ознаки формує загальне уявлення світової спільноти про терористів);

3) соціальні медіа як зброя ТО (як засіб здійснення терористичних актів, інструмент вербування та навчання прихильників).

Грунтовний аналіз кожного напрямку сприятиме розробці ефективних заходів та механізмів, які обмежать можливості використання соціальних медіа у терористичних цілях.

На початковому етапі взаємодії ТО та ЗМІ головна увага акцентувалась саме на донесенні інформації про акти насильства до більш ширшої аудиторії з метою посилення їх ефекту. Як влучно підкреслила таку особливість взаємовідносин тероризму і ЗМІ експерт Центру аналізу та міждисциплінарних досліджень медіа (CARISM) Паризького університету (Centre d'Analyse et de Recherche Interdisciplinaires sur les Médias (CARISM) Université Paris) Маргеріт Бореллі (Marguerite Borelli), охарактеризувавши це як «пропаганду вчинку» [126]. Сьогодні терористи, усвідомивши значення та силу сучасних соціальних медіа, посилили маніпулювання ними для досягнення власних цілей. Зокрема, найбільш потужні терористичні організації «Ісламська Держава» (Islamic State) та Аль-Каїда (Al-Qaida), взявши на озброєння соціальні медіа, доклали максимум зусиль для посилення своїх позицій у ніші глобальної світової уваги, розширення з їх допомогою власної бази шляхом вербування та навчання прихильників, активізації закликів до здійснення терористичних атак тощо. Це засвідчив Глобальний індекс тероризму 2020 та 2022 років. Зокрема, констатовано, що шляхом висвітлення в соціальних медіа своєї діяльності ТО посилюють власний вплив [20, с. 77], а також сприяють радикалізації колишніх та нинішніх членів ТО, їхніх прихильників [21, с. 67]. А отже, у зазначеному контексті слід вести мову про таке явище, як медіатероризм.

Вже наприкінці ХХ століття терористичні акти опинились у центрі уваги світової глядацької аудиторії, отримали можливість онлайн-трансляції в

реальному часі з подальшим її повторенням. ІД активно перейняла модель, яка використовує соціальні медіа як «шлях до краудсорсингу тероризму» [79, с. 24].

Поняття «медіатероризму» розглядається дослідниками як вид інформаційно-психологічного тероризму, спрямованого на цільову аудиторію, який покликаний поширити в інформаційному просторі дезінформацію, що спровокує у глядача або слухача відчуття страху та тривоги, небезпеки, невдоволення щодо забезпечення державними та правовими органами захисту населення. Українські дослідники розглядають поняття «медіатероризму» як інформаційно-психологічного тероризму: «важливий інструмент негативного психологічного впливу на громадську думку завдяки активному використанню можливостей сучасних соціальних медіа» (Р. О. Банк [30], А. В. Ілляшенко [38], Д. В. Кіслов [41], Б. Д. Леонова [46, 47], І. В. Царьова [69] тощо). Водночас при дослідженні цього явища науковці роблять різні акценти. Дослідниця Т. В. Єрохіна звертає увагу на «симбіоз взаємодії ТО та медіа, де одна сторона отримує інформаційний супровід своєї діяльності, а інша – інформаційні приводи та зацікавленість публіки» [35]. Науковець О. В. Саган розглядає «медіа-інформаційний тероризм» як суцільне поняття, у якому «ресурс масмедіа тісно пов'язується з контентом інформаційно-комунікативної сфери людини» [61, с. 16]. На нашу думку, найбільш повноцінно зміст поняття «медіатероризму» обґрунтовує професор Києво-Могилянської академії М. А. Ожеван, який акцентує увагу саме на «зловживаннях медіакомунікативними процесами з метою підризу знаково-символьної системи держави чи суспільства» [51].

У науковому дослідженні ми розглядатимемо медіатероризм як особливий вид інформаційно-психологічного терору з використанням соціальних медіа як інструменту для створення та поширення негативного/терористичного/екстремістського контенту з метою забезпечення психологічного тиску на свідомість мас, що провокує поширення відчуття небезпеки, страху та паніки, нестабільності, невдоволення мас щодо діяльності державних та правоохоронних органів. Медіатероризм представляє собою

«особливий вид терористичної діяльності, що виділений за критерієм використання інструментів досягнення терористами власних цілей» [30, с. 113]. На думку окремих дослідників, саме використання ТО соціальних медіа з метою радикалізації та підбурювання до насильницьких дій є центральним питанням у зусиллях щодо стримування поширення терористичного контенту в Інтернеті.

Поруч із терміном «медіатероризм» доволі часто використовують поняття «інформаційного тероризму» та «кібертероризму». На наш погляд, у зазначених поняттях є чітке розмежування сфери поширення. Інформаційний тероризм передбачає «злочинне використання з метою здійснення терористичних актів та інших насильницьких дій, залякування та психологічного тиску тощо інформаційних систем та мереж» [46, с. 174]. Кібертероризм є різновидом інформаційно-технічного тероризму, зміст якого полягає «у здійсненні інформаційної атаки саме на комп'ютерну мережу та обчислювальні системи, або інші складові інформаційної інфраструктури» [34, с. 61]. Таким чином, інформаційний тероризм охоплює обидва поняття медіатероризму та кібертероризму, та виступає як узагальнюючий термін.



## 1.2. Стан джерельної бази дослідження

На основі аналізу джерельної бази магістерської роботи необхідно відзначити величезну кількість наукових розробок вітчизняних та зарубіжних вчених з питань медіатероризму, використання ТО соціальних медіа як своєрідної зброї, а також наявність значної нормативно-правової бази.

Досліджуючи питання соціальних медіа як інструменту діяльності ТО у контексті загрози сучасній міжнародній безпеці ми систематизували джерельну базу наступним чином:

- наукові розробки вітчизняних та зарубіжних вчених;
- документальна та нормативно-правова база міжнародних організацій ООН, ЄС, ОБСЄ;
- дослідження аналітичних центрів та інформаційних агентств;
- матеріали міжнародних форумів та конференцій.

Проаналізувавши джерельну базу магістерської роботи, необхідно відзначити значну кількість досліджень вітчизняних та зарубіжних науковців з проблематики соціальних медіа як інструменту діяльності ТО. Водночас, наукові розробки носять фрагментарний характер та спрямовані на дослідження окремих аспектів зазначеного питання. Серед публікацій вітчизняних науковців немає фундаментального дослідження, яке б охоплювало теоретично-концептуальний аспект медіатероризму, висвітлення практичних механізмів використання ТО соціальних медіа, аналіз напрямків та механізмів протидії медіатероризму, дослідження нормативно-правової бази щодо упередження використання ТО соціальних медіа у власних цілях тощо.

Серед вітчизняних дослідників, коло наукових інтересів яких окреслено проблемами медіатероризму як різновиду інформаційно-психологічного тероризму, механізмами його протидії слід виокремити праці Р. Банка [30], Т. В. Єрохіної [35, 36, 37], Д. В. Кіслова [41], Б. Д. Леонова [46, 47], О. В. Саган [61], І. В. Царьової [69] та інших. Зокрема, науковці акцентують увагу на тому, що сьогодні медіатероризм представляє собою найбільш розповсюджену форму

міжнародного тероризму, а також є способом ведення інформаційної війни. Цінність наукових розробок дослідників полягає у тому, що вони розглядають проблематику медіатероризму у контексті нинішньої ситуації в Україні в умовах загрози національної безпеки.

Питання розгляду сучасного тероризму як продукту інформаційного суспільства, форм та методів використання терористами соціальних медіа, механізми взаємодії терористів та ЗМІ висвітлені у колективних працях А. В. Саміла, О. В. Повстин, М. Я. Купчак [62], І. М. Сопілко, М. О. Медведєвої, Арів Г. Гулієва, С. Д. Білоцького, О. Н. Буханевича, Д. І. Сіроха, Т. А. Терехової [146]. Науково цінними є запропоновані дослідниками механізми висвітлення тероризму в медіа («спіраль насильства» та «ефект зараження» [146]), а також висновки щодо впливу діяльності ЗМІ на активне поширення тероризму.

Аналіз питання використання соціальних медіа як інформаційної зброї ТО на прикладі ІД та Аль-Каїди, створення ними власних медіаресурсів та медіаконтенту, розгляд механізмів боротьби із поширенням терористичного контенту в соціальних мережах, питання міграції медіаресурсів ТО розглянуті у роботах та публікаціях вітчизняних дослідників О. О. Коренькова [44, 45], П. Мазура [48], І. М. Парфенюк [53] та інших. Науковці обґрунтовують взаємозв'язок між ідеологією та цілями ТО із методами використання медіаресурсів у їхній терористичній діяльності.

Значний масив інформаційного та аналітичного матеріалу з питання медіатероризму, а також проблематики використання ТО соціальних медіа як інструменту терористичної діяльності на прикладах ІД та Аль-Каїди презентовано у дослідженнях та публікаціях зарубіжних вчених та експертів Майкла Джеттера (Michael Jetter), Бріджит Л. Накос (Briggite Nacos), Брюса Хоффмана та інших.

Актуальні питання зв'язків між ЗМІ, громадською думкою та міжнародним тероризмом висвітлені в дослідженнях доктора політичних наук Колумбійського університету Бріджит Л. Накос [79]. Зокрема, науковий інтерес

представляють висвітлені автором питання «електронного тероризму», визначення основних комунікативних цілей у контексті взаємозв'язків медіа та тероризму.

Науковий інтерес при дослідженні проблеми комунікативної взаємодії ТО із ЗМІ представляє монографія американського дослідника тероризму Брайан Дженкінса (Brian Jenkins) «Нескорена нація: пізнавати ворога, зміцнювати себе» («Unconquerable Nation: Knowing Our Enemy Strengthening Ourselves») [78], підготовлена за результатами багаторічної діяльності експерта у корпорації RAND – американського аналітичного центру «Дослідження та розробка» (RAND Corporation («Research And Development»). Зокрема, автор праці у загальному контексті дослідження проблематики міжнародного тероризму аналізує психологічний вплив тероризму через ЗМІ, акцентуючи увагу на тому, що терористичні акти зрежисовані терористами ще й з метою привернення уваги ЗМІ: доволі часто терористи для досягнення власних цілей вимагали надати їм можливість виступити перед представниками ЗМІ. Належну увагу експерт відводить висвітленню питання використання терористами нових технологій, що сприяло формуванню більш «витонченого маркетингу» терористів [78].

Питання щодо рушійних сил тероризму, збройних конфліктів та війн, висвітлення тероризму в ЗМІ та використання останніх терористами для просування власних цілей та ідей становлять коло дослідницьких інтересів науковця Університету Західної Австралії в Перті Майкла Джеттера. При написанні наукової роботи використані матеріали публікацій дослідника, в яких проаналізовано причинно-наслідкові зв'язки висвітлення в ЗМІ терористичних актів із наступними терористичними атаками, а також увагу ЗМІ, присвячену терористичним нападам у всьому світі в період 1998 – 2012 років [130]. Зокрема, дослідник констатує позитивний і потужний вплив висвітлення новинними програмами на наступні атаки Аль-Каїди.

Значний масив інформації з проблематики глобального тероризму подано у наукових працях та публікаціях старшого наукового співробітника Центру

боротьби з тероризмом Військової академії США, професора школи дипломатичної служби Едмунда А. Уолша Джорджтаунського університету США Брюса Хоффмана [110, 111, 113]. У контексті ґрунтового аналізу еволюції тероризму дослідник акцентує увагу на питаннях зростання впливу та стійкості найпотужніших ТО – ІД та Аль-Каїди, при цьому відзначає роль активного використання терористами Інтернету та соціальних мереж. Зокрема, Брюс Хоффман наголошує на тому, що сьогодні зброя терористів – це вже не просто зброя чи бомба, але й «мінікамера, відеокасета, професійно виготовлені комп-акт-диски та DVD-диски, ... портативні та настільні комп'ютери, облікові записи електронної пошти, ... і доступ до Інтернету» [113]. У той же час, науковець при розгляді питання висвітлення американськими ЗМІ терористичних актів, звертає увагу на поширення «рабської відданості термінологічній нейтральності»: уникнення термінів «терористи» та «тероризм», віддаючи перевагу поняттям «партизани» та «опір» [110]. Наукові розробки дослідника викликають зацікавленість й тим, що в них подано значний документальний матеріал, зокрема, висновки та звіти Комісії з розслідування подій 11 вересня тощо.

При розгляді питання механізмів протидії медіатероризму міжнародними організаціями ООН, ЄС, ОБСЄ ми використали основні джерела з офіційними документами міжнародних структур: веб-сайти Європейської комісії (Commission européenne), Агентства Європейського Союзу з питань співробітництва правоохоронних органів (European Union Agency for Law Enforcement Cooperation), Офісу Головного комісара ООН з прав людини (The Office of the High Commissioner for Human Rights), системи офіційних документів ООН (Official Document System), ОБСЄ (OSCE) тощо.

В офіційних актах Генеральної Асамблеї ООН та Ради Безпеки ООН констатовано широке використання терористами нових ІКТ для вербування та підбурювання, фінансування, навчання та планування терористичних атак (Резолюції Ради Безпеки ООН № 1963 від 20 грудня 2010 року [4], № 2129 від 17 грудня 2013 року [5] тощо), наголошено на необхідності протидії

міжнародної спільноти у питаннях використання терористами ІКТ на глобальному рівні (Резолюції Генеральної Асамблеї ООН № 72/284 від 26 червня 2018 року [28], Резолюції Ради Безпеки ООН № 1624 від 14 вересня 2005 року [3], № 2178 від 24 вересня 2014 року [7], № 2354 від 24 травня 2017 року [8] тощо). У той же час необхідно акцентувати увагу на тому, що у вище вказаних документах чітко зазначено, що прийняті на національному рівні політичні та законодавчі заходи з попередження та протидії насильницькому онлайн-контенту повинні відповідати зобов'язанням держав у відповідності з міжнародним правом. Важливе значення у питаннях розробки механізмів протидії медіа тероризму належить прийнятій Резолюцією Генеральної Асамблеї ООН № 60/288 від 8 вересня 2006 року Глобальній контртерористичній стратегії ООН [9, с. 7], яка передбачає співпрацю держав-членів з ООН у питаннях координації зусиль на міжнародному та регіональному рівнях у напрямку боротьби з тероризмом у всіх його формах та проявах в мережі Інтернет.

При написанні магістерського дослідження опрацьовано також законодавчу базу ЄС. Так, у питаннях протидії незаконному та насильницькому контенту в Інтернеті вагомим кроком стала прийнята 24 липня 2020 року Європейською комісією нова Стратегія Союзу безпеки ЄС на період 2020 – 2025 років [15]. Зокрема, серед механізмів протидії було передбачено посилення добровільної співпраці між правоохоронними органами та приватним сектором у напрямку боротьби з неправомірним використанням Інтернету терористами.

У контексті боротьби з розповсюдженням терористичного контенту в Інтернеті неможливо залишити поза увагою схвалений Європарламентом у квітні 2021 року Регламент щодо боротьби з поширенням терористичного контенту в Інтернеті [26]. Слід зазначити, що в акті чітко прописано тлумачення терористичного контенту, окреслено механізм боротьби з його розповсюдженням в Інтернет-мережі, визначено зобов'язання постачальника

послуг щодо видалення або заборони оприлюдненого терористичного контенту.

Значний практичний внесок у питання розробки механізмів та інструментів протидії медіатероризму зробила ОБСЄ. Зокрема, Рішенням Ради Міністрів ОБСЄ №3/04 від 7 грудня 2004 року «Боротьба з використанням Інтернету в терористичних цілях» [10] прописано механізм обміну між державами-членами інформацією про використання мережі Інтернет у терористичних цілях та визначення можливих стратегій боротьби з цією загрозою.

Чіткий механізм боротьби із медіатероризмом, а саме: розширення моніторингів вебсайтів терористичних/екстремістських організацій, налагодження обміну інформацією у рамках ОБСЄ та інших відповідних форумів з питань використання Інтернету для терористичних цілей, прописаний у рішенні Ради Міністрів ОБСЄ №7/06 від 6 грудня 2006 року «Протидія використанню Інтернету у терористичних цілях» [11]. Важливо, що при цьому зроблено наголос на дотриманні міжнародних зобов'язань, норм в галузі прав людини, а також внутрішнього законодавства; рекомендовано залучити інститути громадянського суспільства та приватного сектору до діяльності з попередження та поширення використанню Інтернету у терористичних цілях.

Автором дослідження належну увагу приділено матеріалам, які видані за результатами міжнародних форумів та конференцій із зазначеної тематики, що презентують не тільки фактичний матеріал з питань медіатероризму, а також подають рекомендаційні механізми та інструменти з протидії поширенню терористичного медіаконтенту, боротьби з використанням ТО соціальних медіа з метою реалізації власних намірів та цілей. Так, значний матеріал подано в підготовленій за результатами організованих Управлінням ООН з наркотиків та злочинності у співпраці із Робочою групою з протидії використанню Інтернету в терористичних цілях нарад міжнародного рівня у 2011 році та 2012 році у Відні праці «Використання Інтернету в терористичних цілях» («The use of the Internet

for terrorist purposes») [151]. Зокрема, проаналізовано правову практику у проведенні розслідувань справ щодо використання Інтернету у терористичних цілях, співпраці державних та приватних структур у цьому питанні, надано практичну допомогу з метою сприяння більш ефективному розслідуванню у справах проти терористів, пов'язаних із використанням Інтернету. При цьому особливу увагу відведено питанням необхідності забезпечення дотримання прав та основних свобод людини при розслідуванні таких справ.

При написанні магістерської роботи використані результати досліджень, проведених міжнародними науковими установами, аналітичними центрами, інформаційними агентствами. Зокрема, широкий масив статистичних даних подано у комплексних дослідженнях, підготовлених Інститутом економіки та миру (The Institute for Economics) - Глобальний індекс тероризму 2020 (The Global Terrorism Index 2020) [21] та Глобальний індекс тероризму 2022 (The Global Terrorism Index 2022) [22], які аналізують та формують порядковий рейтинг країн за впливом тероризму. У зазначеному контексті наша увага зосереджена на аналітичних матеріалах щодо впливу пандемії на діяльність терористів, інформаційного рейтингу ТО, ідеологічних цілей терористичних груп та стратегії, які використовують терористи тощо.

Значний обсяг аналітичного та статистичного матеріалу щодо висвітлення медіадіяльності та змісту медіаконтенту найпотужніших ТО – ІД та Аль-Каїди подано у дослідженнях Інституту стратегічного діалогу (Institute for Strategic Dialogue (ISD) [103] та Міжнародного центру вивчення радикалізації (International Centre for the Study of Radicalisation (ICSR) [81]. Зокрема, при написанні наукової роботи ми використали результати дослідження Міжнародного центру вивчення радикалізації щодо кількісних та якісних показників, а також тематичного складу офіційної медіапродукції ЗМІ ІД. Так, доведено, що в умовах територіальних та фізичних втрат ТО змінювала наративи власного медіаконтенту, перемістивши основний акцент з висвітлення пропаганди власного управління на військову тематику.

Результати проведеного Інститутом стратегічного діалогу дослідження щодо облікових записів ТО в соціальних мережах доводять, що, зокрема, пов'язані з мережею ІД облікові записи знаходять способи уникнути їхнього виявлення та блокування в соціальних мережах (зокрема, змішують власні матеріали з новинними матеріалами офіційних вебресурсів, наповнюють текст повідомлення зайвими літерами тощо).

Також використано аналітичні та статистичні матеріали американського аналітичного центру RAND Corporation [148]. Зокрема, за результатами вивчення втрат, спричинених тероризмом в країнах ЄС у 2004 – 2016 роках, констатовано, що значний психологічний вплив на масову свідомість здійснює також саме висвітлення в соціальних медіа терористичних актів: навіть ті, хто не є безпосереднім учасником цих подій, все одно зазнає психологічного впливу.

Для написання наукової роботи ми також використали матеріали міжнародних форумів, конференцій та зустрічей: Глобального Інтернет-форуму з протидії тероризму (Global Internet Forum to Counter Terrorism) [175] (щодо розробки механізмів запобігання поширенню екстремістського та терористичного контенту в Інтернеті), Виконавчого директорату Контртерористичного комітету (The Counter-Terrorism Committee Executive Directorate (CTED) (щодо наслідків впливу пандемії COVID-19 на терористичну загрозу) [149] тощо.

Значний обсяг аналітичної інформації ми отримали при опрацюванні матеріалів незалежних досліджень, проведених Британським центром поведінкових та соціальних досліджень загроз безпеці (Centre for Research and Evidence on Security Threats (CREST) [86], які надають можливість проаналізувати механізми використання ТО сучасних інформаційно-комунікаційних технологій у контексті поширення власної пропаганди, самореклами, розширення фінансової бази, вербування нових членів ТО тощо, дослідити медіаконтент ТО, з'ясувати форми та види діяльності ТО в



інформаційному просторі, проаналізувати наслідки впливу терористичного медіаконтенту на світову спільноту.

## РОЗДІЛ 2. МЕДІАТЕРОРИЗМ: ЗАГРОЗИ ТА ВИКЛИКИ СВІТОВОМУ СПІВТОВАРИСТВУ

### 2.1. Трансформаційні процеси медіатероризму на початку XXI століття

Початок XXI століття - своєрідна точка відліку, коли міжнародний тероризм набув рис глобальної загрози міжнародній безпеці. Цьому певною мірою сприяв стрімкий розвиток ІКТ, який кардинально вплинув на зміну інформаційного інструментарію терористичних організацій. Так, традиційні ЗМІ (преса, телебачення, радіо) посіли вторинне місце, а в активний ужиток увійшли саме соціальні медіа (соціальні мережі, месенджери, інші онлайн-платформи тощо). Про актуальність питання щодо інтенсивного використання мережі Інтернет терористами заявляли учасники Економічного форуму в Давосі у 2019 році під час дискусії «Еволюція тероризму: як суспільство та інституції адаптуються» [93]. Зокрема, вони звернули увагу на той факт, що у контексті прагнення терористів до глобального панування вони активно ввели в ужиток нові цифрові досягнення, які спростили процес планування та координування власних дій, набору та навчання нових членів тощо.

Оскільки основна увага дослідження акцентована саме на питаннях зв'язку ТО із соціальними медіа як інструменту для здійснення маніпулятивного впливу на громадську думку, вербування та підготовку прихильників тощо, то основна увага акцентуватиметься саме на понятті медіатероризму як форми міжнародного тероризму в інформаційній сфері та його наслідків для міжнародної безпеки.

Члени ТО продемонстрували «передові навички користування Інтернетом та новими комунікаційними технологіями» [176]. Вони активно використовують задля власної користі соціальні медіа, текстові повідомлення, найновіші досягнення в Інтернеті. Терористи справді оволодівають навичками користування соціальними медіа, здатні адаптуватись до мінливих умов та середовища з метою реалізації власних цілей. Свідченням цього є факт оприлюднення ісламським екстремістом Лароссі Абалла (Larossi Abballa) у

червні 2016 року у Facebook відео, в якому останній присягнув на вірність лідеру ІДІЛ та закликав мусульман до джихаду проти невірних, а також погрожував перетворити Євро-2016 «на цвинтар» [155]. Це відео екстреміст опублікував з будинку поліцейського в Маньяньвілі (Франція), у вбивстві якого разом з дружиною він зізнався під час онлайн-трансляції. Facebook видалив зі своєї мережі оригінал відео терориста. У той же час воно також було оприлюднено на пов'язаному з ІДІЛ сайті інформаційного агентства «Аmaq».

Сьогодні соціальні медіа в руках ТО виступають не лише як засіб інформування світової спільноти про планування та виконання терористичного акту та його наслідків, але й як засіб, за допомогою якого терористи намагаються привернути до себе максимальну увагу світу, як до потужної та жахливої сили, з вимогами якої треба рахуватися. Про вагому роль Інтернету у поширенні терористичних та екстремістських настроїв свідчить і стрілянина в Крайстчерчі (Нова Зеландія) 15 березня 2019 року, у результаті якої озброєний чоловік вбив у двох мечетях 51 людину [121]. Про свої наміри терорист сповістив у Twitter та на форумі 8chat за декілька хвилин до стрілянини, яку потім транслював онлайн у Facebook, пізніше ці кадри були відтворені на YouTube, Twitter та Reddit [121]. Платформи намагались швидко видалити кліпи, хоча доволі швидко з'являлись їхні копії. Інформаційне агентство «The New York Times» сповістило світову спільноту про «масове вбивство Інтернету та заради нього» [121]. Саме це жахливе вбивство стало поштовхом до оголошення прем'єр-міністром Нової Зеландії Джасіндом Ардерном (Jacinda Ardern) і президентом Франції Еммануелем Макроном (Emmanuel Macron) Крайстчерчського заклику (The Christchurch Call) – добровільної глобальної обіцянки знищити терористичний та насильницький контент в Інтернеті [168]. Зазначена спільнота об'єднала 120 урядів, технологічних компаній, організацій громадянського суспільства, колективними зобов'язаннями яких було визначено, зокрема, розробку технічних рішень для запобігання завантаженню, виявлення та негайного видалення терористичного та насильницького контенту в Інтернеті, підтримка дослідницьких та академічних зусиль у цьому напрямку,

забезпечення належної співпраці з правоохоронними органами з метою переслідування незаконної онлайн-діяльності щодо виявленого або видаленого терористичного та насильницького контенту відповідно до принципів верховенства права та захисту прав людини.

Саме шляхом трансляції в онлайн-режимі сцен вбивств та катувань терористи намагаються ввести світову спільноту у стан паніки, відчуття страху, постійної тривожності, що, за ланцюговою реакцією, цілком ймовірно може викликати невдоволення самого населення діяльністю та політикою органів влади, а також правоохоронних органів щодо належного забезпечення захисту населення та забезпечення стану безпеки. Саме з цією метою у серпні 2015 року ІД оприлюднила на YouTube та Twitter відео та фото страти американського журналіста Джеймса Фолі, які були миттєво розтиражовані тисячами користувачів соціальних мереж і тисячі цих твітів стали вірусними [135]. Як свідчать результати проведеного на замовлення Європейського парламенту дослідження RAND Europe щодо втрат, спричинених тероризмом в ЄС між 2004 та 2016 роками, широке висвітлення терористичних атак в соціальних медіа привело до «показового зростання кількості очевидців терактів, які, хоч і не були учасниками таких нападів, зазнавали психологічного впливу та змінювали свою поведінку» [148]. А отже, як справедливо зазначено в дослідженні Глобального індексу тероризму 2022, «Інтернет та соціальні мережі можна вважати соціальним динамітом» [22, с. 76].

Соціальні медіа в руках ТО виступають і як своєрідний засіб тиску на владні кола країн. Так, під час захоплення бойовиками Народного фронту звільнення Палестини 22 липня 1968 року літака ізраїльської авіакомпанії Ель-Аль з вимогою звільнення палестинських терористів з ізраїльської в'язниці, вони фактично змусили уряд Ізраїлю зв'язатися з ними напряму [122]. У той же час, слід зауважити, що показовість таких нападів та ефект, який вони викликають, можуть стати для інших терористичних та екстремістських груп, свого роду, поштовхом до їх наслідування, оскільки в переважній більшості сприймається ними як посилення значення їхньої діяльності.

Активному використанню терористами соціальних медіа сприяли ряд факторів, серед яких можемо виокремити: оперативність донесення інформації до світової спільноти, можливість зацентувати на собі глобальну увагу, отримання онлайн-платформи для спілкування з прихильниками (найефективніший метод комунікацій), відносно низькі витрати при використанні соціальних медіа, забезпечення значного ступеню анонімності користувачів, популярність та поширеність соціальних медіа, а також оприлюднення значного масиву інформаційного матеріалу. Як бачимо, активний розвиток ІКТ відкрив нові можливості перед тероризмом, що стало поштовхом до трансформаційних процесів у медіатероризмі, а це, у свою чергу, вимагає змін у механізмі забезпечення медіабезпеки у світі.

Медіатероризм активно увійшов у вжиток на початку ХХІ століття, коли поруч із практичною діяльністю ТО захопила і медіапростір, що сприяло збільшенню глобальної аудиторії, забезпечило тривале перебування в медійному онлайн-просторі, відкрило нові джерела фінансування ТО та вербування нових членів. Тобто з'явилися нові види ЗМІ, які розширили можливості ТО. Нові технічні засоби забезпечили транслявання подій в реальному часі на всьому світовому просторі: відбулось переміщення уваги з практичної площини в інформаційно-комунікативну онлайн-мережу. У підтвердження цього англо-американський вчений Брюс Хоффман у праці «Обличчя тероризму» наводить події вересня 1972 року, коли на Олімпійських іграх у Мюнхені члени радикального палестинського угруповання «Чорний вересень» вбили спортсменів збірної Ізраїлю. Як зазначає Брюс Хоффман, «терористам вдалось переключити на себе увагу світової телевізійної аудиторії» [111, с. 131].

Наприкінці ХХ століття ТО використовували ЗМІ головним чином як інформаційні канали для оповіщення спільноти про терористичні акти та їх наслідки, при чому така інформативність через технічні можливості ЗМІ носила нетривалий характер та не отримувала широкого розголосу поза межами певної території. З подальшим розвитком ІКТ змін зазнали механізми й напрямки

взаємодії в інформаційній площині ТО та ЗМІ: поява нових медіа відкрила нові можливості для ТО та перетворила їх фактично у зброю, яка працювала вже на ТО. На наш погляд, кардинальну зміну в інформаційних відносинах ТО та ЗМІ у залежності від хронологічних рамок та рівня розвитку ІКТ можна проілюструвати наступним чином:

- наприкінці ХХ століття: «ТО  $\xrightarrow{\text{інформування}}$  ЗМІ» (взаємозв'язок здійснювався переважно в інформаційній площині; наголос слід робити на тому, що у цей період ЗМІ для терористів були, головним чином, транслятором про заплановані або проведені терористичні акти);

- на початку ХХІ століття: «МЕДІА  $\xrightarrow{\text{інформаційна зброя}}$  ТО» (розвиток ІКТ та поява соціальних медіа внесли значні зміни: соціальні медіа вже виступали як ефективна зброя в руках терористів; популярна головна теза серед джихадистів – «ЗМІ – це половина джихаду» [162, с. 24]).

Слід звернути увагу на багатоаспектність процесу трансформації медіатероризму: значних змін зазнали засоби, методи та характер використання терористами соціальних медіа, змінювались їхні функції. Для чіткого розуміння трансформаційних процесів необхідно проаналізувати зміни, які відбулись у загальній структурі ТО - МЕДІА.

1. *Зазнали змін інформаційні засоби медіатероризму.* Якщо наприкінці ХХ століття основними засобами інформування суспільства для ТО були друкована преса, радіо та телебачення, відтепер, з подальшим розвитком ІКТ, цей спектр розширився на всю глобальну мережу Інтернет. Саме Інтернет розширив масштаб терористичної пропаганди та діяльності, став інструментом для терористів для поширення своїх цілей з невеликими витратами. ТО отримали доступ до таких медіаресурсів, як соціальні мережі, месенджери, електронна пошта, Інтернет, які ТО активно використовували для створення власного медіаконтенту (власні канали, онлайн-журнали, сторінки в соціальних мережах тощо). Результати проведеного у березні – вересні 2018 року науковцями та експертами з питань запобігання радикалізації та насильницькому екстремізму (США та Канади) поглибленого інтерв'ювання 10

канадських колишніх правих екстремістів, які брали участь у расистських групах скінхедів, засвідчили, що саме Інтернет сприяв процесам насильницької радикалізації, дозволяючи їм занурюватись в екстремістський контент, а дискусійні форуми, чати та соціальні мережі були ідеальними місцями для рекламування подій, які проводяться насильницькими екстремістськими групами [154].

На відміну від друкованих ЗМІ, сучасні соціальні медіа створюють всі умови для перебування ТО в постійному полі зору суспільства, уможлиблюють швидке розповсюдження терористичних настроїв та маніпулятивного впливу ТО на широку аудиторію і значний територіальний простір, тим самим створюють можливості для поширення панічних настроїв, психологічного тиску. Так, на озброєння терористів стали соціальні мережі Facebook, Instagram, YouTube, Twitter, месенджери WhatsApp, Yik Yak, різноманітні онлайн-платформи тощо. Екстремістські угруповання створили взаємопов'язану «уявну спільноту», яка сприяє груповій згуртованості, заохочуючи до терористичних атак за допомогою різноманітних цифрових платформ» [128]. Активно вжиток терористи ввели користування мобільними пристроями з передовою технологією шифрування, зокрема мобільними додатками для зашифрованого чату (Telegram, Signal). Так, терористична організація ІД, яка використовувала Twitter в якості поширення своєї пропаганди та вербування нових членів, після того, як соціальна мережа почала регулярно блокувати облікові записи ТО (впродовж 2015 – 2016 років Twitter закрит понад 360 тисяч таких облікових записів [75]) перейшла на зашифровані повідомлення на Telegram-каналі з можливістю транслювати відео значній аудиторії глядачів. Одночасно була створена значна кількість каналів Nashir News Agency, які робили перепост офіційного контенту, зокрема інформаційного агентства «Аmaq». З метою забезпечення масової підтримки контенту застосовувалась «прихована технологія створення каналу: спочатку створювався канал, який здобував масу прихильників, і тільки потім він переключався на впізнаваний бренд ІД» [142]. Також ІД розробила проксі-додаток для смартфонів «Dawn of Glab Tidings»,

який дозволи ТО використовувати зовнішні облікові записи Twitter, пов'язані із додатком, для публікації заяв у Twitter, не зважаючи на те, що їх власні облікові записи були закриті [124].

На користь ТО спрацювало і розповсюдження контенту різними мовами, зокрема, її акаунти в Instagram публікували контент арабською, англійською мовами. Онлайн-журнали видавались англійською, німецькою, російською мовами тощо.

В умовах вжитих заходів по боротьбі з поширенням насильницького контенту в глобальній мережі Інтернет (видалення терористичного контенту, блокування облікових записів у соціальних мережах, тиск на технологічні компанії з вимогою вилучення інформації з насильницьким змістом) терористи мігрують на інші платформи. Так, у рамках організованих Європолем у скоординованій діяльності із платформами соціальних медіа Дні дій (Action Days) у жовтні 2018 року та листопаді 2019 році, спрямованих на піддрив мережі джихадистів у Telegram (саме цій платформі віддавали перевагу наближені до ІД та Аль-Каїди терористичні групи), зросла кількість перенаправлень терористів на інші файлообмінні платформи та соціальні медіа. Зокрема, після Дня дій 2019 року, у порівнянні з Днем дій 2018 року, ТО створили значну кількість нових каналів (105 у порівнянні із 12 відповідно) [163, с. 4]. Водночас, тривалість життя таких каналів була різною: створені у 2018 році канали тривали в середньому 302 дні із 4,6 публікаціями у день, в той час, як у 2019 році – 14 днів із середньою кількістю публікацій 56,8 на день) [163, с. 4]. У відповідь на такі заходи прихильники ІД активізували свою онлайн-діяльність у менш модерованих частинах Інтернету - Rocket.Chat, Riot Там Там, Hoop Messenger. Для підтримки призупинених облікових записів в соціальних мережах бойовики та прихильники ІД розробили цілий жанр «облікових записів і мемів для ідентифікації новостворених записів» [163, с. 23].

Новим механізмом онлайн-спілкування стали так звані «віртуальні мертві крапки» [90]. Термін, який використовувався у шпигунстві для таємної передачі інформаційних елементів за допомогою таємних місць, було перенесено у



цифрову площину. У віртуальному просторі під мертвою крапкою маються на увазі форми порталів анонімного обміну інформацією та хмарних служб. Зокрема, ІД та Аль-Каїда активно використовували по декілька таких платформ для зберігання та розповсюдження матеріалів в Інтернеті (тексти, фото, відео, посібники з виготовлення зброї), надаючи своїм підписникам кілька способів до доступу та завантаження контенту. Таким чином терористичним групам вдається уникнути повного видалення власних публікацій. ТО перейшли зі старих анонімних платформ nasher.me, manbar.me, noteshare на нові платформи JustPaste.it, Telegra.ph (остання надана Telegram), Files.fm, які активно використовували для оприлюднення щоденного новинного контенту, фотозвітів, скріншотів останніх номерів журналів.

2. *Зазнав змін акцент взаємовідносин ТО - МЕДІА:* з інформаційної площини, коли ТО через ЗМІ доносили до суспільства, головним чином, інформацію про терористичні акти та їх наслідки, він змістився в площину інформаційно-комунікативну. Активне використання соціальних мереж, месенджерів, глобальної мережі Інтернет створило всі умови для онлайн-контакту терористів із споживачами їхнього інформаційного контенту: відтепер ТО використовують соціальні медіа як засіб для вербування та навчання новобранців, обміну досвідом, планування, координації та виконання «шкідливих онлайн- та офлайн-операцій» [73] тощо. Так, дослідження Глобального індексу тероризму 2022 засвідчило, що у 2018 році за результатами аналізу мережі ІД у Facebook, встановлено зв'язки між 1000 профілями, які підтримували ІД серед 96 країн [22, с. 73]. До того ж, значно зросла роль соціальних медіа в контексті самопіару ТО: якщо раніше питання самореклами суцільно залежало від традиційних ЗМІ, то відтепер соціальні мережі та онлайн-платформи відкрили широкі можливості для самопіару терористів.

3. *Змінюються територіальні межі діяльності терористів.* Сучасні соціальні медіа створюють можливості транслювати екстремістський контент

на необмежену глядацьку аудиторію та широку географічну територію, досить високою є швидкість розповсюдження такого контенту.

4. *Розвиток ІКТ, використання мережі Інтернет прискорили швидкість обміну інформації, з одного боку, і у певній мірі ускладнили сам процес інформування, з іншого, що спровокувало реорганізацію ТО в мережеву структуру, де окремі члени діють більш незалежно, особливо в контексті розповсюдження повідомлень [74], що забезпечує їхню гнучкість та стійкість (у разі випадання з ланцюга ТО будь-якої ланки сама організація продовжує діяти).* Зокрема, як зазначив у 2016 році керівник Федерального відомства з охорони Конституції Німеччини Ханс-Георг Масен (Hans-Georg Maassen), занепокоєння викликає новий тип терористів, які тільки з вигляду здаються одинаками, а керують ними віртуально з-за кордону через систему миттєвих повідомлень [42]. Відповідно до підготовленого підрозділом Інтернет-рефералів ЄС для звернення до Інтернету (EU Internet Referral Unit (IRU EU) третього щорічного звіту щодо комплексного аналізу основних тенденцій та подій в онлайн-пропаганді найвідоміших джихадистських організацій ІД та Аль-Каїди за 2020 рік, констатуємо поширення закликів обох груп до самостійних нападів осіб, які не мають фізичного зв'язку з жодною з груп [160].

5. *Розмаїття та доступність цифрового обладнання надали ТО нових можливостей створення власного якісного вражаючого контенту, що розширило коло споживачів інформації.* Зокрема, за результатами дослідження Університету Центральної Флориди констатовано, що у період вересень – грудень 2016 року понад 46 тисяч акаунтів Twitter підтримували ІД [143, с. 8].

6. *Брендинг ТО.* Завдяки широким можливостям соціальних медіа терористи почали активно розповсюджувати власні логотипи та лозунги. Зокрема, у групах Facebook та Twitter були оприлюднені посилання на спеціалізовані сайти, де можна було створити футболку із логотипом ТО, замовити всілякі гаджети тощо.

Як бачимо, соціальні медіа для ТО виконували інформаційну, пропагандистську та тактичну функції. Для їх реалізації ТО активно та

продумано використовували соціальні мережі та онлайн-платформи. Зокрема, окремі дослідники стверджують, що майже 90% створеного в Інтернеті терористами контенту поширюються саме через соціальні мережі [77, с. 33].

Отже, побачивши ефективність використання соціальних медіа, ТО взяли їх на озброєнні та продемонстрували свою здатність активно використовувати віртуальні платформи для досягнення власних цілей та намірів. Змінюючи онлайн-платформу у цілях збереження власного насильницького контенту, ТО оперують такими головними характеристиками, як безпека, стійкість до зовнішнього впливу та втручання, корисність. Поширений ТО в медіа екстремістський контент впливає на розпалювання інтересу у певного кола учасників до насильницьких ідеологій, формує базу прихильників, забезпечує психологічний та маніпулятивний тиск на населення. У той же час, саме соціальні медіа вплинули на прискорення еволюційних та трансформаційних процесів та практик терористів. Активізація діяльності ТО в мережі Інтернет засвідчила необхідність більш поглибленого розуміння ролі Інтернет-технологій у розповсюдженні екстремістських та терористичних настроїв, розробки більш дієвих механізмів упередження їх розповсюдження у глобальній мережі Інтернет.

## **2.2. Зростання медіатероризму як глобальної загрози міжнародної інформаційної безпеки**

Після подій 11 вересня 2001 року тероризм став глобальним явищем, яке потребує узгодженої відповіді світової спільноти. А в умовах, коли нові ІКТ стали на службу терористів, актуальності набуває питання запобігання поширенню екстремістських та терористичних настроїв саме в мережі Інтернет, як одного з етапу боротьби з терористичною загрозою у контексті забезпечення сучасної міжнародної безпеки.

Згідно з Глобальним індексом тероризму 2022, констатуємо зростання насильницького екстремізму, зокрема, у 2021 році зазначений індекс зріс на 17% [22, с. 12]. Природно, що таке зростання тягне за собою і збільшення екстремістського та терористичного контенту у глобальній мережі Інтернет. З появою нових типів соціальних медіа ТО почали активно використовувати соціальні мережі та месенджери, створювати Інтернет-канали з розповсюдження власних медіаконтентів, що дозволило їм розширити коло аудиторії та збільшити територіальне охоплення, забезпечило постійне перебування в онлайн-просторі, додало нові важелі впливу на світову спільноту, нові джерела вербування прибічників та навчання новобранців. Нова мережева структура, що пов'язана із вербуванням у соціальних мережах, забезпечує здійснення контролю та командування насильницькими операціями. Зокрема, як свідчить восьме видання Глобального індексу тероризму (GTI), майже 50% теперішніх або колишніх членів ІД зазначають, що були радикалізовані виключно через пасивне споживання матеріалів у соціальних мережах [21, с. 77]. На нашу думку, сьогодні цілком підтвердився зроблений у 1991 році Національною академією наук США прогноз, що «звичайний терорист може завдати більше шкоди за допомогою клавіатури, аніж за допомогою бомби» [22, с. 73].

Беручи до уваги той факт, що члени сучасних терористичних організацій володіють навиками не тільки користуватись необхідним технічним обладнанням для підготовки вражаючих відео- чи аудіоматеріалів, але й

вміннями створювати відповідні фотоефекти для емоційного підсилення жахливих сюжетів і репортажів, розповсюджені в медіа матеріали про терор досягатимуть поставлених цілей. Спеціалісти з кримінального права стверджують, що майже в кожній справі про тероризм використовувались потужності Інтернету. Зокрема, відома справа у Франції щодо засудження до п'яти років ув'язнення фізика-ядерника алжирського походження Адлена Хічера (Adlene Nicheur) за участь у терористичній змові з філіалом Аль-Каїди – мова йшла про обмін ідеями в Інтернеті, відвідування Хічером форумів джихадистів [98]. У підтвердження широкого використання Інтернету у терористичних цілях свідчить судова справа штату Флоріда, за якою за спробу підтримати терористичне угруповання ІД, опублікувавши в Інтернеті відео про виготовлення вибухівки, чоловік був засуджений до 20 років ув'язнення [125].

З іншого боку, саме медіа виступають першим джерелом розповсюдження інформації про терористичний акт перед оприлюдненням офіційного повідомлення державних органів, тобто відіграють роль інтерпретатора реальних подій життя, подають погляди, думки та коментарі. Доволі часто медіа травмують глядацьку аудиторію, перебільшуючи погрози, транслуючи безперервні кадри терористичних актів тощо. З цієї точки зору, актуальності набуває функція подачі соціальними медіа чіткої, точної, без упередженості, збалансованої, а головне достовірної інформації. Постає необхідність ґрунтовної перевірки та інтерпретування різних інформаційних потоків. Важливо, щоб соціальні медіа усвідомили свою відповідальність, переглянули та змінили власну риторику щодо висвітлення новин, пов'язаних із терористичною тематикою, зокрема, висвітлювали зазначені питання у менш сенсаційний спосіб, із меншим повторенням жахливих сцен. Так, колишній Прем'єр-міністр Великобританії Маргарет Тетчер (Margaret Thatcher) визнавала зв'язок між ефективністю тероризму та висвітленням терористичних актів у пресі та наголошувала, що «публічність – це кисень тероризму» [97], однак її пропозиція вирішити зазначену проблему шляхом заклику до журналістів ігнорувати та не повідомляти про це не спрацювала.

Враховуючи активний розвиток ІКТ, їхній вплив на особистість, а також гонитву медіа за сенсаційними матеріалами актуальності набуває питання упередження виникнення ситуації, коли увага аудиторії зосереджуватиметься переважно на споживанні контенту з елементами насильства та жорстокості, що негативно впливає на психологічний стан суспільства в цілому. За результатами проведеного дослідницькою консалтинговою компанією Populus у 2017 році міжнародного порівняльного дослідження 20-ти тисяч молодих людей з 20-ти країн світу, 83% респондентів зауважили, що саме тероризм у них викликає страх за їхнє майбутнє [102].

Члени терористичних та екстремістських організацій останнім часом стали активніше використовувати онлайн-платформи для трансляції своїх злочинів в режимі реального часу. При цьому ТО вживають заходів, щоб уникнути контролю вебсайтів соціальних мереж, які б позначали їх негативний вміст та перешкоджали його публікації. Зокрема, результати проведеного у 2020 році міжнародним аналітичним центром – Інститутом стратегічного діалогу (Institute for Strategic Dialogue (ISD) дослідження, в ході якого впродовж трьох місяців відстежувались 288 облікових записів у Facebook, що пов'язані з мережею ІД, підтверджують той факт, що зазначені облікові записи досі знаходять способи уникнути виявлення на платформі соціальних мереж [103]. Серед таких механізмів, які дозволяють ТО зберігати свій контент у мережах, слід виокремити наступні:

- найпоширенішою серед мереж була тактика змішування власних матеріалів з контентом реальних новин (доволі часто додавались бренди головних новинних видань, зокрема BBC News);
- розмивання власного бренду ТО та додавання різноманітних відеоефектів соціальних мереж;
- видозмінювання тексту (використання незрозумілої пунктуації, що ускладнює пошук ключових слів для виокремлення терористичного контенту);
- викрадення терористами облікових записів Facebook, де потім публікують навчальні відео для своїх прихильників [91].

У цьому контексті актуальне та важливе значення має вжиття відповідних заходів реагування урядових установ та самих соціальних мереж на оприлюднений на сторінках їхніх користувачів терористичний контент. Зокрема, що на початку жовтня 2022 року Верховний Суд Вашингтону розпочав розгляд двох справ щодо притягнення компаній соціальних мереж до фінансової відповідальності за сприяння терористичним атакам: родичи загиблих під час терористичних актів у Франції (в листопаді 2015 року угруповання ІД атакувало кафе біля національного стадіону Франції та театр «Батаклан») та Туреччини (у 2017 році чоловік, пов'язаний із ІД, під час нападу на нічний клуб в Стамбулі вбив 39 осіб) подали до суду на соціальні мережі Facebook, Twitter та Google, звинувативши останніх у допомозі терористам в поширенні їхніх повідомлень та радикалізації новобранців [108]. Справа стосовно терористичного акту в Парижі та сприяння цьому з боку соціальної платформи Google була відхилена суддею. У той же час суд дозволив розгляд другої справи щодо терористичного акту у Стамбулі, де платформи Facebook, Twitter та Google звинуватили у сприянні тероризму та розвитку ІД, а також у тому, що останні не доклали зусиль до приборкання терористичної діяльності на своїх платформах [108].

У більшості країн вживаються заходи щодо запобігання поширенню насильницького контенту. Так, у Франції, Німеччині та Великобританії заборонений ворожнечий контент в Інтернеті. Як приклад, у другій половині 2013 року французькі чиновники зробили 87% запитів на видалення вмісту з Twitter у відповідності до звіту про прозорість компанії, останній затримав майже 133 твітів через запити Франції [87, с. 6]. У Сполучених Штатах Америки за підтримки урядових установ такі соціальні мережі як Facebook, Twitter та YouTube видаляють коментарі, пов'язані із терористичним контентом. Як приклад, у серпні 2014 року представники Білого Дому звернулись до адміністрації сайтів соціальних мереж з проханням видалити відео страти американського журналіста Джеймса Фолі (James Foley). Перебуваючи на той час на посаді прес-секретар Білого Дому Нед Прайс (Ned

Price) офіційно заявив про взаємодію Білого Дому, департаментів, агентств із сайтами соціальних медіа з метою позначення публікацій та матеріалів, які «можуть мати наслідки для національної безпеки та які не відповідають власній політиці цих провайдерів» [156]. Після організованого ІД терористичного акту у червні 2016 року у стамбульському аеропорті імені Ататюрка уряд Туреччини видав наказ «про національну безпеку та громадський порядок» [92] щодо цензури новинних груп або онлайн-ЗМІ, а також заблокував доступ до соціальних мереж Facebook, YouTube і Twitter. Відповідно до наказу, блокувалось поширення будь-яких матеріалів та інформації про терористичний акт як таких, що можуть посіяти страх та паніку серед населення.

У той же час, у зазначеному контексті постає ще одна дилема: уряди різних країн відрізняються у своїх мотивах щодо вимог видалення контенту з соціальних мереж. Зокрема, з політичних міркувань можуть висловлюватись вимоги видалення контенту тих чи інших організацій, які віднесені до числа терористичних самими урядами, водночас в інших країнах такими не вважаються.

Що стосується онлайн-платформ, то постає необхідність регулярного перегляду протоколів безпеки облікових записів, які терористам доволі часто вдається обходити. У серпні 2015 року репортер філії CNN – WDBJ Вестер Л. Флананган (Vester L. Flanagan) оприлюднив на своїх сторінках в соціальних мережах Facebook та Twitter (як користувач Брайс Вільямс (Bryce Williams)) відео вбивства двох своїх колег – телевізійних журналістів штату Вірджинія [109]. Через декілька хвилин Facebook та Twitter призупинили роботу його профілю, однак відео за цей час відтворилось на сторінках тих, хто переглядав профіль терориста та завантажував їх онлайн на YouTube. Не залишило поза увагою й той факт, що події у червні 2016 року в нічному клубі в Орландо (Франція), де в результаті терористичного акту, відповідальність за якій взяла на себе ІД, загинуло 40 осіб та отримало поранення 53 особи, стали приводом для того, щоб Facebook вперше в США активував функцію «Перевірка безпеки» [120].



Важливе значення мають прописані правила соціальних спільнот щодо оприлюднення небезпечного контенту на їх сторінках. Зокрема, у поточній версії правил Facebook не дозволена присутність організацій або фізичних осіб, які проголошують насильницьку місію або залучені до насильства, при цьому враховується їх поведінка в мережі та поза нею, їхній зв'язок із насильством [67]. Першочергова увага акцентується саме на комплексних заходах щодо осіб та угруповань, які несуть реальну загрозу, виправдовують насильство, беруть участь у злочинній діяльності (терористичні та злочинні організації) [67]. Також прописано «видалення контенту, деактивацію облікових записів та звернення до правоохоронних органів у разі виникнення загрози небезпеки заподіяння фізичної шкоди або прямої загрози громадській безпеці» [67]. Важливим кроком у напрямку боротьби з поширенням насильницького контенту відведено співпраці Facebook з правоохоронними органами, у результаті чого контент підлягає вилученню у найкоротші терміни. У правилах Twitter також чітко прописано, що «немає місця для насильницьких організацій, у тому числі терористичних організацій, насильницьких екстремістських груп або осіб, які є афілійованими та пропагують свою незаконну діяльність» [107]. У разі виявлення зазначеного контенту Twitter вимагає видалення такого вмісту.

Водночас, жодна з платформ не перевіряє дописи перед їх публікацією. Вони, головним чином, покладаються на те, що користувачі самі поінформують про вміст підозрілого контенту. Доволі складна ситуація виникає з відеотрансляцією в онлайн-режимі, оскільки вона в прямому ефірі може залучити значну кількість глядачів, що створює підвищений тиск на Інтернет-сервіси, щоб швидко зреагувати на поширення загрозового контенту. Ситуація ускладнюється й тим, що існує певне коло тих, хто підтримує дозвіл оприлюднення джихадистського контенту в соціальних мережах, аргументуючи такі кроки його «розвідувальною цінністю». Так, зокрема, науковці Брукінгського інституту Даніел Байман (Daniel Byman) та Джеремі Шапіро (Jeremy Shapiro) у статті «We shouldn't stop terrorists from tweeting» в газеті «The

Washington Post» наголошують на «розвідувальній цінності активних у соціальних мережах груп, як ІД» [88]. На наш погляд, такий аргумент є невиправданим, оскільки в умовах активного розвитку ІКТ, широкого опанування населення комп'ютерних технологій, активного споживання інформації саме з онлайн-джерел тощо, поширений в Інтернеті терористичний контент є доволі потужним джерелом психологічного тиску на населення, підбурювання до вбивств, поширення насильства, радикалізації населення, вербування прибічників екстремістів та терористів тощо. На наш погляд, жодні аналогічні пропозиції за таких обставин не можуть бути аргументованими.

Нові виклики у боротьбу з тероризмом принесла пандемія COVID-19 та її соціальні й економічні наслідки: скорочення антитерористичних бюджетів, посилення політичної напруженості, економічні збитки, міграційні процеси, зростання невдоволення урядової політики [22, с. 12] тощо.

1. Введені у зв'язку із пандемією обмеження сприяли зосередженню в онлайн-просторі громадян (як споживачів вебконтенту), екстремістських та терористичних угруповань (як розробників вебконтенту). В умовах, коли світова спільнота всі зусилля спрямувала на боротьбу з пандемією COVID-19, коли введені урядами країн обмеження та встановлені вимоги обов'язкової вакцинації населення проти COVID-19 викликали громадські невдоволення, ТО використали зазначені катаклізми на свою користь: вони вдалися до активного поширення в онлайн-просторі дезінформації з метою отримання широкої підтримки власної ідеології, маніпуляції, підбурювання тощо. Так, терористи використали COVID-19 для шахрайського збору коштів на гуманітарну допомогу під час пандемії: у Південно-Східній Азії активно збирали кошти через пов'язані з терористами канали Facebook та Telegram для підтримки сімей бойовиків ІД з Філіппін та Індонезії [83]. Як підкреслив виконавчий директор UNODC Гада Уолі (Ghada Waly), під час пандемії терористи працювали, щоб обійти обмеження на подорожі, використовуючи «віртуальні валюти та цифрові сервіси для збору та переміщення коштів у цифровому просторі» [85]. До того ж через введені обмеження масово

закривались підприємства та організації, що вплинуло на зростання ринку безробіття. В таких умовах безробітні, залишившись без засобів до існування, стають вразливими до будь-яких впливів ззовні, а надто – до маніпулятивного впливу терористів. Саме в цей час, до прикладу, ІД почала активно використовувати TikTok з метою вербування прихильників [94]. Таким чином, пандемія, спровокувавши соціальні невдоволення, фактично «створила свого роду живильне середовище для тероризму» [177, с. 17]. У той же час не варто залишати поза увагою й те, що після скасування загальних обмежень, пов'язаних із пандемією, в умовах активної діяльності ТО в медіапросторі цілком ймовірно, що широка аудиторія, яка раніше сконцентрована була на проблемах пандемії, потрапить під вплив насильницького контенту. За таких умов перед світовою спільнотою постає необхідність переосмислення загрози медіатероризму.

2. Мережі захоплених та зламаних облікових записів включали теми щодо пандемії COVID-19 у Facebook та Twitter для поширення повідомлень про ТО. Зокрема, у ході проведеного міжнародним аналітичним центром - Інститутом стратегічного діалогу дослідження встановлено, що пов'язаний з пандемією контент ІД отримав понад півмільйона переглядів. Також виявлені випадки стратегічного використання «платної реклами для поширення вмісту ІД та спроби заглушити інші публікації зазначеної тематики» [131]. У цьому контексті ТО активно розповсюджували в Інтернеті теорії змов (до прикладу, антисемітських змов), пов'язані із поширенням коронавірусу. Зокрема, у центрі уваги сторінок та каналів ТО перебувала тема діяльності еліти у світлі кризи COVID-19: всесвітньовідомі діячі Джордж Сорос та Білл Гейтс ототожнювались з «єврейською змовою» та були звинувачені у використанні вірусу як інструменту цілеспрямованої змови знищення певних груп населення, отримання прибутку на випуску вірусу тощо [54]. Це були необґрунтовані та нічим не підтвержені заяви.

3. ТО розглядають пандемію як «можливість підживити існуючі наративи зростанням расистської, антисемітської, ісламофобської ненависті» [22, с. 15],

адже саме в умовах нестабільності терористам вдається з легкістю реалізувати власні плани та цілі. ТО активно використали пандемію для просування власних рухів та ідеологій. Так, ІД в умовах кризи закликала своїх прихильників скористатись моментом слабкості західних суспільств, відволіканням уваги урядів до проблем пандемії, перерозподілом військових, охоронних та медичних ресурсів для здійснення терористичних атак. В англomовних ЗМІ наголошувалось на тому, що «вірус є покаранням за несправедливі утиски проти мусульман, які вчинили західні уряди, а мусульман, що проживали на Заході, закликано повстати проти гноблення» [158]. ТО активно проводили дезінформаційну кампанію: філія Аль-Каїди Аль-Шабаб використала викликане пандемією невдоволення серед населення для підриву довіри до уряду Сомалі. Потрясіння від пандемії використала й ІД, яка оголосила коронавірус «солдатом Аллаха» та, «зважаючи на перевантажені можливості безпеки, закликала своїх послідовників до активного продовження війни проти невірних» [118].

У період пандемії COVID-19 терористичні організації ІД та Аль-Каїда активно використовували соціальні мережі, зокрема, як засіб для підбурювання своїх прибічників до навмисного зараження коронавірусом, тим самим використовуючи COVID-19 як свого роду «біологічну бомбу» [182, с. 10]. У зазначеному контексті навмисне поширення COVID-19 розглядалось як «засіб прискорення колапсу цивілізації та усунення ненависних» [129]. Водночас, як попередили експерти Ради Європи, після пандемії у світі може зрости небезпека терактів з використанням біологічної зброї, оскільки пандемія довела вразливість суспільства.

4. З іншого боку, як зазначає Глобальний індекс тероризму 2022, на фоні пандемії через введені обмеження свободи пересування та публічного зібрання відбулось зниження самої терористичної активності: вжиті урядами обмежувальні заходи стали своєрідною перепорою на шляху переміщення терористичних груп, що вплинуло на зменшення кількості терористичних атак, відповідно й кількості потенційних жертв. Зокрема, констатовано, що за

останні шість місяців 2020 року зафіксовано найнижчу загальну кількість атак з використанням саморобного вибухового пристрою за трирічний період у Сирії, Афганістані та Сомалі [119].

Отже, COVID-19 став своєрідною зброєю, яку ТО активно використали для загострення конфліктів, прискорення громадянських заворушень, посилення соціальної та політичної поляризації суспільства тощо. Насильницькі екстремістські мережі використовують вразливі місця, пов'язані з пандемією, шляхом онлайн-пропаганди та вербування.

Як бачимо, на сьогодні однією з глобальних проблем на шляху забезпечення міжнародної безпеки перебуває питання боротьби з медіатероризмом, а точніше питання розробки правових та технічних механізмів, які б гарантували міжнародну інформаційну безпеку. Це питання перебуває на порядку денному в більшості країн світу. Ще у 2019 році лідери країн G20 після саміту в Осаці виступили із заявою щодо запобігання використанню Інтернету для фінансування та сприяння тероризму та екстремізму та закликали онлайн-платформи дотримуватися принципу верховенства права «як онлайн, так і офлайн» [99]. Водночас, в умовах пандемії COVID-19 відбулись певні трансформаційні процеси у контексті терористичної загрози: встановлені обмеження пересування, масові невдоволення карантинними обмеженнями та введенням обов'язкової вакцинації вплинули не тільки на певне зниження практичного рівня терористичної загрози, але й створили умови для швидкого та активного опанування терористами соціальних мереж для розповсюдження маніпулятивної та фейкової інформації. При чому, така інформація знаходила підтримку, головним чином, серед невдоволених політикою карантинних обмежень, посилюючи їх гнів та розчарування. Не слід залишати поза увагою ймовірність виникнення після пандемії, враховуючи її соціальні та економічні наслідки, нової загрози радикалізації населення, створення для ТО нових можливостей вербування прибічників та здійснення терористичних нападів тощо. Отже, в умовах пандемії COVID-19 неможливо втрачати пильність у питаннях терористичної

загрози у світі, необхідно виробити ефективний та дієвий спосіб поєднання механізмів стримування поширення COVID-19 із глобальною боротьбою з терористичною загрозою. Уряди краї повинні мати спільну відповідальність перед терористичною загрозою глобального масштабу.

Результати проведеного у 2020 році Виконавчим директором Контртерористичного комітету (CTED) дослідження щодо впливу пандемії на терористичну загрозу в короткостроковій перспективі засвідчили, що обмеження забезпечили терористичним групам онлайн-аудиторію, а серед довгострокових наслідків виокремлені «перенаправлення ресурсів для боротьби з тероризмом та насильницьким екстремізмом на пандемію та відновлення після неї» [149]. Така ситуація створює сприятливі умови для активізації діяльності ТО, спрямованої на розширення власної бази та зміцнення власних позицій. З іншого боку, обмеження спрямованих на боротьбу з тероризмом ресурсів впливає й на якість та ефективність відповідних вжитих заходів та операцій. За таких умов державним, правоохоронним органам, технологічним компаніям та інститутам громадянського суспільства необхідно активізувати співпрацю у напрямку вироблення технологічних інструментів, які перешкоджатимуть терористичним організаціям використовувати сайти соціальних мереж. При цьому спільні зусилля повинні бути чітко скоординовані, щоб впорядкувати ініціативи:

- державні та правоохоронні органи в боротьбі з розповсюдженням насильницького контенту оперують нормами чинного законодавства та акцентують увагу на виявленні авторства – тобто того, хто публікує матеріал, і звідки);

- технологічні компанії володіють технічним досвідом та значними технічними ресурсами, які можуть бути ефективно використані в плані реалізації заходів, спрямованих на попередження та протидію насильницького екстремізму в Інтернеті (в наявності є інструменти та механізми для швидкого виявлення та вилучення терористичного контенту в Інтернеті);

- інститути громадянського суспільства мають можливості для підтримки ефективних заходів реагування на місцевому рівні (вагома роль належить у прищепленні споживачам контенту здатності критично оцінювати та спростовувати дезінформацію, виявляти оманливі повідомлення).

Важливо зрозуміти, як терористичні групи використовують мережі для поширення інформації та вербування нових членів, а для протистояння терористичній пропаганді вкрай важливо зрозуміти, як така пропаганда створюється, якими шляхами поширюється, які стратегії ТО використовує для підтримки постійної участі своїх онлайн-користувачів. Важливим аспектом при цьому є забезпечення максимально можливого рівня свободи вираження думок при одночасному обмеженні поширення насильницького контенту в соціальних мережах.

## РОЗДІЛ 3. СОЦІАЛЬНІ МЕДІА ЯК ІНФОРМАЦІЙНА ЗБРОЯ ТЕРОРИСТИЧНИХ ОРГАНІЗАЦІЙ

### 3.1. Медіаконтент «Ісламської держави»: зміст, види та форми

За останні десятиліття соціальні медіа стали провідними інструментами екстремістських угруповань, які використовуються ними з метою поширення терористичної пропаганди та екстремістських настроїв, залякування та страху, привернення максимальної уваги усього світу, самореклами, вербування та навчання нових членів, розширення джерел фінансування ТО. У науковий ужиток входить поняття «медійний джихад» або «кіберджихад» [48, с. 81], під яким розуміють ведення джихаду з використанням інформаційних (цифрових) технологій. Про вагомую роль соціальних медіа у поширенні терористичної пропаганди зазначав у 2006 році колишній голова Міноборони США Дональд Рамсфельд (Donald Rumsfeld), який наголошував, що США програють інформаційну війну терористам. Як зауважив політик, «ворог вміло маніпулює ЗМІ», а «Вашингтон та армія повинні швидше реагувати на події та навчитися використовувати Інтернет та супутникове телебачення» [152].

Механізми та напрямки використання соціальних медіа ТО в якості інформаційної зброї можна чітко прослідкувати на основі аналізу діяльності в медіапросторі найбільш потужних терористичних організацій - «Ісламська держава» та Аль-Каїда. Ідеологія та цілі ТО чітко визначають роль медіаресурсів у їхній терористичній діяльності, методи їх використання, цільову аудиторію, медіаконтент тощо. Аналіз діяльності ТО в медіапросторі встановлює відмінні та спільні риси, які необхідно врахувати при розробці стратегії та механізмів боротьби з медіатероризмом.

«Ісламська держава» (до 2014 року - Ісламська держава Іраку та Леванту (ІДІЛ), у червні 2014 року – оголосила про заснування Ісламського халіфату) – одна з провідних міжнародних радикальних ісламістських організацій, яка станом на 2015 рік розширила свій контроль над північно-західним Іраком, східною та центральною Сирією, провінціями східного Афганістану.



Терористична організація робила спроби створити свої філії в інших мусульманських країнах світу, зокрема, знайти підтримку в Лівії, Нігерії, Саудівській Аравії, у той же час філії ТО активно діють в Азії, Африці, на Близькому Сході. Водночас, хоча станом на 2017 рік ІД і втратила майже 95% території, яку колись контролювала у Сирії та Іраку [136], все ж вона залишилась впливовою та потужною ТО. За рейтингом Глобального індексу тероризму 2022, саме ІД стала найбільш смертоносним терористичним угрупованням 2021 року [22, с. 15].

Ідеологічна доктрина ІД прописана у книзі «Управління жорстокістю», написаній у 2004 році одним з ідеологів Аль-Каїди Абу Бакром аль-Наджі. Провідна ідея - стратегія знищення держави шляхом виснаження економіки, розпалювання внутрішніх конфліктів, що поступово перетікає в стадію «управління жорстокістю» [44, с. 140]. Головними методами боротьби оголошено анархію та терор, відповідно у медіаконтенті ІД робить акцент на насиллі та жорстокості, яке транслюється на всіх медіаресурсах ТО. В онлайн-ефірах медіа ІД подає кадри вбивств та знищень (зокрема, під час захоплення міста Мосул на півночі Іраку у червні 2014 року, під час теракту в місті Дакка (Бангладеш) у липні 2016 року тощо).

Феномен використання ІД соціальних медіа викликає значний інтерес у дослідників різних галузей. Зазначена ТО створила потужну медіамашину, контент якої зацікавив десятки тисяч осіб. ІД ефективно використала технологічні розробки в Інтернеті та соціальних медіа, останні ж, в свою чергу, також вплинули на розвиток самої ТО. Власне, для ІД основні медіазасоби за умови правильного їх використання вважаються доволі ефективною зброєю, яка має всі можливості «перевищити силу найпотужніших бомб», і часом вважаються «важливішими за військовий джихад» [80].

Усвідомлюючи силу та впливовість онлайн-медіа, захоплюючись сучасними ІКТ, ІД активно почала вивчати цифрові технології, вдосконалювати навички їх застосування та активно впроваджувати їх у практику. ІД вивела медіапродукцію джихадистів на новий рівень: випуск високоякісних зображень

та відео, підготовка текстових матеріалів із якісними зображеннями та перепосиланнями на інші Інтернет-сторінки ТО.

Розглядаючи питання медіатероризму ІД, на наш погляд, доцільним є виокремлення двох аспектів:

- медіаструктура ТО;
- напрямки використання соціальних медіа.

ІД ефективно проводила свою діяльність в інформаційному просторі, результатом чого стало створення власної медіа імперії [50]. В ІД створена потужна медіакоманда, що нараховує понад 100 осіб - режисерів, графічних дизайнерів, технічних фахівців, фахівців з комунікації. Мережею медіаофісів, які створені в кожній провінції, керує Базовий фонд або Центральний медіаофіс – аль-Муасасат аль-Ум (al-Mu'asasat al-Um) [101, с. 22]. Основними медіавиробниками ІД є медіафонди «аль-Аджнад» («al-Ajnad») (підготовка аудіозаписів), «аль-Фуркан» («al-Furqan») (виробництво відеопродукції), «Мактабат аль-Хімма» («Maktabat al-Himma») (випуск релігійної літератури), радіостанція «аль-Баян» («al-Bayan») [101, с. 21-22] тощо. У 2014 році ІД створила власний медіацентр – «аль-Хаят» («al-Hayat Media Center»), який випускав цифрові журнали «Дабік» («Dibaq»), «Дар аль-Іслам» («Dar al-Islam Magazine»), «Румія» («Rumiyah»), «аль-Манба» («al-Manba Magazine») різними мовами, а також російськомовний журнал «Істок», інформаційний бюлетень «аль-Наба» («al-Naba») [101, с. 22]. Така потужна відеовиробнича кампанія створила для ІД значну кількість відеорепартажів, в яких якісно використані елементи кінематографії (монтажі, уповільнені сцени, діалоги), що суттєво відрізняє медійний контент ІД від інших терористичних організацій.

В якості основних засобів трансляції терористичної пропаганди ІД використовувала соцмережі Facebook, Instagram, YouTube та Ask.fm, месенджери Twitter, WhatsApp, Yik Yak. За оцінками Європолу, станом на 2015 рік щоденно в соціальних мережах публікувалось майже 100 тисяч повідомлень на 45-50-ти тисячах акаунтів, пов'язаних з ІД [32]. У 2018 році за результатами аналізу мережі ІД у Facebook, встановлено зв'язки між 1000

профілями, які підтримували ІД серед 96 країн, що свідчить про професійну та поширену присутність ІД на платформах соціальних медіа [22, с. 73]. Також для соціальної мережі Twitter ІД створила арабомовний додаток під назвою «Світанок» («Dawn of Glad Tiding»), в якому при реєстрації користувачі надавали дозвіл надсилати твіти через їхні облікові записи [101, с. 24]. Як бачимо, ТО активно використовувала соціальні мережі як джерело терористичної пропаганди, як інструмент поширення власного впливу.

Після блокування контенту ІД в соціальних мережах ТО оперативно переходила на нові платформи. У 2014 році Facebook, Twitter, YouTube видалили весь контент ІД. Так, Twitter у 2015 році заборонив 125 тисяч акаунтів, у 2016 році ця цифра зросла до 325 тисяч [70]. З цього часу ІД переорієнтувалась на платформи тих соціальних мереж, які або мають систему захисту вмісту, або надають можливість миттєво його публікувати: найбільш популярним став месенджер Telegram, онлайн-журнали, програми для смартфонів. Наприкінці 2015 року ІД перемістилась в Telegram, де створила значну кількість каналів, на яких транслювала те, що випускалось на офіційних медіаресурсах. Зазначена програма передбачала обмін повідомленнями з шифруванням. До того ж тут передбачена функція таймеру самознищення, яка видаляє будь-які докази та свідчення, пов'язані з діяльністю ТО.

Використання соціальних медіа ІД має чіткий підхід: в залежності від мети контент спрямовано на певні кола аудиторії. Так, для вербування прихильників свій медіаконтент ІД спрямовує саме на соціально невдоволене населення, яке відкрите та схильне до сприйняття такої інформації, має свого роду живильне середовище для розвитку радикальних поглядів та протестних ідей. Цим можна пояснити успіхи ІД в африканських державах. Водночас, ІД стала популярною платформою й для «обманутих та відчайдушних осіб» [70]. Також ІД фокусує свою медіапродукцію і за територіальним принципом. Зокрема, журнал «Дабік» був орієнтований на європейську спільноту, журнал «Константиніє» - на аудиторію Туреччини, російськомовний журнал «Істок» - відповідно був спрямований проти «невірних росіян».

Аналізуючи медіаконтент ІД, можемо виокремити основні напрямки використання ТО соціальних медіа.

1. *Поширення терористичної пропаганди, утримання контролю над захопленою територією, залякування потенційних суперників.* Для ІД цифрова пропаганда стала «центральною аспектом підходу до сучасного джихаду» [153, с. 14]. Основний контент в медіа – сцени вбивств, насилля та жорстокості, засвідчують силу, міць та вплив ТО, дають розуміння того, що будь-який опір терористам буде знищено. ІД активно здійснювала військову інформаційну підтримку там, де ще не мала істотної військової присутності. Як приклад, впродовж липня 2013 року – червня 2014 року масово розповсюджувались у формі друкованих заяв та відеозаписів погрози на адресу іракських сил безпеки.

2. *Забезпечення постійної присутності ІД в онлайн-просторі.* Демонструючи в соціальних медіа тортури та масові вбивства, ІД заволоділа увагою глобальної аудиторії, викликала бурхливу реакцію світової спільноти та стала провідною темою світового дискусійного майданчику з питань міжнародної безпеки. Всі ці складові підсилював і той факт, що медійний контент ІД розповсюджувала на значній кількості онлайн-платформ багатьма мовами (англійською, російською, арабською, турецькою, німецькою тощо), що й забезпечило постійну присутність ІД в медіапросторі.

3. *Рекламування ІД.* ІД активно використовує медіа для оприлюднення інформації щодо організаційної структури та взаємовідносин у середині ІД, транслює власні військові перемоги тощо (свого роду самореклама в Інтернеті). Такі кроки розраховані на презентацію всьому світу стабільності та міцності терористичної організації, метою чого є наміри привабити до своєї організації широке коло осіб. Так, широкого розповсюдження набув оприлюднений у червні 2016 року пропагандистський відеоролік про структуру ІД, в якому чітко можна прослідкувати зміни в ТО на шляху до створення халіфату [44, с. 188].

3. *Супровід військових операцій.* Після захоплення у 2014 році Мосулу в пропаганді ІД більш поширеними темами були представлення громадськості військово-політичних успіхів як проявів божественного схвалення, а поразки

ворогів пояснювались як «доказ божественної кари» [106]. У той же час, поряд із матеріалами, які висвітлюють власне терористичні атаки та насильницькі акти, значна увага зосереджується на відображенні реакції - політичної чи військової - на ці події. Зокрема, як засвідчує Глобальний Індекс тероризму 2020, 17 жовтня 2019 року, напередодні масштабного терористичного акту в Афганістані інформування про ІДІЛ в новинах зросло на 39%, а власне у день атаки – у новинах зменшилось на 27%, а в соціальних мережах – на 35% [138]. У самий день теракту основний новинний контент стосувався питань угоди про припинення війни у Сирії, яку уклали США та Туреччина. Впродовж декількох подальших днів інформаційний рейтинг ІД в новинах та соціальних мережах й надалі спадав.

Також ТО активно використовувала соціальні медіа й для отримання інформації про ворогів, відстежуючи їхні дії у соціальних мережах, оперативно обмінюючись між членами угруповання інформацією про цілі та вибухи тощо.

*4. Вербування прибічників.* Для зміцнення власних позицій та поширення свого впливу ІД посилює свою діяльність у напрямку залучення до свого табору значної кількості прибічників та симпатиків. Усвідомлюючи впливовість та вагомість соціальних медіа в сучасному інформаційному світі, ІД активно застосовує останні (особливо Facebook, Twitter, YouTube) в якості засобу для взаємодії з потенційними послідовниками. Зокрема, для вербування часом використовують платформу Ask.fm, яка забезпечує зворотній зв'язок (питання - відповідь). Не слід залишати поза увагою й той факт, що соціальні мережі Facebook, Instagram та YouTube тощо є найбільш поширеними ресурсами для молодшої демографічної групи, що фактично створює сприятливі умови для залучення в ТО нових членів молодого віку. З іншого боку, саме ця категорія осіб доволі добре оперує цифровими технологіями.

У зазначеному контексті варто зосередити увагу на проведенні ТО «автопропаганди» [112, с. 3], спрямованої на членів терористичних угруповань з метою зміцнення морального духу, придушення інакомислення або для

виправдання чи пояснення особливо суперечливих рішень або операцій. Основна мета таких дій – посилити внутрішню згуртованість терористів.

Слід звернути увагу на той факт, що у різні періоди діяльності ІД змінювався й власне медіаконтент ТО. Після 2015 року діяльність ІД різко впала: значна кількість лідерів були вбиті, скоротилась їхня територія, зменшилася кількість притоку іноземців-новобранців. Це, в свою чергу, привело до спаду присутності ТО в медіапросторі. Це засвідчують результати проведеного співробітником Міжнародного центру вивчення радикалізації (International Centre for the Study of Radicalisation (ICSR) Чарлі Вінтером аналізу вибірки ЗМІ, створених ІД впродовж січня-лютого 2017 року. Звернуто увагу на той факт, що влітку 2015 року ІД випустила понад 890 одиниць пропаганди, а впродовж двох місяців 2017 року - випустила 570 окремих медіапродуктів (фоторепортажі, медіаролики, письмові матеріали, аудіозаписи) [81]. Констатовано падіння продуктивності орієнтовно на 36%. У цей період майже три чверті медіаофісів ІД закрилися. Така ситуація також вплинула на зміну пропагандистського нарративу: якщо раніше центральною медіатематикою було питання пропаганди управління, то тепер ІД активізувало увагу на військовій тематиці.

Проведене у листопаді 2017 року (після втрати ІД у жовтня 2017 року Ракки, яка вважалась столицею ТО) підрозділом Британської телерадіомовної корпорації BBC Monitoring дослідження також засвідчило падіння медіаконтенту. Так, кількість заяв інформаційного агентства «Атақ» з 421 у вересні впало до 193 у жовтні, а кількість відео – з 52 у вересні до 11 у жовтні, на значний час припинили свої випуски журнал «Румія» («Rumiya») та радіо «аль-Баян» [163]. Фактично склалась ситуація, коли в ІД не було чітко визначеної моделі медіапродукції.

У той же час, таке пропагандистське затишшя в медіапросторі часом було заплановане з метою проведення перегрупування: так, після краху у 2016 році ІД випустила новий журнал «Румія» [113] та пропагандистський фільм «Полум'я війни 2: До останньої години» з погрозами нападів на США [137].

За результатами оприлюдненого у «Vision of Humanity» дослідження, 28 жовтня 2019 року соціальні медіа зафіксували зростаючий рівень висвітлення інформації про ІД, хоча жодного повідомлення про запланований чи здійснений екстремістською організацією теракт взагалі не було. Вагома частина таких публікацій стосувалась висвітлення інформації про вбивство під час військового рейду США лідера ІД Абу Бакра аль-Багдаді (Abu Bakr al-Baghdadi) [138].

У 2019 році, після низки поразок та вбивства лідера ІД Абу Бакра аль-Багдаді, ІД змушена була перейти в підпілля, а для збереження свого медіаконтенту терористи створили архів у хмарному сховищі, де зберігається приблизно чотири тисячі папок з текстовими файлами, відео та різноманітними презентаціями (інструкції про створення бомб та хімічної зброї, фото з воєнними трофеями та полоненими), навчальними файлами кількома мовами [68]. Посилання на зазначений архів розповсюджують за допомогою відкритого каналу в Telegram, де новим користувачам відправляється посилання на файли в хмарному середовищі. У той же час, такі посилання відправляють з акаунтів, що через певний час блокуються соціальними мережами. Для подальшого поширення медіаконтенту ІД терористи створюють нові акаунти або викрадають вже існуючі. Також медіаконтент ІД активно поширюється і на інших сайтах, зокрема, Muslim News, «Netflix для джихадистів» [66].

2020 рік став переломним моментом в еволюції діяльності ІД: військові поразки ІД, фізичні та практичні втрати, соціальна та економічна кризи, спровоковані введеними через пандемією COVID-19 обмеженнями, змусили ГО вжити заходів, щоб надалі забезпечити свою присутність та залишитись актуальними як в онлайн-, так і в офлайн-просторі. У цей час ІД основні зусилля зацентрувала на розширенні глобальної мережі філій та збереженні власної присутності в Інтернеті, оскільки можливості виробництва власних ЗМІ були на цей час обмежені. Наприкінці 2020 року ІД запустила медійну кампанію «Відповісти на дзвінок» («Answer the call») [134, с. 9], спрямовану на звільнення в'язнів-мусульман по всьому світу. Прихильники ІД

використовували хештегі, пов'язані із кампанією, щоб поширити свої матеріали на інших онлайн-платформах, зокрема, Telegram.

У 2021 – 2022 роках ІД активно використовує соціальні медіа для поширення пропагандистського контенту (головним чином, висвітлювала військові досягнення місцевих повстанців, які виступали під брендом ІД), оприлюднює цитати впливових (вже померлих) діячів ІД, високо оцінює зусилля своїх прихильників щодо «медійного джихаду» [134, с. 6].

Можна зробити висновок, що ІД – унікальний медіафеномен, який полягає в тому, що терористична організація вміло та ефективно використала сучасні інформаційно-комунікаційні технології в контексті поширення власної пропаганди, самореклами, розширення фінансової бази, вербування нових членів тощо. Симпатизи та пропагандисти ІД першими використали Facebook та Twitter у побудові свого «віртуального халіфату» [128]. Як засвідчує науковий співробітник Міжнародного центру вивчення радикалізації (The International Centre for the Study of Radicalisation (ICSR) Чарлі Вінтер (Charlie Winter), ІД заохочує медіаактивістів «символічною ідеологічною, релігійною, емоційною винагородами, які в сукупності формують потужну та всепоглинаючу систему переконань» [80].

Таким чином, на підставі проведеного дослідження, можна виокремити основні особливості використання ІД соціальних медіа:

- соціальні медіа на рівні із зброєю виступають одним з головних засобів, які ІД використовує у своїй діяльності;
- основними цілями використання соціальних медіа є розповсюдження терористичної пропаганди, самореклама, фінансування, вербування та навчання прибічників ТО з усього світу;
- багатоплатформний підхід до поширення пропаганди та вербування;
- медіаконтент ІД високоякісний та професійний, охоплює широке коло інструментів при переважанні візуальних форм спілкування: відеотрансляція з місця події, аудіо- та відеозаписи промов лідерів, навчальні програми та посібники, різноманітні інструкції, віртуальні ігри тощо;



- медіадіяльність ІД спрямована на охоплення широкої аудиторії, переважно молодого віку.

Враховуючи всі особливості використання ІД соціальних медіа (використання сучасних інформаційних технологій, власне виробництво якісного медіаконтенту на професійній основі, широкий ужиток онлайн-платформ, низки соціальних мереж та месенджерів тощо), навіть у періоди територіальних та фізичних втрат (як було у 2015 та 2017 роках) медіаресурс для ІД залишається і надалі однією з головних видів дієвої та ефективної зброї. ІД розробила інноваційну цифрову комунікаційну стратегію (з елементами ієрархічності), яка дозволила ТО досягти поставлених цілей щодо радикалізації до насильства та встановлення халіфату.

### **3.2. Діяльність Аль-Каїди в Інтернет-просторі: форми, види та інструменти**

Створена Усамою бен Ладаном у 1988 році міжнародна військово-терористична організація Аль-Каїда головним завданням передбачала вербування та тренування бійців з метою боротьби проти країн західного світу та їхнього впливу, а особливо США, дестабілізації інших держав, прагнула розширити вплив свого руху. Осередки Аль-Каїди діяли в Пакистані, Афганістані, Іранку, на території Близького Сходу тощо.

Як і ІД, Аль-Каїда робила ставку на ефективне використання соціальних медіа в своїй діяльності. Так, в оприлюдненому, відповідно до Резолюції Ради Безпеки ООН № 2161 від 17 червня 2014 року [6, с. 2], санкційному переліку осіб, причетних до Аль-Каїди, наведено встановлені факти використання Інтернету та соціальних мереж з метою вербування прихильників терористів, закликів до терористичних атак, пропаганди жорстокості та насилля [161].

Аль-Каїда розробила успішну медіастратегію, спрямовану проти країн західного світу, головним чином, проти США. У той же час, інформаційні операції Аль-Каїди проти Заходу, організовані у цифровому просторі, не досягли такого резонансу, як у ІД. Вони були спрямовані, головним чином, на висвітлення слабких сторін держав західного світу. Саме з цією метою Аль-Каїда видає англomовний онлайн-журнал «Inspire», в якому, головним чином, вміщено значну кількість ідеологічного матеріалу щодо заохочення тероризму, критики Заходу, подані промови Усама бен Ладена та Аймана ал-Завахірі (Ayman al-Zawahiri).

Вплинути на західну аудиторію Аль-Каїда намагалась і за допомогою відеолекцій відомого ідеолога радикального ісламу та пропагандиста екстремізму Анвара аль-Авлакі (Anwar al Awlaki) (громадянина США єменського походження), який активно використав свою присутність у цифровому просторі (поширення відеолекцій в Інтернеті, на компакт-дисках, створений його власний Інтернет-блог, групи підтримки в соціальних мережах)

та надихнув, зокрема, майора медичної служби США Нідала Маліка Хасана (Nidal Malik Hussain) на масове вбивство на військовій базі Форт-Худа в Техасі у 2009 році [101, с. 27]. Також, проповіді Анвара аль-Авлакі відвідували терористи, які 11 вересня 2001 року викрали літаки та спрямували їх на вежі-близнюки у Нью-Йорку.

Аль-Каїда використовувала нові медіатехнології, що суперечило її ідеологічним поглядам: проголошуючи консервативні релігійні ідеї та заперечуючи будь-яку модернізацію, Аль-Каїда у своїй пропагандистській діяльності використовує інноваційні технології, хоча в цьому плані вона поступається ІД. До того ж, Аль-Каїда намагається підкреслити у своїй медіапродукції відчутну різницю з ІД, зокрема, заявляє про неприйняття розбудованої ієрархічної моделі ІД. Аль-Каїда є мережевою організацією, в якій керівництво виступає, головним чином, як осередок для поширення інформації, а не виконує функції командування та контролю. Також Аль-Каїда, на відміну від ІД, медіаінструменти використовувала, в першу чергу, для поширення пропаганди (намагаючись знищити вплив західних країн) та здійснення атак на відстані.

На основі аналізу діяльності Аль-Каїди в онлайн-просторі можна виділити три основних шляхи використання медіаресурсів:

1. Використання закритих онлайн-платформ для спілкування лідерів Аль-Каїди.

2. Спілкування членів ТО на спеціальних форумах, де спільно обговорювались актуальні питання та стратегічні плани. На таких форумах надавався доступ новим користувачам. Найбільш надійною для онлайн-комунікацій Аль-Каїди є платформа Rocket.Chat, яка дозволяє групам джихадистів активно спілкуватися зі своїми прихильниками та поширювати терористичну пропаганду. Водночас у 2021 році Rocket.Chat засудила використання терористами програмного забезпечення та наголосила, що в співпраці із правоохоронними органами закритиме такі сервери.

3. Відкриті соціальні мережі та Інтернет-сайти для вільного спілкування терористів. Групи Аль-Каїди представлені в Telegram, WhatsApp, Riot і Minds, активно розробляють веб-сайти Emaad. Пропагандистське інформаційне видання Thabat News Agency, що з'явилося у 2020 році, інформує про діяльність філій Аль-Каїди, керує ботами в Telegram, використовує безкоштовні конструктори веб-сайтів для поширення пропаганди на сайті Yola для розповсюдження інформаційного бюлетеня. Саме Аль-Каїда першою опанувала нову платформу Chirpwire, схожу на Twitter [134, с. 31].

Період найвищої медіаактивності Аль-Каїди припадає на початок 2000-их років, коли був створений медіапідрозділ «Ас-Сахаб» («As-Sahab») [76, с. 6], що кожні чотири дні публікував в Інтернеті переважно документальні фільми, відео читання бійцями Аль-Каїди Корану та молитов, відео- та аудіоверсії виступів (проповідей) лідерів ТО (так, наприклад, з початку громадянської війни у Сирії у 2011 році Айман ал-Завахірі опублікував понад 70 заяв, книг та інших комюніке, де виклав своє бачення Близького Сходу, Північної Африки, мусульманської громади у цілому [89]), відео міжнародних терористичних операцій, які проводила Аль-Каїда. Лише у 2007 році «Ас-Сахаб» випустив понад 90 відео, більшість з яких висвітлювали військові дії Аль-Каїди та «Талібану» [76, с. 7]. Медіапідрприємство при виробництві медіаконтенту активно використовувало сучасні технології, методи фотомонтажної фотографії. Водночас, слід звернути увагу на те, що медіапродукція вироблялась переважно арабською мовою з перекладами англійською або іншою мовою, залежно від регіону, на який спрямовувалась проблема. Це дозволяло регулярно та безпосередньо спілкуватися різними мовами з потенційними новобранцями по всьому світу. Також медіапідрозділ «Ас-Сахаб» має власні субканали в залежності від географічних регіонів та відомих груп Аль-Каїди у цих регіонах. Такі субканали транслують переважно виступи своїх місцевих лідерів. Аль-Каїда заохочує свої регіональні філії створювати власні засоби масової інформації. На відміну від ІД, Аль-Каїда основну увагу акцентувала на координації діяльності власних центрів, прихованих

відеостудій, перевагу віддавала використанню саме закритих онлайн-каналів та платформ, де можна контролювати доступ користувачів до медіаконтенту. Зокрема, записані відео лідера Аль-Каїди Усама бен Ладена, з метою уникнення його виявлення, ймовірно записувались в прихованому будинку, далі передавались на флеш-накопичувачах кур'єрами, доки не досягали «Ас-Сахаб», де технічно монтувались до завершення (накладались субтитри з перекладами, додавались цитати з Корану тощо) і вже готовий продукт загрузали на відеофоруми джихадистів [159]. Приховані відеостудії були оснащені сучасним обладнанням для редагування аудіовізуальних матеріалів.

Свій перший медіапроект «Ас-Сахаб» опублікував в Інтернеті у 2001 році – відео під назвою «Знищення американського міноносця USS Cole», в якому вихвалялись терористи-смертники, що у 2000 році спрямували начинений вибухівкою човен у борт американського військового корабля в єменському порту Аден, в результаті чого загинуло 17 американських моряків. Так, в оприлюднених в міжнародному агентстві новин Reuters свідчень колишнього спецагенту ФБР Алі Суфана (Ali Soufan) у судовому процесі США щодо військових злочинів підсудного Алі Хамзи аль-Бахлула (Ali Hamza al Bahlul) – автора пропагандистського відео зазначено, що Усама бен Ладен був вражений відеозаписом та просунув Бахлула на посаду свого медіасекретаря [104].

Основними напрямками використання соціальних медіа Аль-Каїдою є:

1. *Пропаганда тероризму, залякування.* Пропаганда була спрямована проти країн західного світу, головним чином, проти США. Зокрема, з метою розповсюдження паніки після терористичних актів 11 вересня 2001 року Аль-Каїда регулярно розміщувала на своїх сайтах повідомлення про планування «великого нападу на цілі в Америці» [12], які отримали широке розповсюдження в друкованих виданнях і, відповідно, сіяли панічні настрої серед населення.

Важливим джерелом ісламістської пропаганди стала створена у 2004 році організація ісламістського руху – Ісламський глобальний медіафронт (Global Islamic Media Front (GMIF)), який був тісно пов'язаний з Аль-Каїдою [40, с. 16].

Основна діяльність фонду зводилась до виробництва та розповсюдження матеріалів терористичної пропаганди: інструкції від створення бомб до програмного забезпечення, переважно арабською, а такою німецькою, французькою та англійською мовами. Зокрема, таким є поширений медіафондом збірник, що містив стислі файли програмного забезпечення, необхідні для злому паролів та виявлення витоків безпеки [114, с. 22]. Також Ісламський глобальний медіафронт створив власний вебсайт та телевізійний канал «Голос Халіфату» («Voice of the Califhate»), де в інформаційних програмах вихваляли тероризм.

2. *Оперативне планування та координація терористичних актів.* Аль-Каїда активно використовувала Інтернет при плануванні терористичних актів 11 вересня 2001 року. Зокрема, федеральними посадовими особами були виявлені тисячі зашифрованих повідомлень на комп'ютері арештованого терориста Аль-Каїди Абу Забейда (Abu Zubaydah), який брав участь у керуванні терористичним актом [100, с. 10]. З метою збереження анонімності терористи використовували публічні місця з доступом до Інтернету та надсилали повідомлення через електронну пошту.

3. *Вербування прибічників.* Аль-Каїда основну увагу в медіапросторі акцентує на вербуванні прибічників по всьому світу та підготовці їх до терористичних актів (шляхом онлайн-розповсюдження спеціальних посібників та навчальних матеріалів, текстових повідомлень). Однак, на відміну від ІД, медіаконтент Аль-Каїди з метою вербування спрямовувався, головним чином, на залучення розлючених мусульман, які були «розчаровані підтримкою США Ізраїлю та американським вторгненням в мусульманський світ» [96, с. 22]. Саме їм розсилались релігійні декрети та антиамериканська пропаганда, інструкції, як стати терористом Аль-Каїди.

4. *Навчання прибічників.* Активне використання соціальних медіа з метою навчання прибічників та членів ТО. Зокрема, онлайн-журнал одного з відділень Аль-Каїди – «Табір меча» («Mu'askar al-Battar») у січні 2004 року оприлюднив

інструкцію щодо приєднання до навчального табору та виконання навчальної програми у режимі онлайн [112, с. 13].

5. *Збір розвідувальних даних та цілей.* 15 січня 2003 року у своїй доповіді Міністр оборони США Д. Рамсфельд наголосив, що виявлений в Афганістані посібник Аль-Каїди дає інструкції щодо використання громадських джерел відкрито без застосування незаконних засобів для збору як мінімум 80% інформації про ворога [12]. До того ж ТО саме з Інтернету можуть отримати безліч інформації про критичну інфраструктуру у вільному доступі. Так, у звіті Комісії з розслідування терактів зазначено, що терористи отримали доступ до оприлюдненої в Інтернеті інформації, яку використали, щоб спланувати та сприяти терористичним атакам. Зокрема, терористи володіли інформацією щодо архітектурної моделі греблі в США та програмним забезпеченням, за допомогою якого можна було зімітувати різні катастрофічні збої [112, с. 15].

6. *Фінансування ТО.* Аль-Каїда використовувала Інтернет для збору коштів, адже вона залежала від пожертвувань: її глобальна мережа збору коштів побудована на благодійних внесках неурядових організацій, фінансових установ, які використовують Інтернет-чати та форуми [100, с. 7].

У 2020 році Аль-Каїда, як і ІД, зазнала низку ударів та втрат своїх лідерів. За такої ситуації ТО внесла зміни у власний тематичний аспект щодо відмови від жорстокості та заборони вбивати невинних мусульман, що, в кінцевому результаті, представило зазначену ТО як менш екстремістську джихадистську організацію, в порівнянні з ІД [134, с. 5].

Таким чином, основними особливостями використання соціальних медіа Аль-Каїдою є:

- соціальні медіа використовуються ТО головним чином для поширення терористичної пропаганди, вербування та навчання новобранців, фінансування;
- багатоплатформний підхід до поширення пропаганди та вербування;
- медіаконтент Аль-Каїди, в порівнянні з ІД, низької якості, переважають текстові повідомлення (часом із зображеннями), усні звернення лідерів ТО;

- медіадіяльність ТО спрямована на охоплення аудиторії переважно старшої вікової групи.

Як висновок, констатуємо, що ІД та Аль-Каїда основні зусилля зосереджують на забезпеченні онлайн-стійкості, адаптивності до змін в онлайн-середовищі, підтримки своєї актуальності. Роль ефективної комунікації у цих процесах є ключовою. На напрямки та інструменти, а також особливості використання ІД та Аль-Каїдою соціальних медіа активний вплив здійснюють ідеологічні настанови ТО, їхні мета та цілі. Відповідно при розробці стратегії щодо упередження та запобігання використанню соціальних медіа у терористичних цілях, а також боротьби з впливом ТО в медіапросторі необхідно враховувати всі вищевказані фактори.



### **3.3. Механізми протидії медіатероризму міжнародними організаціями: ООН, ЄС, ОБСЄ**

На сьогодні ТО продемонстрували свою здатність активно та ефективно використовувати віртуальні платформи для реалізації власних цілей та намірів. Постійна присутність терористичного контенту в онлайн-просторі, його активне поширення загрожує безпеці громадян та всього суспільства. Як стверджують фахівці з кримінального права, сьогодні більшість кримінальних справ мають цифрову складову. Як приклад, відома справа у Франції щодо засудження до п'яти років ув'язнення фізика-ядерника алжирського походження Адлена Хічера (Adlene Nicheur) за участь у терористичній змові з філіалом Аль-Каїди – мова йшла про обмін ідеями в Інтернеті, відвідування Хічером форумів джихадистів [98].

Соціальні медіа в руках ТО виступають не лише як засіб оповіщення світової спільноти про терористичний акт та його жахливі наслідки. Саме з їх допомогою терористи намагаються привернути максимальну увагу всього світу, щоб представити себе потужною силою, на вимоги якої треба зважати і з якою треба рахуватись. Так, у 2016 році наближена до ІД група хакерів-ісламістів «Об'єднаний кіберхаліфат» викрала та оприлюднила особисті дані працівників Держдепартаменту США з погрозами вбити цих людей, а також дані 18 тисяч працівників органів безпеки Саудівської Аравії [49], чим посіяла страх серед суспільства. Забезпечивши трансляцію терактів у соціальних медіа, терористи таким чином намагаються ввести у панічний стан масовий потік глядачів. Як свідчить звіт за результатами проведеного на замовлення Європейського парламенту дослідження RAND Europe щодо втрат, спричинених тероризмом в ЄС між 2004 та 2016 роками, широке висвітлення терористичних атак в соціальних медіа привело до показового зростання кількості очевидців терактів, які, не будучи учасниками таких атак, зазнавали психологічного впливу та змінювали свою поведінку [148]. Саме в цьому й виявляється найбільша небезпека медійних матеріалів про терористичні акти:

відчуття страху, небезпеки та постійної тривожності можуть спровокувати реакцію, яка поставить під загрозу власне демократичні основи.

Враховуючи активний розвиток ІКТ, їхній вплив на свідомість громадян, а також гонитву медіа за сенсаційними матеріалами актуальності набуває питання упередження виникнення ситуації, коли увага аудиторії зосереджуватиметься переважно на споживанні контенту з елементами насильства та жорстокості. Враховуючи те, що члени сучасних терористичних організацій володіють навиками не тільки користуватись необхідним технічним обладнанням для підготовки відео- та аудіоматеріалів, але й вміннями створювати відповідні фото- та відеоефекти для емоційного підсилення сюжетів та репортажів про акти вбивств та інших насильницьких дій терористів, розповсюджені в медіа матеріали про терор досягатимуть своєї мети. А отже, на порядку денному перебуває також моральна дилема висвітлення питань тероризму в медіа.

Водночас у зазначеному контексті на шляху боротьби з використанням соціальних медіаресурсів у терористичних цілях, а також як із засобом поширення міжнародної ворожнечі тощо, порушується питання дотримання міжнародних норм у сфері прав та свобод людини, оскільки передбачається вжиття таких заходів, як блокування контенту або облікових записів, надмірну цензуру тощо. Як приклад, з метою боротьби з поширенням російської насильницької пропаганди Національна Рада електронних медіа у Латвії (Nacionālā elektronisko plašsaziņas līdzekļu padome) 24 лютого 2022 року приймає низку рішень про заборону трансляції на території країни російських програм. Так, відповідно до рішення № 85/1-2 «Про обмеження розповсюдження програми “Россия - РТР” на території Латвії» («Par programmas “Rossij RTR” izplatīšanas ierobežošanu Latvijas teritorijā») [23] трансляція на території країни зазначеної програми була заборонена впродовж п'яти років. Рішення прийнято через порушення статті 26 «Закону про електронні ЗМІ» («Elektronisko plašsaziņas līdzekļu likums») [16] від 12 липня 2010 року, а саме: трансляцію в програмах телеканалу контенту, який закликає

до розпалювання військових конфліктів, насильницького повалення влади або зміни державного апарату, підриває територіальну цілісність держави, загрожує національній безпеці та громадському порядку [16]. Аналогічним є рішення Національної Ради електронних медіа від 24 лютого 2022 року № 86/1-2 «Про обмеження розповсюдження програми “Російський інформаційний канал “Россия-24” на території Латвії» [24]. Як наголосив голова Національної Ради електронних медіа в Латвії Іварс Аболіньш, за останні два роки Латвія, обмеживши роботу 41 російського каналу, «дала чіткий сигнал, що захищала та захищатиме свій інформаційний простір» [132]. Слід зауважити, що таке рішення, за словами голова Національної Ради електронних медіа в Латвії, було прийнято вперше в історії ЄС, запустивши надзвичайну процедуру Директиви про аудіовізуальні медіапослуги, яка дозволяє державам-членам приймати такі рішення без проходження офіційної та тривалої процедури [132].

Відповідні рішення були вжиті і в Україні. 15 травня 2017 року Президент України Петро Порошенко підписав Указ України «Про рішення Ради національної безпеки та оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)», яким було введено санкції відносно ряду російських інформаційних продуктів: зокрема, соціальних мереж «ВКонтакте», «Однокласники», Інтернет-порталу Yandex та поштового сервісу Mail.ru, низки російських новинних видань тощо. Також встановлено заборону інтернет-провайдером щодо надання доступу користувачам мережі Інтернет до вищевказаних ресурсів. У той же час міжнародна правозахисна організація Human Rights Watch виступила з вимогою скасувати зазначену заборону, «яка завдає удару по свободі слова в Україні» [157]. Після розгляду зазначеного питання прес-служба Північноатлантичного альянсу погодилась з пропозицією України розглядати питання блокування російських Інтернет-ресурсів як «питання безпеки, а не питання свободи слова» [52].

Питання співвідношення свободи слова та думки із забороною поширення в онлайн-просторі шкідливого контенту висвітлена і в прийнятій спеціальними

уповноваженими з питань свободи слова та доступу до інформації ООН, ОБСЄ, Організації американських держав (ОАД) та Африки 4 травня 2015 року Спільній декларації про свободу вираження поглядів і відповіді на конфліктні ситуації [116]. Зокрема, в документі наголошено на тому, що «... держави не повинні реагувати на кризові ситуації запровадженням додаткових обмежень свободи вираження поглядів, за винятком випадків, суворо виправданих ситуацією та міжнародним правом у сфері прав людини...; фільтрація вмісту в Інтернеті, використання комунікаційних «перемикачів» і фізичне захоплення станцій мовлення – заходи, які ніколи не можуть бути виправданими згідно із законодавством про права людини» [116]. Отже, як бачимо, виникає ситуація, коли вжиті урядами країн заходи у боротьбі з поширенням терористичного контенту перетинаються із проблемами свободи преси (особливо, коли мова йде про закриття або блокування вебсайтів тощо).

Також важливим та позитивним кроком у зазначеному напрямку було прийняття 3 березня 2017 року Спільної декларації про свободу висловлювання думки, а також «фейкові» новини, дезінформацію та пропаганду, яку оголосили спеціальні уповноважені з питань свободи слова ООН, ОБСЄ, Організації американських держав (ОАД) та Африки [115]. Основними меседжами Спільної декларації були:

- держава може обмежувати право на свободу висловлювання тільки з дотриманням усіх передбачених у міжнародному праві критеріїв (блокування державою вебсайтів, IP-адрес, мережевих протоколів є надмірним заходом, який визнано лише у випадках, коли він передбачений законом, спрямований на захист прав людини чи інших законних суспільних інтересів, в залежності від відсутності менш обмежувальних альтернативних заходів та дотримання мінімально необхідних процесуальних норм);
- визнано неправомірним введення запропонованої державою системи фільтрування неконтрольованого кінцевим користувачем контенту;
- визнано недопустимість відповідальності посередників за розміщений на їхніх ресурсах третіми особами контент;

- державам необхідно вжити інших заходів, що сприятимуть утвердженню плюралізму у засобах масової інформації тощо.

В умовах активного використання терористами соціальних медіа у якості планування та виконання «шкідливих онлайн- та офлайн-операцій» [73] тощо, на технологічні кампанії покладається відповідальність за розповсюджений на їхніх платформах контент, відповідно вони зазнають тиску з боку державних структур з вимогою активізувати свою діяльність у напрямку запобігання та боротьби з діяльністю ТО в онлайн-просторі.

Отже, однією з глобальних проблем на шляху забезпечення міжнародної безпеки є питання боротьби з медіатероризмом, розробки правових та технічних механізмів упередження розповсюдження в соціальних медіа екстремістського та терористичного контенту, запобігання залучення за допомогою мережі Інтернет представників молодого покоління до участі в екстремістських та терористичних організаціях. Ці питання перебувають на порядку денному в більшості країн світу, де вже започатковано законодавчі ініціативи, розроблені та реалізуються різноманітні програми і проекти. Важливим є використання та подальше удосконалення вже існуючого досвіду, інструментів та механізмів боротьби з медіатероризмом.

## ООН

Провідна роль у питаннях аналізу та узгодження загальних підходів до питань боротьби з використанням глобальної мережі Інтернет у терористичних цілях, обміну досвідом належить ООН. В офіційних актах Генеральної Асамблеї ООН та Ради Безпеки ООН значна увага акцентована на актуальності та важливості проблеми використання глобальної мережі Інтернет в терористичних цілях. Зокрема, у резолюціях Ради Безпеки ООН № 1963 від 20 грудня 2010 року [4], № 2129 від 17 грудня 2013 року [5] висловлено занепокоєння щодо широкого використання терористами нових ІКТ для вербування та підбурювання, фінансування, навчання та планування терористичних атак.

В офіційних актах ООН також наголошено на необхідності розробки інструментів та механізмів протидії використанню терористами Інтернету як складової загальної стратегії боротьби з тероризмом. 11 травня 2016 року під час розгляду питання «Загрози міжнародного миру та безпеки, створеної терористичними актами» голова Ради Безпеки ООН виступив із заявою, в якій наголосив, що міжнародна спільнота повинна розглянути можливість розробки ефективних засобів протидії терористичній пропаганді, підбурюванню та вербовці, у тому числі через Інтернет, у відповідності з міжнародним правом [1]. Зокрема, про наполегливу необхідність протидії міжнародної спільноти у питаннях використання терористами ІКТ на глобальному рівні наголошено також в Резолюції Генеральної Асамблеї ООН № 72/284 від 26 червня 2018 року [28], Резолюціях Ради Безпеки ООН № 1624 від 14 вересня 2005 року [3], № 2178 від 24 вересня 2014 року [7], № 2354 від 24 травня 2017 року [8]. Відзначимо, що у зазначених актах наголошено на тому, що прийняті на національному рівні політичні та законодавчі заходи з попередження та протидії насильницькому онлайн-контенту повинні відповідати зобов'язанням держав у відповідності з міжнародним правом.

Важливим актом у питаннях світової протидії тероризму є прийнята Резолюцією Генеральної Асамблеї ООН № 60/288 від 8 вересня 2006 року Глобальна контртерористична стратегія ООН [9], відповідно до якої держави-члени зобов'язуються співпрацювати з ООН у питаннях координації зусиль на міжнародному та регіональному рівнях з метою боротьби з тероризмом у всіх його формах та проявах в мережі Інтернет, використання останнього в якості інструменту боротьби з розповсюдженням тероризму. На наш погляд, важливим є той факт, що за умов еволюційних змін у процесах використання терористами соціальних медіа, переглядається, оновлюється та вдосконалюється і власне Глобальна контртерористична стратегія, враховуючи нові вимоги часу.

Значний внесок у розробку зазначеного питання зробила Робоча група з протидії використанню Інтернету в терористичних цілях (Working Group on

Countering the Use of the Internet for Terrorist Purposes) при Цільовій групі з проведення контртерористичних заходів, яка працює у трьох напрямках: правові та технічні питання, а також розробка методів, за допомогою яких світова спільнота здатна буде більш ефективно використовувати Інтернет у боротьбі з тероризмом. При цьому належна увага приділяється дослідженню зразків законодавства держав-членів з питань використання Інтернету у терористичних цілях, розгляду реальних судових справ, які демонструють певні труднощі у питаннях криміналізації зазначених актів діяння та карного переслідування за їх виконання. У січні 2010 року саме з ініціативи Робочої групи з протидії використанню Інтернету в терористичних цілях з метою оцінки використання Інтернету у терористичних цілях і потенційних можливостей боротьби з цим у Німеччині (Берліні) та США (Сіетлі) відбулись конференції за участі представників урядів, міжнародних організацій та аналітичних центрів, наукових кіл та бізнес-структур [151, с. 15]. Учасники зустрічей здійснили огляд поточного стану справ зазначеної проблеми, проаналізували настанови, проекти та практичні рекомендації з правових та технічних аспектів проблеми.

Важлива роль у питаннях розробки механізмів боротьби з використанням терористами соціальних мереж та Інтернету відведена Управлінню ООН з наркотиків та злочинності (United Nations Office on Drugs and Crime (UNODC)). Так, відповідно до прийнятої 19 грудня 2011 року Резолюції Генеральної Асамблеї ООН №66/178 «Технічна допомога у виконанні міжнародних конвенцій та протоколів, що стосуються боротьби з тероризмом» [13], Управлінню ООН з наркотиків та злочинності (United Nations Office on Drugs and Crime (UNODC)) запропоновано, в межах мандату, «розвивати правові знання у сфері боротьби з тероризмом, продовжувати надавати державам-членам, що звертаються з таким проханням, допомогу в протидії використанню Інтернету в терористичних цілях, а також підтримувати держави-члени у прийнятті ефективних заходів з криміналізації, розслідуванню та кримінальному переслідуванню у зв'язку з такими випадками» [27, с. 3].

Водночас, Управління ООН з наркотиків та злочинності у тісній співпраці із Робочою групою з протидії використанню Інтернету в терористичних цілях при Цільовій групі з проведення контртерористичних заходів розробляє матеріали щодо надання технічної допомоги для використання слідчими органами та прокуратурою у справах, пов'язаних із використанням Інтернету у терористичних цілях. З цією метою 5-6 жовтня 2011 року та 2 лютого 2012 року у Відні відбулись наради за участі представників 25 держав-членів, під час яких групи експертів (представники правоохоронних органів, розвідувальних служб, міжнародних організацій, наукові співробітники, спеціалісти-практики) обмінялись досвідом, що стосується використання Інтернету з терористичними цілями [13]. Підготовлена за результатами нарад публікація «Використання Інтернету в терористичних цілях» («The use of the Internet for terrorist purposes») [151] покликана була на основі огляду та аналізу передової правової практики у проведенні розслідувань та судовому переслідуванні таких справ, вивчення можливостей співпраці державних та приватних структур у цьому питанні, надати практичну допомогу з метою сприяння більш ефективному розслідуванню у справах проти терористів, пов'язаних із використанням Інтернету. При цьому особлива увага також відводилась питанням необхідності забезпечення дотримання прав та основних свобод людини при розслідуванні таких справ. Зазначена публікація була інструментом для підтримки заходів з розробки основного потенціалу у сфері боротьби з використанням Інтернету у терористичних цілях.

У питаннях розробки стратегії щодо попередження та протидії використанню соціальних мереж у терористичних цілях належна увага відведена співпраці урядових кіл, міжнародних організацій та приватного сектору. Так, 30 листопада - 1 грудня 2016 року у центральних закладах ООН відбулась нарада на тему: «Попередження використання інформаційно-комунікаційних технологій у терористичних цілях при дотриманні прав людини та основних свобод», учасники якої розглянули питання ролі приватних кампаній у справі попередження та протидії розповсюдженню терористичних



ідей в Інтернеті. Констатовано, що ділові кола, поруч із іншими структурами, покликані відігравати важливу роль у запобіганні створенню ситуацій з розповсюдження підбурювання до тероризму.

Отже, як бачимо діяльність ООН у питаннях запобігання використанню Інтернету терористичними та екстремістськими організаціями спрямована на розробку міжнародно-правової бази та механізмів протидії використанню онлайн-медіа з метою поширення терористичного контенту. Важливе значення у цьому контексті відведено плідній співпраці урядових кіл, міжнародних організацій та приватного сектору.

## ЄС

Одним з провідних напрямків діяльності ЄС є боротьба з розповсюдженням в Інтернеті незаконного контенту. Перші кроки у цьому напрямку були зроблені на рівні добровільних ініціатив і мали рекомендаційний характер. Однак така система була визнана недостатньою.

Вагомий крок на шляху до боротьби з терористичною пропагандою зроблено у 2015 році з оголошенням «Європейського порядку денного з безпеки» («European Agenda on Security») [18], де передбачались основні заходи з упередження розповсюдження екстремістської та терористичної пропаганди: основний акцент зроблено на просуванні спільних європейських цінностей толерантності та взаємоповаги, підтримки вільних спільнот тощо.

Усвідомлюючи зростаючу загрозу використанню терористами Інтернету та соціальних мереж, у 2015 році було створено підрозділ Інтернет-рефералів ЄС для звернення до Інтернету (EU Internet Referral Unit (IRU EU) [17], функції якого полягали у виявленні та розслідуванні поширеного в Інтернеті та соціальних мережах інформації шкідливого змісту. У підрозділі працюють окремі чотири команди та низка спеціалістів з різними навичками (мовними, технічними, операційними тощо). Мережа має 6 тисяч прямих практиків з усієї Європи (вчителів, поліцейських, працівників пенітенціарних установ), що здійснює обмін досвідом. На основі дослідження загальнодоступної інформації

створюється «реферальний пакет» для оцінки загрози, розслідувань і пропозицій щодо постачальників онлайн-послуг стосовно вмісту повідомлень. Зокрема, у грудні 2017 року підрозділ ЄС для звернення до Інтернету опрацював понад 42 тисячі одиниць контенту, за результатами чого прийнято понад 40 тисяч рішень про перенаправлення інформації на понад 80 платформах понад 10 мовами. У середньому вміст було видалено у 86% випадків [17]. На основі таких перенаправлень підрозділ ЄС для звернення до Інтернету проводить Referral Action Day [17], які сприяють співпраці з представниками правоохоронних органів у державах-членах ЄС. З 2015 року підрозділ організував понад 20 Referral Action Day. Так, зокрема, 1 лютого 2022 року у Гаазі (штаб-квартирі Європолу) за участі представників спеціалізованих антитерористичних підрозділів з Франції, Німеччини, Угорщини, Італії, Нідерландів, Португалії, Іспанії, Швейцарії та Великобританії, відбувся Referral Action Day, спрямований проти поширення терористичного контенту в Інтернеті. Основна увага акцентувалась на онлайн-контенті про використання вибухонебезпечних хімічних речовин, який поширювався мережами підтримки терористів. За результатами розгляду 563 одиниці вмісту на 106 вебсайтах було оцінено для перенаправлення до постачальників онлайн-послуг для подальшого їх добровільного розгляду відповідно до їхніх умов [19].

У грудні 2015 року з метою боротьби з неправомірним використанням терористичними організаціями цифрових платформ, для виявлення та усунення шкідливих матеріалів в Інтернеті Європейська комісія започаткувала Інтернет-форум ЄС (EU Internet Forum), де на принципах партнерства співпрацювали представники урядів, Європолу, технологічної індустрії, громадянського суспільства, інші зацікавлені сторони [173]. У відкритті Інтернет-форуму ЄС також взяли участь представники Ask.fm, Facebook, Twitter, Microsoft. Як зазначив єврокомісар з питань міграції, внутрішніх справ та громадянства Дімітріс Аврамопулос, метою Інтернет-форуму є «відслідковування контенту екстремістського спрямування у мережі та швидке його видалення» [32].

Водночас, ще одним інструментом в боротьбі ЄС з поширенням терористичного контенту була розробка програм з питань обізнаності з радикалізацією, поширення антитерористичної тематики. Так, у рамках Інтернет-форуму у 2015 році з метою боротьби з успішним використанням терористичними та екстремістськими групами технологій та соціальних медіа була прийнята Програма розширення можливостей громадянського суспільства (Civil Society Empowerment Programme (CSEP) [169], яка, зокрема, передбачає грантову підтримку для напрацювання саме антитерористичного контенту. У рамках Програми проводять тренінги та навчання для компаній та організацій громадянського суспільства з метою розробки заходів з мінімізації залучення вразливої категорії осіб до терористичних угруповань.

Одним з важливих, на нашу думку, кроків є домовленість, досягнута у 2016 році провідними соціальними мережами Facebook, Twitter, YouTube, Microsoft про новий Кодекс поведінки в онлайн-просторі, який полягав у перегляді «ненависного онлайн-контенту» та зобов'язанні видалення його впродовж 24 годин задля боротьби з терористичною пропагандою в ЄС» [170]. Отже, більше відповідальності у питаннях вилучення зазначеного контенту тепер покладалось на самі платформи, без будь-якого контролю з боку інституцій. Зокрема, за результатами оцінки Кодексу поведінки щодо поширення мови ворожнечі в Інтернеті, проведеної у 2020 році, констатовано, що у середньому впродовж 24 годин розглядається 90% повідомлень, з яких 71% вмісту видаляється як такий, що «вважається незаконним та таким, що розпалює ворожнечу» [171].

У 2017 році Facebook, Twitter, YouTube та Microsoft створили Глобальний Інтернет-форум з протидії тероризму (Global Internet Forum to Counter Terrorism (GIFCT) [20], основний акцент якого було спрямовано на запобігання поширенню екстремістського та терористичного контенту в Інтернеті. Передбачалась співпраця з обміну знаннями, розробка найкращих практик, вдосконалення існуючої спільної технічної роботи, впровадження нових методів виявлення та класифікації вмісту за допомогою машинного навчання

тощо. Позитивним кроком було створення спільної «бази даних хеш-обміну», де збирали унікальні фрагменти терористичного контенту, позначених та видалених зі своїх серверів компаніями-засновниками Глобального Інтернет-форуму з протидії тероризму [176]. Зокрема, у 2017 році база включала 40 тисяч фрагментів, на середину 2019 року – понад 200 тисяч, на середину 2021 року – 320 тисяч різних фото та відео [175].

У 2018 році Єврокомісія запропонувала правовий інструмент вирішення питання запобігання поширенню терористичного контенту в Інтернеті: постачальників цифрових послуг було зобов'язано видаляти такий контент в чіткі часові рамки (впродовж години після отримання), встановлено конкретні правила та зобов'язання для провайдерів щодо виявлення, ідентифікації та видалення терористичного контенту на їхніх платформах [123] встановлено штрафні санкції (у розмірі 4% від їх світового доходу) для платформ, які не дотримуватимуться вказаних вимог [172, с. 21]. Також на постачальників хостингу були покладені зобов'язання щодо підготовки та оприлюднення щорічного звіту за результатами вжитих заходів та дій проти розповсюдження терористичного контенту.

Після теракту у квітні 2019 року в новозеландському місті Крайстчерчі, який транслювали в прямому ефірі на Facebook, учасники Глобального Інтернет-форуму з протидії тероризму, представники урядів G7 та лідери технологічної галузі підписали ініціативу «Заклик до дії» («The Christchurch Call to Action») [168], яка передбачала конкретні кроки (як з боку постачальників онлайн-послуг, так і з боку урядів) для боротьби із зловживанням технологіями з метою поширення терористичного контенту (передбачалась співпраця для розробки технічних рішень щодо запобігання завантаження в Інтернет, виявлення та видалення терористичного та екстремістського контенту в Інтернеті) [168].

У листопаді 2019 року країни-члени ЄС та Європолу скоординували свої дії проти діяльності ІД в онлайн-мережі: організоване ТО розповсюдження пропаганди зазнало відчутного удару. Відтоді онлан-прихильники ІД

намагались відновити свої мережі в Telegram, а також на інших онлайн-платформах, як Rocket.Chat, Tam Tam, Hoop Messenger тощо.

Протидія незаконному контенту в Інтернеті була чітко окреслена у прийнятій 24 липня 2020 року Європейською комісією нової Стратегії Союзу безпеки ЄС на період 2020 – 2025 років [15]. Зокрема, увагу акцентовано на необхідності посилення добровільної співпраці між правоохоронними органами та приватним сектором у напрямку боротьби з неправомірним використанням Інтернету терористами.

З метою запобігання зловживаннями Інтернет-платформ насильницькими екстремістами, терористичними групами та їх симпатиками 9 грудня 2020 року Єврокомісія представила оновлену програму боротьби з тероризмом, основними гаслами якої стали «передбачити, запобігти, захистити, реагувати» [162].

Знаковим кроком на шляху боротьби з медіатероризмом було схвалення Європарламентом у квітні 2021 року нового закону про боротьбу з розповсюдженням терористичного контенту в Інтернеті – Регламенту щодо боротьби з поширенням терористичного контенту в Інтернеті [26]. Основна увага акцентована на «терористичному контенті» - відео- та аудіо-записах, зображеннях та текстах, які відкрито закликають або пропагують терористичні злочини, містять матеріали щодо виготовлення вибухівки або інструкцій з використання вогнепальної або іншої зброї у терористичних цілях. Передбачено, що у разі появи такого контенту та видачі відповідного наказу компетентного органу в кожній державі-учасниці ЄС постачальники послуг хостингу зобов'язані впродовж години його видалити або заборонити доступ до терористичного контенту у всіх державах-членах ЄС [26] (як бачимо, вибір конкретних заходів щодо запобігання поширенню терористичного контенту, в Інтернеті залишається за постачальником). Також варто зосередити увагу на такому важливому аспекті: поряд із заходами з боротьби з розповсюдженням терористичного контенту наголошено на необхідності посилення «медіаграмотності та критичного мислення, розробку контрнарративів» [26].

Слід зауважити, що, хоча зазначений Регламент був покликаний гармонізувати правову базу для забезпечення видалення такого змісту контенту та підвищити прозорість щодо відповідальності провайдерів у цій сфері, однак ще у березні 2021 року 61-на правозахисна організація звернулась до Європейського парламенту із спільним листом, в якому закликали не підтримувати зазначений Регламент [117]. Серед аргументів громадських правозахисників: загроза для свободи вираження поглядів та думок, право на інформацію; обмежений час для видалення контенту, що передбачає використання автоматизованих інструментів модерації (у цьому випадку відсутня чіткість розмежування терористичного вмісту від, до прикладу, сатиричного контенту про тероризм, що може потягнути за собою ненавмисне видалення легального контенту; у цьому випадку потрібні нагляд та перевірка); питання наявності ефективного механізму нагляду за виконанням правового інструменту (пропозиція щодо видалення контенту не передбачала судового перегляду рішення). На нашу думку, доволі влучним є твердження євродепутата Патрика Які (Patryk Jaki's), який, коментуючи новий Регламент щодо боротьби з розповсюдженням терористичного контенту в Інтернеті, наголосив на тому, що цей новий інструмент заснований на співпраці та довірі між державами, «збалансує безпеку, свободу слова та вираження поглядів в Інтернеті» [133]. У червні 2022 року Регламент ЄС щодо терористичного контенту набув чинності. Відтепер соціальні мережі Facebook, Twitter, Google зобов'язані за годину видалити позначений терористичний контент, що поширений на їхніх платформах. У разі невиконання на технологічні компанії накладатиметься штраф у розмірі 4% їхнього глобального доходу. Як бачимо, законодавчий акт зафіксував чітку сферу застосування та чітко визначення терористичного контенту з дотримання основних прав, надав додаткові інструменти державам-членам для забезпечення швидкого видалення терористичного контенту, сформував ефективні засоби захисту як для користувачів, чий контент було вилучено, так і постачальників послуг – технологічних компаній.

Європол щорічно готує звіт про онлайн-пропаганду джихадистів, в якому проаналізовано основні тенденції та події в пропаганді терористичних організацій. На основі досліджень інформаційних першоджерел (відео, аудіозаписи, заяви, публікації) встановлено основні теми та типи публікацій, зміни в основних наративах тощо. Зокрема, у четвертому виданні щорічного звіту Європолу, на основі аналізу зібраних впродовж 2021 року пропагандистських матеріалів терористичних організацій ІД та Аль-Каїди, констатовано, що мережі прихильників ТО продемонстрували підвищені технічні можливості у своїх зусиллях з поширення пропаганди [134, с. 50].

У грудні 2020 року Європарламент виступив з двома законодавчими ініціативами для оновлення правил, які регулюють цифрові послуги в ЄС. Ухвалення Закону про цифрові ринки (Digital Markets Act (DMA) 25 березня 2022 року [166] та Закону про цифрові послуги (Digital Services Act (DSA) 23 квітня 2022 року [167] створило єдиний набір нових правил, які застосовуватимуться для всього ЄС з метою створення безпечного та відкритого цифрового простору із захищеними правами користувачів цифрових послуг та рівними умовами для бізнесу, сприяння інноваціям, зростанню конкурентноспроможності. Як точно зазначила Президент Європейської комісії Урсула фон дер Ляєн (Ursula von der Leyen), Закон про цифрові послуги оновлює основні правила для всіх онлайн-сервісів ЄС, що дає практичну реалізацію принципу: що є незаконним офлайн, має бути незаконним і онлайн [167]. Закон про цифрові послуги передбачає нові заходи протидії незаконному контенту в Інтернеті та зобов'язує платформи швидко на нього реагувати, дотримуючись прав та свобод людини; можливість оскарження рішення платформ щодо модерації контенту тощо. Зазначені законодавчі ініціативи засвідчили актуальність впливу соціальних сервісів на світову спільноту та національну безпеку, а також подали механізми його протидії.

Протидія поширенню терористичного контенту в онлайн-просторі посідає одне з центральних місць у діяльності ОБСЄ щодо подолання транснаціональних загроз безпеці. Так, відповідно до Консолідованої рамкової програми ОБСЄ для боротьби з тероризмом, одним із стратегічних напрямків визначена протидія використанню Інтернету в терористичних цілях, а координуючим центром, інформаційним ресурсом та партнером з практичного виконання контртерористичної діяльності ОБСЄ визнано антитерористичний підрозділ Департаменту з питань транснаціональних загроз [25].

Масштабність використання глобальної мережі Інтернет терористичними організаціями з метою вербування нових членів, забезпечення фінансових накопичень, організації терористичних актів визнано у Рішенні Ради Міністрів ОБСЄ №3/04 від 7 грудня 2004 року «Боротьба з використанням Інтернету в терористичних цілях» [10]. Також Рішенням передбачено обмін між державами-членами інформацією про використання мережі Інтернет у терористичних цілях та визначення можливих стратегій боротьби з цією загрозою. Зазначені питання були темою проведених у 2005 та 2006 роках експертних семінарів ОБСЄ.

Відповідно до Рішення Ради Міністрів ОБСЄ №7/06 від 6 грудня 2006 року «Протидія використанню Інтернету у терористичних цілях» [11], де увагу звернуто на масштабності використання глобальної мережі Інтернет терористами, державам-членам запропоновано розширити моніторинги вебсайтів терористичних/екстремістських організацій та їхніх прибічників, налагодити обмін інформацією у рамках ОБСЄ та інших відповідних форумів з питань використання Інтернету для терористичних цілей, а також засобів, використаних для протидії такому використанню у відповідності з внутрішнім законодавством, забезпечуючи при цьому дотримання міжнародних зобов'язань та норм в галузі прав людини. Також висловлено рекомендації щодо вивчення можливості більш активного залучення інститутів громадянського суспільства та приватного сектору у діяльність з попередження та протидії використанню Інтернету для терористичних цілей.



ОБСЄ організовує онлайн-платформу, на якій представники урядових кіл, громадянського суспільства та бізнес-структур проводять подальші напрацювання та просування найкращих практик, спрямованих на упередження та протидію екстремізму та тероризму в Інтернет-просторі. З цією метою 12 грудня 2019 року у Душанбе за сприяння антитерористичного підрозділу Департаменту з питань транснаціональних загроз ОБСЄ відбулась дводенна зустріч представників правоохоронних органів, відповідних державних установ, ІКТ-індустрії, громадянського суспільства, наукових кіл та ЗМІ усіх держав Центральної Азії та Афганістану з питань вирішення проблем цифрових аспектів насильницького екстремізму в Центральній Азії [182]. Виконуючий на той час обов'язки заступника голови Офісу програм ОБСЄ в Душанбе Герріт Зак (Gerrit Zach) закликав уряди пам'ятати, що «регулювання Інтернету може бути неефективним або навіть контрпродуктивним, якщо воно не поважатиме міжнародні права та свободи людини» [182].

25 травня 2020 року відділ боротьби з тероризмом Департаменту транснаціональних загроз ОБСЄ запустив для широкої аудиторії електронний навчальний курс (англійською та російською мовами) «Попередження та боротьба з використанням мережі Інтернет у терористичних цілях» [84], під час якого проаналізовано приклади зловживання Інтернетом терористами та екстремістами, а також розроблено практичні рекомендації щодо реагування на такі виклики з дотриманням прав людини.

У рамках міжнародної дискусії з питання використання глобальної мережі Інтернет терористами, прогалин в нормативно-правовій базі Відділ протидії тероризму Департаменту транснаціональних загроз ОБСЄ організував 12 квітня 2021 року вебінар «Використання Інтернету терористами: позначення незаконного онлайн-контенту та прогалини в нормативно-правовій базі» [181]. Під час онлайн-заходу понад 180 експертів та посадовців розглянули нові тенденції, проблеми та прогалини у питаннях нормативного визначення понять незаконного та терористичного контенту в Інтернеті, а також обговорили можливий негативний вплив на основні права людини у контексті ініціатив

щодо боротьби з терористичним та екстремістським контентом в Інтернеті. У той же час, присутні на заході представники Канади, Італії та Японії презентували інноваційні практики та знання щодо модерування терористичного та екстремістського контенту в Інтернеті.

Як бачимо, у питаннях упередження та боротьби з поширенням в онлайн-просторі екстремістських та терористичних настроїв ОБСЄ, головним чином, основні зусилля спрямовує на створення дискусійних онлайн-платформ, сприянні співпраці державного та приватного секторів, на забезпеченні цифрової грамотності тощо.

Отже, сьогодні в умовах активного використання соціальних медіа ТО як інструментів ведення насильницької пропаганди, організації терористичних актів, забезпечення фінансування терористів, вербування їх прибічників актуальності набуває питання забезпечення міжнародної безпеки. З метою розробки ефективної стратегії боротьби з медіатероризмом (із врахуванням чіткої різниці між ідеологією ТО, їх цільовою аудиторією, каналами поширення медіаконтенту, власне його змістом тощо) необхідною та доцільною, на наш погляд, є співпраця урядових кіл, правоохоронних органів, громадських організацій, приватного сектору та науковців на міжнародному рівні. Спільний досвід та розробки у зазначеній проблематиці дозволять розробити ефективні заходи щодо обмеження обігу терористичного медіаконтенту, сформувати дієві механізми протидії каналам його поширення. Зазначені кроки необхідно узгодити з нормами чинного законодавства, адже доволі часто заходи, що спрямовані на блокування чи фільтрацію негативного контенту в онлайн-платформах, критикуються за можливу цензуру. А отже, відповідні заходи необхідно реалізовувати при дотриманні принципу невтручання в приватне життя та свободу думки, збереження вільного та безпечного обміну інформацією у мережі. У цьому контексті ми не підтримаємо точку зору дослідників О. Білаш, М. Сорокато, Р. Ковальчука, які наголошують, що задля запобігання тероризму в сучасній Україні необхідно запровадити саме

авторитарний контроль над інформаційним простором на усій території України [31, с. 304].

Водночас, на нашу думку, ще одним з інструментів боротьби з поширенням негативного контенту в медіасередовищі виступають такі заходи, як створення цифрової стійкості, поширення медіаграмотності, формування стійкості до впливу дезінформації тощо. Адже громадськість повинна бути обізнана у питаннях розуміння позитивних та негативних аспектів соціальних мереж та кіберпростору.

У той же час, у контексті останніх подій в Україні (виявлення та затримання Службою безпеки України у вересні 2020 року та серпні - вересні 2021 року учасників ІД [66]) важливе значення має взаємодія з іншими країнами та міжнародними організаціями у напрямку спільних напрацювань з розробки інструментів та механізмів боротьби з тероризмом та використанням соціальних медіа у терористичних цілях.

## ВИСНОВКИ

На початку XXI століття міжнародний тероризм набув рис глобальної загрози міжнародної безпеки. Активний розвиток ІКТ, процеси діджиталізації охопили всі сфери суспільного життя та безпосередньо вплинули на діяльність ТО: розвиток цифрових технологій кардинально змінив інформаційний інструментарій терористів, які швидко адаптувались до технологічних інновацій. Так, на заміну традиційних ЗМІ (преса, телебачення, радіо), які раніше використовувались терористами переважно як джерело оповіщення спільноти про терористичні акти та їх наслідки, прийшли соціальні медіа (соціальні мережі, месенджери, онлайн-платформи тощо). Останні стали справжньою зброєю в руках екстремістських та терористичних організацій, які зрозуміли всі переваги онлайн-середовища для досягнення власних цілей (оперативність донесення інформації до світової спільноти, акцентування глобальної уваги, онлайн-спілкування з прибічниками, низькі витрати при використанні соціальних медіа, оприлюднення значного масиву інформації, анонімність користувачів тощо). На порядок денний постало питання боротьби з медіатероризмом – особливим видом інформаційного тероризму, який полягає в систематичному та цілеспрямованому використанні соціальних медіа з метою дестабілізації ситуації, психологічного впливу на масову свідомість (поширення серед населення почуття тривоги, занепокоєння, страху та паніки, забезпечення маніпулятивного впливу).

Соціальні медіа виконують для ТО інформаційну, пропагандистську та тактичну функції:

- поширення пропагандистських настроїв та забезпечення маніпулятивного впливу;
- поширення серед світової спільноти відчуття паніки та страху;
- забезпечення постійної присутності в онлайн-просторі, самореклама;
- супровід військових операцій;
- збір даних;

- вербування та навчання прибічників, обміну досвідом;
- розширення фінансової бази забезпечення ТО.

Активне використання ТО соціальних медіа вплинуло і власне на зміну механізму взаємодії ТО – МЕДІА:

- зазнав змін акцент взаємовідносин ТО – МЕДІА (якщо наприкінці ХХ століття ЗМІ терористами використовувались лише для інформування про терористичні акти, відтепер МЕДІА стали інформаційною зброєю для терористів з цілим набором функцій – інформування, пропагування, маніпулювання, вербування, фінансування, навчання тощо);

- змінились основні засоби медіатероризму (на озброєння ТО стала глобальна мережа Інтернет з усіма її перевагами: активне використання соціальних мереж Facebook, Instagram, YouTube, Twitter, месенджерів WhatsApp, Yik Yak, онлайн-платформ JustPaste.it, Telegra.ph, так званих «віртуальних мертвих крапок» тощо; забезпечення мігрування онлайн-платформами через блокування облікових записів ТО);

- розширились територіальні межі діяльності терористів (відтепер відголос терористичних актів отримував поширення далеко за його географічні межі та охоплював глобальну аудиторію глядачів);

- прискорення швидкості процесу обміну інформацією між ТО, а також між ТО та її прибічниками;

- розмаїття та доступність цифрового обладнання надали ТО можливостей створення вражаючого контенту власного виробництва: маючи навички користування новим технічним обладнанням для зйомок та записів, терористи сьогодні опанували нові технологічні засоби для створення емоційно та психологічно вражаючого контенту (відео та фото вбивств, тортур, насилля), його масового поширення в онлайн-просторі, що вплинуло на розширення кола споживачів такої інформації;

- завдяки широким можливостям соціальних медіа терористи почали активно розповсюджувати власні бренди та логотипи.

Отже, констатуємо, що саме соціальні медіа впливають на прискорення еволюційних процесів та практик терористів. У свою чергу, поширений ТО в медіа екстремістський контент впливає на розпалювання інтересу у певного кола учасників до насильницьких ідеологій, формує базу прихильників, забезпечує психологічний та маніпулятивний тиск на населення. Такі механізми та напрямки взаємодії ТО – МЕДІА чітко прослідковуються на прикладі діяльності в медіапросторі найбільш потужних терористичних організацій - ІД та Аль-Каїди, яким вдалось ефективно використати сучасні ІКТ, сформувати власні медіаструктури, адаптуватись до медіасередовища, забезпечити постійну присутність в онлайн-просторі. Діяльність ТО в інформаційному просторі довела актуальність та важливість впливу соціальних медіа для забезпечення конкурентної пропагандистської війни. У той же час на напрямки та інструменти, особливості використання соціальних медіа ІД та Аль-Каїдою активний вплив здійснюють їхні ідеологічні настанови, мета та цілі. Аналіз діяльності зазначених ТО в медіапросторі надає можливість встановити відмінні та спільні риси (із врахуванням чіткої різниці між ідеологією ТО, їх цільовою аудиторією, каналами поширення медіаконтенту, власне його змістом тощо), які необхідно врахувати при розробці стратегії та механізмів боротьби з медіатероризмом.

Значний внесок у розробку механізмів протидії медіатероризму зробили міжнародні організації ООН, ЄС, ОБСЄ, які сформували правові та технічні механізми упередження розповсюдження в соціальних медіа екстремістського та терористичного контенту, запобігання залучення за допомогою мережі Інтернет представників молодого покоління до участі в екстремістських та терористичних організаціях тощо. Ці питання перебувають на порядку денному в більшості країн світу, де вже започатковано законодавчі ініціативи, розроблені та реалізуються різноманітні програми і проекти. Важливим є використання та подальше удосконалення вже існуючого досвіду, інструментів та механізмів боротьби з медіатероризмом. На наш погляд, у зазначеному контексті необхідно зосередити увагу на співпраці органів влади, громадських

організацій, наукових кіл, приватного сектору на міжнародному рівні. Спільний досвід та практика дозволять розробити ефективні заходи щодо обмеження обігу терористичного медіаконтенту та сформувати дієві механізми протидії каналам його поширення. У той же час, важливим є питання узгодження зазначених заходів із нормами чинного законодавства щодо забезпечення невторчання у приватне життя та свободу думки, збереження вільного та безпечного обміну інформацією у мережі.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

### Нормативно – правові документи

1. Заявление Председателя Совета Безопасности на 7690-м заседании Совета Безопасности, состоявшемся 11 мая 2016 года. URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N16/133/15/PDF/N1613315.pdf?OpenElement> (дата звернення: 18.10.2022)
2. Про рішення Ради національної безпеки та оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: Указ України від 15.05.2017 р. № 133/2017. URL: <https://zakon.rada.gov.ua/laws/show/133/2017#Text> (дата звернення: 19.10.2022)
3. Резолюция 1624 (2005), принятая Советом Безопасности на его 5261-м заседании 14 сентября 2005 года. URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/510/54/PDF/N0551054.pdf?OpenElement> (дата звернення: 18.10.2022)
4. Резолюция 1963 (2010), принятая Советом Безопасности на его 6459-м заседании 20 декабря 2010 года. URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N10/702/25/PDF/N1070225.pdf?OpenElement> (дата звернення: 18.10.2022)
5. Резолюция 2129 (2013), принятая Советом Безопасности на его 7086-м заседании 17 декабря 2013 года. URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/624/39/PDF/N1362439.pdf?OpenElement> (дата звернення: 19.10.2022)
6. Резолюция 2161 (2014), принятая Советом Безопасности на его 7198-м заседании 17 июня 2014 года. URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/433/00/PDF/N1443300.pdf?OpenElement> (дата звернення: 19.10.2022)
7. Резолюция 2178 (2014), принятая Советом Безопасности на его 7272-м заседании 24 сентября 2014 года. URL: [https://documents-dds-](https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/433/00/PDF/N1443300.pdf?OpenElement)



ny.un.org/doc/UNDOC/GEN/N14/548/01/PDF/N1454801.pdf?OpenElement (дата звернення: 21.10.2022)

8. Резолюция 2354 (2017), принятая Советом Безопасности на его 7949-м заседании 24 мая 2017 года. URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/149/26/PDF/N1714926.pdf?OpenElement> (дата звернення: 18.10.2022)

9. Резолюция, принятая Генеральной Ассамблеей 8 сентября 2006 года. URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/504/90/PDF/N0550490.pdf?OpenElement> (дата звернення: 18.10.2022)

10. Решение № 3/04: Борьба с использованием интернета в террористических целях. URL: <https://www.osce.org/ru/mc/42651> (дата звернення: 18.10.2022)

11. Решение № 7/06 о противодействии использованию интернета в террористических целях. URL: <https://www.osce.org/ru/mc/23082> (дата звернення: 18.10.2022)

12. Спецдоклад № 116. Как современные террористы используют Интернет, 3 жовтня 2006 р. URL: <https://cripo.com.ua/likbez/p-24673/> (дата звернення: 19.10.2022)

13. Техническая помощь в осуществлении международных конвенций и протоколов, касающихся терроризма. Доклад Генерального секретаря. United Nations Office on Drugs and Crime (UNODC). URL: [https://www.unodc.org/documents/commissions/General\\_Assembly/Preparation\\_Documentation/GA\\_67\\_2012/A-67-158/A-67-158\\_R.pdf](https://www.unodc.org/documents/commissions/General_Assembly/Preparation_Documentation/GA_67_2012/A-67-158/A-67-158_R.pdf) (дата звернення: 18.10.2022)

14. Christchurch Call story. *CHRISTCHURCH CALL*. URL: <https://www.christchurchcall.com/about/the-christchurch-call-story/> (Last accessed: 31.10.2022)

15. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE

OF THE REGIONS on the EU Security Union Strategy. *EUR-Lex*. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605> (Last accessed: 15.10.2022)

16. Elektronisko plašsaziņas līdzekļu likums. Saeima. 12 jūlijā 2020. URL: <https://likumi.lv/ta/id/214039-elektronisko-plassazinas-lidzeklu-likums#p26> (Last accessed: 22.10.2022)

17. EU Internet Referral Unit (EU IRU). URL: <https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-etc/eu-internet-referral-unit-eu-iru> (Last accessed: 17.10.2022)

18. European Agenda on Security – Legislative documents. URL: [https://home-affairs.ec.europa.eu/what-we-do/policies/internal-security/european-agenda-security-legislative-documents\\_en](https://home-affairs.ec.europa.eu/what-we-do/policies/internal-security/european-agenda-security-legislative-documents_en) (Last accessed: 17.10.2022)

19. Europol coordinates action against bomb manuals available online. *European Union Agency for Law Enforcement Cooperation (Europol)*. 03.02.2022. URL: <https://www.europol.europa.eu/media-press/newsroom/news/europol-coordinates-action-against-bomb-manuals-available-online> (Last accessed: 17.10.2022)

20. Global Internet Forum to Counter Terrorism (GIFKT). URL: <https://gifct.org/> (Last accessed: 05.10.2022)

21. Global Terrorism Index 2020. Measuring the Impact of Terrorism. URL: <https://www.visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-2.pdf> (Last accessed: 09.10.2022)

22. Global Terrorism Index 2022. Measuring the Impact of Terrorism. URL: <https://www.visionofhumanity.org/wp-content/uploads/2022/03/GTI-2022-web-09062022.pdf> (Last accessed: 09.10.2022)

23. Lēmums Nr. 85/1-2, 24 februārī 2022. Par programmas "Rossija RTR" izplatīšanas ierobežošanu Latvijas teritorijā. Nacionālā elektronisko plašsaziņas līdzekļu padome. URL: <https://likumi.lv/ta/id/330345-par-programmas-rossija-rtr-izplatisanas-ierobezosanu-latvijas-teritorija> (Last accessed: 22.10.2022)

24. Lēmums Nr. 86/1-2, 24 februārī 2022. Par programmas "Rossiyskiy Informatsionnyy Kanal "Rossiya - 24"" izplatīšanas ierobežošanu Latvijas teritorijā. Nacionālā elektronisko plašsaziņas līdzecļu padome. URL: <https://likumi.lv/ta/id/330347-par-programmas-rossiyskiy-informatsionnyy-kanal-rossiya--24-izplatisanas-ierobezosanu-latvijas-teritorija> (Last accessed: 22.10.2022)
25. Permanent Council Decision No. 1063. OSCE Consolidated Framework for the Fight against Terrorism. URL: <https://www.osce.org/pc/98008> (Last accessed: 18.10.2022)
26. Regulation (EU) 2021/784 of the European Parliament and of the Council on addressing the dissemination of terrorist content online. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32021R07> (Last accessed: 17.10.2022)
27. Resolution adopted by the General Assembly 66/178. Technical assistance for implementing the international conventions and protocols related to counter-terrorism. URL: [https://www.unodc.org/documents/commissions/CCPCJ/Crime\\_Resolutions/2010-2019/2011/General\\_Assembly/Resolution\\_66-178.pdf](https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2011/General_Assembly/Resolution_66-178.pdf) (Last accessed: 19.10.2022)
28. Resolution adopted by the General Assembly on 26 June 2018. URL: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/198/80/PDF/N1819880.pdf?OpenElement> (Last accessed: 22.10.2022)

### **Інтернет-ресурси**

29. Алексеєнко Ю. О. Соціальні медіа як основа інформаційно-мережевого суспільства. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Філологія. Журналістика*. 2021. Том 32. № 2. Ч. 2. С. 204-208. URL: [https://www.philol.vernadskyjournals.in.ua/journals/2021/2\\_2021/part\\_2/38.pdf](https://www.philol.vernadskyjournals.in.ua/journals/2021/2_2021/part_2/38.pdf) (Last accessed: 26.11.2022)

30. Банк Р. О. Інформаційний тероризм як загроза національній безпеці України: теоретико-правовий аспект. *Інформація і право*. 2016. № 1(16). С. 110-116. URL: <http://ippi.org.ua/sites/default/files/17.pdf> (Last accessed: 12.11.2022)
31. Білаш О. В., Сорокатиий М. І., Ковальчук Р. А. Контроль над інформаційним простором – необхідна умова у боротьбі з проявами сепаратизму та тероризму. *Протидія проявам тероризму, сепаратизму, екстремізму та нелегальній міграції в сучасних умовах: стан, проблеми та перспективи*: матеріали Міжнар. наук.-практ. конф. (м. Дніпро, 28 жовт. 2016 р.). Дніпро: Дніпроп. держ. ун-т внутр. справ, 2016. С. 302-304. URL: <https://dduvs.in.ua/wp-content/uploads/files/Structure/library/student/20161103.pdf> (Last accessed: 21.10.2022)
32. В Европе задержали 13 джихадистов. *DELFI*. 12.11.2015. URL: <https://www.delfi.lt/ru/abroad/global/v-evrope-zaderzhali-13-dzhihadistov.d?id=69558786> (Last accessed: 19.10.2022)
33. Григорова З. В. Нові медіа, соціальні медіа, соціальні мережі — ієрархія інформаційного простору. *Збірник наукових праць «Технологія і техніка друкарства»*. 2017. № 3. С. 93-100. URL: [https://ela.kpi.ua/bitstream/123456789/22642/1/10\\_hryhorova\\_zv\\_new\\_media.pdf](https://ela.kpi.ua/bitstream/123456789/22642/1/10_hryhorova_zv_new_media.pdf) (Last accessed: 24.11.2022)
34. Гриник Р. О., Пилипенко В. М. Кібертероризм як нова форма міжнародного тероризму. *Актуальні задачі та досягнення у галузі кібербезпеки*: матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23-25 листопада 2016 р. Кропивницький: КНТУ, 2016. С. 61-62. URL: <https://sci.ldubgd.edu.ua/bitstream/123456789/3203/1/13.pdf> (Last accessed: 17.11.2022)
35. Ерохина Т. В. Влияние медиа-тероризма на массовое сознание. URL: [https://virtkafedra.ucoz.ua/el\\_gurnal/pages/vyp11/3/Erohina\\_copy.pdf](https://virtkafedra.ucoz.ua/el_gurnal/pages/vyp11/3/Erohina_copy.pdf) (Last accessed: 16.11.2022)

36. Єрохіна Т. В. Медіа-тероризм та інформаційна війна: до питання співвідношення. *Освіта регіону*. 2013. № 4. С. 171-175. URL: <https://social-science.uu.edu.ua/article/1201> (Last accessed: 23.11.2022)
37. Єрохіна Т. В. Проблема визначення поняття «медіа-тероризм». *Освіта регіону*. 2012. № 1. С. 202-206. URL: <https://social-science.uu.edu.ua/article/751> (Last accessed: 16.11.2022)
38. Ілляшенко А. В., Кияшко Ю. М. Інформаційний тероризм як злочинна діяльність міжнародного масштабу. *Журнал східноєвропейського права*. 2016. № 27. С. 94-100. URL: [http://easternlaw.com.ua/wp-content/uploads/2016/05/illiashenko\\_kiiashko\\_27.pdf](http://easternlaw.com.ua/wp-content/uploads/2016/05/illiashenko_kiiashko_27.pdf) (Last accessed: 22.11.2022)
39. Каплуненко В. О., Бондаренко С. В. Основні підходи до визначення поняття соціальні медіа (огляд зарубіжних та вітчизняних досліджень). *Вісник студентського наукового товариства ДонНУ ім. Василя Стуса*. 2020. № 12. С. 236-240. URL: <https://jvestnik-sss.donnu.edu.ua/article/view/9274/9218> (Last accessed: 22.11.2022)
40. Карпчук Н. П. Ініціативи Європейського Союзу в боротьбі з пропагандою тероризму. *Політичні науки*. 2020. № 2. С. 15-20. URL: [https://science.lpnu.ua/sites/default/files/journal-paper/2020/nov/22649/karpchuk220201520\\_1.pdf](https://science.lpnu.ua/sites/default/files/journal-paper/2020/nov/22649/karpchuk220201520_1.pdf) (Last accessed: 19.10.2022)
41. Кіслов Д. В. Трансформаційні процеси медіа-безпеки та медіа-тероризму. *Інформація і право*. 2011. № 2. С. 114-122. URL: <http://ippi.org.ua/sites/default/files/11kdmbmt.pdf> (Last accessed: 17.11.2022)
42. Коваль І. Террористы получают указания от ИГ по интернету. *Deutsche Welle*. 14.09.2016. URL: <https://www.dw.com/ru/%D0%B3%D0%BB%D0%B0%D0%B2%D0%B0-%D0%BF%D0%BE%D0%BB%D0%B8%D1%86%D0%B5%D0%B9%D1%81%D0%BA%D0%BE%D0%B9-%D1%81%D0%BF%D0%B5%D1%86%D1%81%D0%BB%D1%83%D0%B6%D0%B1%D1%8B-%D1%84%D1%80%D0%B3->

%D1%82%D0%B5%D1%80%D1%80%D0%BE%D1%80%D0%B8%D1%81%D1%82%D1%8B-

%D0%BF%D0%BE%D0%BB%D1%83%D1%87%D0%B0%D1%8E%D1%82-%D1%83%D0%BA%D0%B0%D0%B7%D0%B0%D0%BD%D0%B8%D1%8F-%D0%BE%D1%82-%D0%B8%D0%B3-%D0%BF%D0%BE-

%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D1%83/a-19550224 (Last accessed: 12.10.2022)

43. Кондратенко М. Рада Європи попереджає про зростання загрози біотерактів. *Deutsche Welle*. 25.05.2020. URL:

[https://www.dw.com/uk/%D0%BD%D0%B0%D1%81%D0%BB%D1%96%D0%B4%D0%BA%D0%B8-](https://www.dw.com/uk/%D0%BD%D0%B0%D1%81%D0%BB%D1%96%D0%B4%D0%BA%D0%B8-%D0%BF%D0%B0%D0%BD%D0%B4%D0%B5%D0%BC%D1%96%D1%97-%D1%83-%D1%80%D0%B0%D0%B4%D1%96-%D1%94%D0%B2%D1%80%D0%BE%D0%BF%D0%B8-%D0%BF%D0%BE%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D0%B8%D0%BB%D0%B8-%D0%BF%D1%80%D0%BE-%D0%B7%D0%B0%D0%B3%D1%80%D0%BE%D0%B7%D1%83-%D0%B1%D1%96%D0%BE%D1%82%D0%B5%D1%80%D0%B0%D0%BA%D1%82%D1%96%D0%B2/a-53554895)

%D0%BF%D0%B0%D0%BD%D0%B4%D0%B5%D0%BC%D1%96%D1%97-%D1%83-%D1%80%D0%B0%D0%B4%D1%96-

%D1%94%D0%B2%D1%80%D0%BE%D0%BF%D0%B8-

%D0%BF%D0%BE%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D0%B8%D0%BB%D0%B8-%D0%BF%D1%80%D0%BE-

%D0%B7%D0%B0%D0%B3%D1%80%D0%BE%D0%B7%D1%83-

%D0%B1%D1%96%D0%BE%D1%82%D0%B5%D1%80%D0%B0%D0%BA%D1%82%D1%96%D0%B2/a-53554895 (Last accessed: 05.11.2022)

44. Кореньков О. Політична стратегія й структура організації «Ісламська держава Іраку й Леванту». *Politicus*. 2017. Вип. 1. С. 186-190. URL: <https://philarchive.org/archive/KOR-13> (Last accessed: 15.10.2022)

45. Кореньков О. Стратегія виснаження терористів «Ісламської держави» на прикладі кампанії в Іраку в травні-червні 2019 року. *Politicus*. 2020. № 2. С. 139-154. URL: [http://politicus.od.ua/2\\_2020/22.pdf](http://politicus.od.ua/2_2020/22.pdf) (Last accessed: 23.11.2022)

46. Леонов Б. Д., Лихова С. Я. Інформаційний тероризм як загроза національній безпеці України. *Юридичний вісник*. 2021. № 2. С. 170-176. URL: <https://er.nau.edu.ua/bitstream/NAU/53546/1/22858.pdf> (Last accessed: 12.11.2022)

47. Леонов Б. Д. Тероризм в аспекті діяльності засобів масової інформації. *Інформація і право*. 2014. № 1. С. 87-92. URL: <http://ippi.org.ua/sites/default/files/14lbdzmi.pdf> (Last accessed: 13.11.2022)
48. Мазур П., Нетреба А. Е-джихад. Інформаційна боротьба Аль-Каїди й Ісламської держави на «Стежці Бога»: вибрані приклади. *Міжнародні відносини, суспільні комунікації, регіональні студії*. 2020. № 1. С. 81-93. URL: <https://relint.vnu.edu.ua/index.php/relint/article/view/130/115> (Last accessed: 24.11.2022)
49. Марутян Р. «Кібер-халіфат» ІДІЛ. *Matrix-divergent*. 05.04.2018. URL: <https://matrix-info.com/kiber-halifat-idil/> (Last accessed: 16.10.2022)
50. Медіа-імперія ІДІЛ. Як терористи виграють війну в соціальних медіа. Дослідження. *TEXTY.ORG.UA*. 13.05.2016. URL: [https://texty.org.ua/articles/67603/Mediaimperija\\_IDIL\\_Jak\\_terorysty\\_vygrajut\\_vijnu\\_v-67603/](https://texty.org.ua/articles/67603/Mediaimperija_IDIL_Jak_terorysty_vygrajut_vijnu_v-67603/) (Last accessed: 23.09.2022)
51. Медіа-тероризм: тепер і в Україні? *Детектор медіа*. 21.05.2002. URL: <https://detector.media/community/article/444/2002-05-21-media-teroryzm-teper-i-v-ukraini-/> (Last accessed: 22.11.2022)
52. НАТО: блокування сайтів – питання безпеки, а не свободи слова. *BBC NEWS Україна*. 17.05.2017. URL: <https://www.bbc.com/ukrainian/news-39948904> (Last accessed: 17.10.2022)
53. Парфенюк І. М. Інформаційний тероризм як новітній засіб інформаційнопсихологічного впливу. *Digital media: становлення новітньої комунікації*: колект. монографія / за ред. М. М. Поплавського, Л. О. Кочубей. Київ: Вид. центр КНУКіМ, 2020. С. 107-119. URL: [http://kzgzih.knukim.edu.ua/images/nauka/kolektyvna-monohrafiia\\_digital-media-stanovlennia-novitnoi-komunikatsii.pdf](http://kzgzih.knukim.edu.ua/images/nauka/kolektyvna-monohrafiia_digital-media-stanovlennia-novitnoi-komunikatsii.pdf) (Last accessed: 24.11.2022)
54. Півоваров С. Довкола коронавірусу множаться теорії змови, але всі вони не нові. *Бабель*. 15.04.2020. URL: <https://babel.ua/texts/42060-navkolo-koronavirusu-mnozhatysya-teoriji-zmovi-ale-vsi-voni-ne-novi-ranishe-v-epidemiyah->

uzhe-zvinuvachuvali-yevrejiv-likariv-uryadi-y-telegrafni-droti (Last accessed: 04.11.2022)

55. Піпченко Н. О. Соціальні медіа як механізм забезпечення інтернет-комунікації у сфері зовнішньої політики. *Міжнародні відносини: політичні науки*. 2017. № 17. URL: [http://journals.iir.kiev.ua/index.php/pol\\_n/article/viewFile/3322/3001](http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/3322/3001) (Last accessed: 23.11.2022)

56. Покровська Н. В., Федорович М. М., Щербина М. О. Репрезентація університетських бібліотек у соціальних медіа. *Тези VI Міжнародної конференції*, м. Дніпро, НТБ ДНУЗТ, 7–8 жовтня 2021 р. URL: <http://eadnurt.diit.edu.ua/bitstream/123456789/14208/1/Pokrovska.pdf> (Last accessed: 22.11.2022)

57. Почепцов Г. Г. Поле битвы — соцмедиа. *Хвиля*. 22.02.2019. URL: <https://hvylya.net/analytics/society/pole-bitvyi-sotsmedia.html> (Last accessed: 24.11.2022)

58. Почепцов Г. Г. Социальные медиа как дружеские сети и как опасные ловушки. *Хвиля*. 22.05.2017. URL: <https://hvylya.net/analytics/society/sotsialnyie-media-kak-druzheskie-seti-i-kak-opasnyie-lovushki.html> (Last accessed: 24.11.2022)

59. Примбс Ш. Соціальні медіа для журналістів. Редакційна робота з Facebook, Twitter & Co / за загал. ред. В. Ф. Іванова (скорочено). Київ: Академія української преси, Центр вільної преси, 2018. 17 с. *Pressclub*. URL: [https://pressclub.te.ua/wp-content/uploads/2019/03/Stefan\\_Primbs\\_short.pdf](https://pressclub.te.ua/wp-content/uploads/2019/03/Stefan_Primbs_short.pdf) (Last accessed: 26.11.2022)

60. Пилипчук В., Дзьобань О. Глобальні виклики й загрози національній безпеці в інформаційній сфері. *Вісник Національної академії правових наук України*. 2014. № 3 (78). – С. 43-52. URL: [http://visnyk.kh.ua/web/uploads/pdf/ilovepdf\\_com-43-52.pdf](http://visnyk.kh.ua/web/uploads/pdf/ilovepdf_com-43-52.pdf) (Last accessed: 22.11.2022)



61. Саган О. В. Медіа-інформаційний тероризм у когнітивно-поведінковому підході. *Держава і право: Збірник наукових праць. Серія Політичні науки. Випуск 83 / Ін-т держави і права імені В. М. Корецького НАН України. Київ: Вид-во «Юридична думка», 2019. С. 14-26. URL: [http://idpnan.org.ua/files/2019/derjava-i-pravo.-politichni-nauki.-vipusk-83-\\_2019\\_.pdf](http://idpnan.org.ua/files/2019/derjava-i-pravo.-politichni-nauki.-vipusk-83-_2019_.pdf) (Last accessed: 21.11.2022)*
62. Саміло А. В., Повстин О.В., Купчак М. Я. Інформаційно-комунікативний вплив терористичних організацій як новий виклик українському суспільству. *Вісник ЛДУ БЖД. 2014. № 10. С. 151-157. URL: [https://ldubgd.edu.ua/sites/default/files/files/18\\_6.pdf](https://ldubgd.edu.ua/sites/default/files/files/18_6.pdf) (Last accessed: 24.11.2022)*
63. СБУ затримала учасницю міжнародної терористичної організації «Ісламська держава» у Києві. *Служба Безпеки України. 06.08.2021. URL: <https://ssu.gov.ua/novyny/sbu-zatrymala-uchasnytsiu-mizhnarodnoi-terorystychnoi-orhanizatsii-islamska-derzhava-u-kyievi> (Last accessed: 21.10.2022)*
64. СБУ спільно з Інтерполом затримала учасника міжнародної терористичної організації «Ісламська держава» на Одещині. *Служба Безпеки України. 09.09.2021. URL: <https://ssu.gov.ua/novyny/sbu-spilno-z-interpolom-zatrymala-uchasnyka-mizhnarodnoi-terorystychnoi-orhanizatsii-islamska-derzhava-na-odeshchyni> (Last accessed: 21.10.2022)*
65. Собецька Я., Спирін Є. Терористи «Ісламської держави» на випадок відродження створили «резервну копію» ІДІЛ. У архів чотири тисячі папок з інструкціями, як робити бомби та викрадати літаки – переказуємо матеріали Wired. *Бабель. 10.09.2020. URL: <https://babel.ua/texts/50898-teroristi-islamskoji-derzhavi-na-vipadok-vidrozhennya-stvorili-rezervnu-kopiyu-idil-u-arhivi-chotiritisyachi-papok-z-instrukciyami-yak-robiti-bombi-ta-vikradati-litaki-perekazuemo-material-wired> (Last accessed: 16.10.2022)*
66. Стандарти спільноти Facebook. Небезпечні особи й організації. *META. URL: <https://transparency.fb.com/ru-ru/policies/community-standards/dangerous-individuals-organizations/> (Last accessed: 25.10.2022)*

67. Субота І. Пошукові системи та соціальні медіа — найпопулярніші джерела новин та інформації в Україні, — дослідження. *Інтернет свобода*. 06.10.2021. URL: <https://netfreedom.org.ua/article/poshukovi-sistemi-ta-socialni-media-najpopulyarnishi-dzherela-novin-ta-informaciyi-v-ukrayini-doslidzhennya> (Last accessed: 23.11.2022)
68. У Києві СБУ затримала іноземного бойовика МТО «Ісламська держава». *Служба Безпеки України*. 09.09.2022. URL: <https://ssu.gov.ua/novyny/u-kyievi-sbu-zatrymala-inozemnoho-boiovyka-mto-islamska-derzhava> (Last accessed: 21.10.2022)
69. Царьова І. В. Медіа-тероризм у контексті загрози національній безпеці України. *Протидія проявам тероризму, сепаратизму, екстремізму та нелегальній міграції в сучасних умовах: стан, проблеми та перспективи*: матеріали Міжнар. наук.-практ. конф. (м. Дніпро, 28 жовт. 2016 р.). Дніпро: Дніпроп. держ. ун-т внутр. справ, 2016. 356 с. URL: <https://dduvs.in.ua/wp-content/uploads/files/Structure/library/student/20161103.pdf> (Last accessed: 21.11.2022)
70. Чому ІДІЛ продовжує існування: терористи будують медіаімперію. *24 Канал*. 05.10.2020. URL: [https://24tv.ua/idil-teroristi-zalyakuyut-svit-cherez-media-ta-sotsmerezhi\\_n1429314](https://24tv.ua/idil-teroristi-zalyakuyut-svit-cherez-media-ta-sotsmerezhi_n1429314) (Last accessed: 07.10.2022)
71. Що таке PR? *Словник термінів*. URL: <https://pr-portal.com.ua/slovnyk> (Last accessed: 25.11.2022)
72. Що таке соціальні медіа? *Gadget-info*. URL: <https://uk.gadget-info.com/43430-what-is-social-media> (Last accessed: 25.11.2022)
73. Alexandra T. Evans, Heather J. Williams. How Extremism Operates Online. *RAND Corporations*. URL: <https://www.rand.org/pubs/perspectives/PEA1458-2.html> (Last accessed: 04.10.2022)
74. Alex P. Schmid. Handbook of Terrorism Prevention and Preparedness. The Hague, NL: *ICCT Press*. 2020. URL: <https://icct.nl/handbook-of-terrorism-prevention-and-preparedness/> (Last accessed: 08.10.2022)

75. An update on our efforts to combat violent extremism. *Blog.Twitter*. 18.08.2016. URL: [https://blog.twitter.com/en\\_us/a/2016/an-update-on-our-efforts-to-combat-violent-extremism](https://blog.twitter.com/en_us/a/2016/an-update-on-our-efforts-to-combat-violent-extremism) (Last accessed: 12.10.2022)
76. Attacking ISIL on Twitter: Addressing Ethical Responsibility in the Weaponization of Social Media. *Intersect*, Vol 10, № 2. 2017. URL: <https://ojs.stanford.edu/ojs/index.php/intersect/article/view/975> (Last accessed: 29.11.2022)
77. Bieda, D., Halawi, L. Cyberspace: A Venue for Terrorism. *Issues in Information Systems*, 16(3). 2015. C. 33-42. URL: <https://commons.erau.edu/cgi/viewcontent.cgi?article=1348&context=publication> (Last accessed: 31.10.2022)
78. Brian Michael Jenkins. Unconquerable Nation: Knowing Our Enemy Strengthening Ourselves. *RAND Corporation*. URL: <https://www.rand.org/pubs/monographs/MG454.html> (Last accessed: 09.11.2022)
79. Brigitte Nacos. Terrorism and Counterterrorism. New York, 2017. *Taylor & Francis Group*. URL: <https://www.taylorfrancis.com/books/mono/10.4324/9781315641270/terrorism-counterterrorism-brigitte-nacos?refId=cc458d28-71b4-4f8d-8b63-85957b53c199&context=ubx> (Last accessed: 26.11.2022)
80. Charlie Winter. Media Jihad: The Islamic State's Doctrine for Information Warfare. *The International Centre for the Study of Radicalisation (ICSR)*. 2017. URL: <https://icsr.info/wp-content/uploads/2017/02/ICSR-Report-Media-Jihad-The-Islamic-State%E2%80%99s-Doctrine-for-Information-Warfare.pdf>
81. Charlie Winter. The ISIS Propaganda Decline. *The International Centre for the Study of Radicalisation (ICSR)*. 2017. URL: <https://icsr.info/2017/03/23/isis-propaganda-decline/> (Last accessed: 30.09.2022)
82. Colin P. Clarke. Five Trends Driving the Future of Terrorism. *Foreign Policy Research Institute*. 02.09.2022. URL:

<https://www.fpri.org/article/2022/09/five-trends-driving-the-future-of-terrorism/> (Last accessed: 14.11.2022)

83. COUNTERTERRORISM YEARBOOK 2021. *The Australian Strategic Policy Institute Limited*. 2021. URL: <https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2021-03/ASPI%20Counterterrorism%20YB2021-v2.pdf?VersionId=qRIjpA0b0aLaWsvXREMAf8yo8I.uyWxN> (Last accessed: 04.11.2022)

84. Counter-terrorism: PCUITP. Preventing and Countering the Use of the Internet for Terrorist Purposes. *Organization for Security and Cooperation in Europe (OSCE)*. URL: [https://elearning.osce.org/courses/course-v1:OSCE+PCUITP+2020\\_1\\_EN/about](https://elearning.osce.org/courses/course-v1:OSCE+PCUITP+2020_1_EN/about) (Last accessed: 21.10.2022)

85. COVID-19 and global security: how terrorist adapted as the world shut down. *United Nations Office on Drugs and Crime (UNODC)*. URL: [https://www.unodc.org/unodc/frontpage/2021/July/covid-19-and-global-security\\_-how-terrorists-adapted-as-the-world-shut-down.html](https://www.unodc.org/unodc/frontpage/2021/July/covid-19-and-global-security_-how-terrorists-adapted-as-the-world-shut-down.html) (Last accessed: 10.10.2022)

86. CREST is the UK's hub for behavioural and social science research into security threats. URL: <https://crestresearch.ac.uk/about/> (Last accessed: 02.11.2022)

87. Cyber Counterterrorism, Cyber International Conflict, Virtual Cyber War Crimes. *Journal of L Technology Risk Management*. July, 2015. 152 c. URL: [https://books.google.com.ua/books?id=o5AXCgAAQBAJ&pg=PA6&lpg=PA6&dq=why+French+officials+made+87+percent+of+the+requests+to+remove+content+from+Twitter+in+the+second+half+of+2013&source=bl&ots=XUVpiISFPY&sig=ACfU3U2XpQlrN1NYgMITEk8F446FIdARUQ&hl=ru&sa=X&ved=2ahUKEwic-oGnmI\\_7AhVGpYsKHba5DLEQ6AF6BAg5EAM#v=onepage&q=why%20French%20officials%20made%2087%20percent%20of%20the%20requests%20to%20remove%20content%20from%20Twitter%20in%20the%20second%20half%20of%202013&f=false](https://books.google.com.ua/books?id=o5AXCgAAQBAJ&pg=PA6&lpg=PA6&dq=why+French+officials+made+87+percent+of+the+requests+to+remove+content+from+Twitter+in+the+second+half+of+2013&source=bl&ots=XUVpiISFPY&sig=ACfU3U2XpQlrN1NYgMITEk8F446FIdARUQ&hl=ru&sa=X&ved=2ahUKEwic-oGnmI_7AhVGpYsKHba5DLEQ6AF6BAg5EAM#v=onepage&q=why%20French%20officials%20made%2087%20percent%20of%20the%20requests%20to%20remove%20content%20from%20Twitter%20in%20the%20second%20half%20of%202013&f=false) (Last accessed: 02.1.2022)

88. Daniel Byman, Jeremy Shapiro. We shouldn't stop terrorists from tweeting. *Washingtonpost.com*. 09.10.2014. URL: [https://www.washingtonpost.com/opinions/we-shouldnt-stop-terrorists-from-](https://www.washingtonpost.com/opinions/we-shouldnt-stop-terrorists-from-tweeting/)

tweeting/2014/10/09/106939b6-4d9f-11e4-8c24-

487e92bc997b\_story.html?tid=a\_inl\_manual (Last accessed: 01.11.2022)

89. Donald Holbrook. The Islamic State And Ayman Al-Zawahiri's 'Alternative Jihad'. *Centre for Research and Evidence on Security Threats (CREST)*. 22.06.2014. URL: <https://crestresearch.ac.uk/comment/ayman-al-zawahiri-jihad-holbrook/> (Last accessed: 04.11.2022)

90. Dr. Gabriel Weimann, Asia Vellante. The Dead Drops of Online Terrorism. *International Institute for Counter-Terrorism (ICT)*. October 2021. URL: <https://ict.org.il/wp-content/uploads/2022/02/Dead-Drops-of-Online-Terrorism-2.pdf> (Last accessed: 28.10.2022)

91. Dr. Jarrod Sadulski. Why Social Media Is So Appealing to Terrorist Organizations. *American Public University System (APUS)*. 05.10.2022. URL: <https://amuedge.com/why-social-media-is-so-appealing-to-terrorist-organizations/> (Last accessed: 01.11.2022)

92. Efe Kerem Sözeri. Turkey Blocks News Sites, Twitter, Facebook. After Deadly Attack. *Vocativ*. 28.06.2016. URL: <https://www.vocativ.com/334890/turkey-blocks-news-sites-twitter-facebook-after-deadly-attack/> (Last accessed: 02.11.2022)

93. Evolution of Terrorism: How Society and Institutions Are Adapting? *World Economic Forum Annual Meeting*. 23.01.2019. URL: <https://www.weforum.org/events/world-economic-forum-annual-meeting-2019/sessions/space-the-strategic-frontier> (Last accessed: 10.10.2022)

94. Farah Pandith. Teen terrorism inspired by social media is on the rise. Here's what we need to do. *NBC News Digital*. 22.03.2021. URL: <https://www.nbcnews.com/think/opinion/teen-terrorism-inspired-social-media-rise-here-s-what-we-ncna1261307rise-here-s-what-we-ncna1261307> (Last accessed: 28.11.2022)

95. Find the latest news, stories, reports, publications and more. *The Office of the High Commissioner for Human Rights (OHCHR)*. URL: [https://www.ohchr.org/en/latest?hide\\_hero\\_cards=TRUE&field\\_content\\_category\\_ta](https://www.ohchr.org/en/latest?hide_hero_cards=TRUE&field_content_category_ta)

rget\_id%5B187%5D=187&field\_content\_category\_target\_id%5B190%5D=190&field\_content\_category\_target\_id%5B189%5D=189 (Last accessed: 18.10.2022)

96. Florez A. Radicalization Through the Internet: How ISIS Became So Successful and Why the United States Needs to Catch Up. *The Office of the High Commissioner for Human Rights (OHCHR)*. 18.05.2019. URL: [https://research.library.fordham.edu/cgi/viewcontent.cgi?article=1020&context=international\\_senior](https://research.library.fordham.edu/cgi/viewcontent.cgi?article=1020&context=international_senior) (Last accessed: 15.10.2022)

97. Fredrick Swenson. Research Paper-Terrorism and Mass Media. *ResearchGate GmbH*. 05.2014. URL: [https://www.researchgate.net/publication/261176593\\_Research\\_Paper-Terrorism\\_and\\_Mass\\_Media](https://www.researchgate.net/publication/261176593_Research_Paper-Terrorism_and_Mass_Media) (Last accessed: 14.11.2022)

98. French gunman buried after terror attacks. *CBC/Radio-Canada*. 29.03.2012. URL: <https://www.cbc.ca/news/world/french-gunman-buried-after-terror-attacks-1.1192530> (Last accessed: 04.10.2022)

99. G20 leaders resolve to prevent use of internet for terrorism. *The Economic Times. Politics*. 29.06.2019. URL: <https://economictimes.indiatimes.com/news/politics-and-nation/g20-leaders-resolve-to-prevent-use-of-internet-for-terrorism-extremism/articleshow/70003214.cms?from=mdr> (Last accessed: 10.10.2022)

100. Gabriel Weimann How Modern Terrorism Uses the Internet. *The United States Institute of Peace*. 03.2004. URL: <https://www.usip.org/sites/default/files/sr116.pdf> (Last accessed: 19.10.2022)

101. Gambhir H. The Virtual Caliphate ISIS's Information Warfare. *The Institute for the Study of War*. 2016. URL: <https://www.understandingwar.org/sites/default/files/ISW%20The%20Virtual%20Caliphate%20Gambhir%202016.pdf> (Last accessed: 14.10.2022)

102. Generation Z: Global Citizenship Survey. *VARKEY FOUNDATION*. URL: <https://www.varkeyfoundation.org/what-we-do/research/generation-z-global-citizenship-survey> (Last accessed: 03.10.2022).

103. Gordon Corera. ISIS 'still evading detection on Facebook', report says. *BBC News*. 13.07.2020. URL: <https://www.bbc.com/news/technology-53389657> (Last accessed: 01.11.2022)
104. Guantanamo Yemeni claims al Qaeda's «best» video. *Reuters*. 29.10.2008. URL: <https://www.reuters.com/article/us-guantanamo-hearings-idUSTRE49R5OZ20081029> (Last accessed: 19.10.2022)
105. Gulnara Akhundova, Emma Lygnerud Boberg. The right to know and the duty to protect: terrorism and the media. *International Media Support (IMS)*. 25.01.2021. URL: <https://www.mediasupport.org/blogpost/the-right-to-know-and-the-duty-to-protect-terrorism-and-the-media/> (Last accessed: 28.11.2022)
106. Haroro J. Ingram How ISIS survives defeat: propaganda and decisive minorities. *CAÏT* 26.09.2016. URL: <https://sustainablesecurity.org/2016/09/26/how-isis-survives-defeat-propaganda-and-decisive-minorities/> (Last accessed: 01.10.2022)
107. Help Center/Safety and cybercrime. Violent organizations policy. *Twitter, Inc.* October, 2020. URL: <https://help.twitter.com/en/rules-and-policies/violent-groups> (Last accessed: 25.10.2022)
108. High court will hear social media terrorism lawsuits. *THE FREE SPEECH CENTER*. 04.10.2022. URL: <https://www.mtsu.edu/first-amendment/post/3447/high-court-will-hear-social-media-terrorism-lawsuits> (Last accessed: 02.11.2022)
109. Hope King. Facebook and Twitter suspend suspected shooter's accounts. *CNN Business*. 26.08.2015. URL: <https://money.cnn.com/2015/08/26/technology/facebook-twitter-virginia-shooter/?iid=EL> (Last accessed: 25.10.2022)
110. Hoffman B. Inside Terrorism. *Columbia University Press. Books*. URL: [https://archive.nytimes.com/www.nytimes.com/books/first/h/hoffman-terrorism.html?\\_r=1](https://archive.nytimes.com/www.nytimes.com/books/first/h/hoffman-terrorism.html?_r=1) (Last accessed: 24.11.2022)
111. Hoffman B. Oblicza terroryzmu. *New York: Columbia university Press. Docer*. URL: <https://docer.pl/doc/n0cc5s0> (Last accessed: 08.10.2022)

112. Hoffman B. The Use of the Internet by Islamic Extremists. *RAND Corporation*. 2006. URL: [https://www.rand.org/content/dam/rand/pubs/testimonies/2006/RAND\\_CT262-1.pdf](https://www.rand.org/content/dam/rand/pubs/testimonies/2006/RAND_CT262-1.pdf) (Last accessed: 24.11.2022)
113. Isis' new magazine Rumiya shows the terror group is 'struggling to adjust to losses'. *The Independent*. 06.09.2016. URL: <https://www.independent.co.uk/news/world/middle-east/isis-propaganda-terror-group-losses-syria-iraq-a7228286.html> (Last accessed: 02.10.2022)
114. Jihadis and the internet. *Intelligence Resource Program*. 2007. URL: <https://irp.fas.org/world/netherlands/jihadis.pdf> (Last accessed: 17.10.2022)
115. Joint declaration on freedom of expression and “fake news”, disinformation and propaganda. *Детектор Медиа*. 06.03.2012. URL: <https://detector.media/infospace/article/123841/2017-03-06-feyky-slid-rozvinchuvaty-v-novynakh-a-ne-nakladaty-na-nykh-zagalnu-zaboronu-spilna-deklaratsiya-oon-obsie-o-ad-i-afryky/> (Last accessed: 18.10.2022)
116. Joint Declaration on Freedom of Expression and responses to conflict situations. *The Office of the High Commissioner for Human Rights (OHCHR)*. 04.05.2015. URL: <https://www.ohchr.org/en/statements/2015/05/joint-declaration-freedom-expression-and-responses-conflict-situations> (Last accessed: 18.10.2022)
117. Joint Letter to EU Parliament: Vote Against Proposed Terrorist Content Online Regulation. *Human Rights Watch*. 25.03.2021. URL: <https://www.hrw.org/news/2021/03/25/joint-letter-eu-parliament-vote-against-proposed-terrorist-content-online> (Last accessed: 04.10.2022)
118. Julie Coleman J.D. *The Impact of Coronavirus on Terrorism in the Sahel (ICCT)*. 16.04.2020. URL: <https://icct.nl/publication/the-impact-of-coronavirus-on-terrorism-in-the-sahel/> (Last accessed: 11.10.2022)
119. Julie Flint. Covid-19 and its impact on extremist groups' use of IEDs. *Action on Armed Violence*. 03.03.2022. URL: <https://aoav.org.uk/2022/covid-19-and-its-impact-on-extremist-groups-use-of-ieds/> (Last accessed: 03.11.2022)



120. Kathleen Chaykowski. Terrorism Suspect's Use Of 'Facebook Live' Stream Highlights Challenges Of Live Video. *Forbes*. 15.06.2016. URL: <https://www.forbes.com/sites/kathleenchaykowski/2016/06/15/terrorist-suspects-use-of-facebook-live-stream-highlights-challenges-of-live-video/?sh=24bb2b492408> (Last accessed: 27.10.2022)
121. Kevin Roose. A Mass Murder of, and for, the Internet. *The New York Times*. 15.03.2019. URL: <https://www.nytimes.com/2019/03/15/technology/facebook-youtube-christchurch-shooting.html> (Last accessed: 31.10.2022)
122. Kos A. Theoretical aspects of terrorism. Globalization, the State and the Individual. 2017. № 4(16). P. 39-47. *GSI JOURNAL*. URL: <http://www.gsjournal.bg/gsjournal/images/dok/GSI16/Kos.pdf> - 08.10.2022 (Last accessed: 08.10.2022)
123. Lidia Dutkiewicz, Noemiek Krack. All eyes riveted on the trilogue closed doors of the Proposal for a Regulation on preventing the dissemination of terrorist content online [Part I]. *KU Leuven Centre for IT & IP Law*. 24.11.2020. URL: <https://www.law.kuleuven.be/citip/blog/all-eyes-riveted-on-the-trilogue-closed-doors-of-the-proposal-for-a-regulation-on-preventing-the-dissemination-of-terrorist-content-online-part-i/> (Last accessed: 04.10.2022)
124. Luke Bertram. Terrorism, the Internet and the Social Media Advantage: Exploring how terrorist organizations exploit aspects of the internet, social media and how these same platforms could be used to counter-violent extremism. *Doaj*. 06.2016. URL: <https://doaj.org/article/660ec5b479604e06a89a886e2cfa7a40> (Last accessed: 29.10.2022)
125. Man Sentenced to 20 Years in Prison for Attempting to Provide Material Support to ISIS. *Department of Justice*. 07.07.2022. URL: <https://www.justice.gov/opa/pr/man-sentenced-20-years-prison-attempting-provide-material-support-isis-1> (Last accessed: 02.11.2022)

126. Marguerite Borelli. Social media corporations as actors of counter-terrorism. *SAGE Publishing*. 08.2021. URL: <https://journals.sagepub.com/doi/full/10.1177/14614448211035121#con> (Last accessed: 26.11.2022)

127. Maya Dollarhide. Social Media: Definition, Effects, and List of Top Apps. *Investopedia*. 31.08.2021. URL: <https://www.investopedia.com/terms/s/social-media.asp> (Last accessed: 10.11.2022)

128. Mia Bloom. Islamic State Messaging On Telegram. *Centre for Research and Evidence on Security Threats*. 28.08.2017. URL: <https://crestresearch.ac.uk/comment/islamic-state-messaging-telegram/> (Last accessed: 02.11.2022)

129. Michele Grossman. How Has COVID-19 Changed The Violent Extremist Landscape? *Centre for Research and Evidence on Security Threats*. 15.10.2021. URL: <https://crestresearch.ac.uk/comment/how-has-covid-19-changed-the-violent-extremist-landscape/> (Last accessed: 05.11.2022)

130. Michael Jetter. Terrorism and the Media: The Effect of US Television Coverage on Al-Qaeda Attacks. *IZA*. 04.2017. URL: <https://www.iza.org/publications/dp/10708/terrorism-and-the-media-the-effect-of-us-television-coverage-on-al-qaeda-attacks> (Last accessed: 10.11.2022)

131. Miles Comerford. How have terrorist organisations responded to COVID-19? *Institute for Economics & Peace*. URL: <https://www.visionofhumanity.org/how-have-terrorist-organisations-responded-to-covid-19/> (Last accessed: 04.11.2022)

132. NEPLP aizliedz Krievijas kanālu "Rossija RTR" un "Rossija 24" retranslāciju Latvijā. Portāls „Sargs.lv”. *SARGA.Lv*. 24.02.2022. URL: <https://www.sargs.lv/lv/sabiedriba/2022-02-24/neplp-aizliedz-krievijas-kanalu-rossija-rtr-un-rossija-24-retranslaciju> (Last accessed: 25.11.2022)

133. New EU regulation will help counter the spread of extremist ideologies on the Internet. *European Conservatives and Reformists*. 24.04.2021. URL:

[https://ecrgroup.eu/article/new\\_eu\\_regulation\\_will\\_help\\_counter\\_the\\_spread\\_of\\_extremist\\_ideologies\\_on\\_t](https://ecrgroup.eu/article/new_eu_regulation_will_help_counter_the_spread_of_extremist_ideologies_on_t) (Last accessed: 05.10.2022)

134. Online Jihadist Propaganda 2021 in review, Publications Office of the European Union, Luxembourg. *European Union Agency for Law Enforcement Cooperation (Europol)*. 2022. URL: [https://www.europol.europa.eu/cms/sites/default/files/documents/Online\\_Jihadist\\_Propaganda\\_2021\\_in\\_review.pdf](https://www.europol.europa.eu/cms/sites/default/files/documents/Online_Jihadist_Propaganda_2021_in_review.pdf) (Last accessed: 17.10.2022)

135. Paweł Kmieciak. MEDIA SPOŁECZNOŚCIOWE W SŁUŻBIE TERRORYSTÓW. *FORBS*. 30.01.2015. URL: <https://www.forbes.com/sites/realspin/2015/01/30/terrorist-use-of-u-s-social-media-is-a-national-security-threat/?sh=76a2f40a4761> (Last accessed: 31.10.2022)

136. Readout of the Meeting of the Small Group of the Global Coalition To Defeat ISIS in Jordan. *Media Note Office of the Spokesperson*. 15.11.2017. URL: <https://2017-2021.state.gov/readout-of-the-meeting-of-the-small-group-of-the-global-coalition-to-defeat-isis-in-jordan/index.html> (Last accessed: 13.10.2022)

137. Sara Malm. Flames of War: ISIS threatens attacks on the US in latest propaganda video where they continue to insist that they were behind Las Vegas shooting. *MailOnline*. 30.11.2017. URL: <https://www.dailymail.co.uk/news/article-5132459/ISIS-threatens-attacks-new-propaganda-video.html> (Last accessed: 02.10.2022)

138. Shelby Hoffman. Terrorism and the Media: How ISIL Benefits from news Coverage. *Institute for Economics*. URL: <https://www.visionofhumanity.org/media-coverage-and-terrorism/> (Last accessed: 27.09.2022)

139. Shelley Walsh. What Is Social Media? *Search Engine Journal*. 18.08.2022. URL: <https://www.searchenginejournal.com/social-media/> (Last accessed: 22.11.2022)

140. Simon Kemp. DIGITAL 2022: GLOBAL OVERVIEW REPORT. *DataReportal*. 26.01.2022. URL: <https://datareportal.com/reports/digital-2022-global-overview-report> (Last accessed: 10.11.2022)
141. Simon Kemp. LOOKING AHEAD: KEY DIGITAL THEMES FOR 2023. *DataReportal*. 07.10.2022. URL: <https://datareportal.com/reports/looking-ahead-to-what-2023-holds> (Last accessed: 10.11.2022)
142. Smith L. Messaging app Telegram centrpiece of IS social media strategy. *BBC News*. 05.06.2017. URL: <https://www.bbc.com/news/technology-39743252> (Last accessed: 11.10.2022)
143. Social Media and Terrorist Organizations: Observing Success of Recruitment Through Social Media. *University of Central Florida*. 2017. URL: <https://stars.library.ucf.edu/cgi/viewcontent.cgi?article=1339&context=honorsthesis> (Last accessed: 11.10.2022)
144. Social media. *Encyclopedia Britannica*. URL: <https://www.britannica.com/topic/social-media> (Last accessed: 20.11.2022)
145. Social media. *Merriam-Webster, Incorporated*. URL: <https://www.merriam-webster.com/dictionary/social%20media> (Last accessed: 20.11.2022)
146. Sopilko I. N., Medvedieva M. O., Arif G. Guliev, Bilotsky S. D., Bukhanevych O. N., Sirokha D. I., Terekhova T. A. *Journal of Legal, Ethical and Regulatory Issues*. Volume 21, Issue 2, 2018. URL: <https://www.abacademies.org/articles/international-terrorism-and-mass-media-7313.html> (Last accessed: 24.11.2022)
147. The Cambridge Dictionary. URL: <https://dictionary.cambridge.org/dictionary/english/social-media> (Last accessed: 09.11.2022)
148. The cost of terrorism in Europe. *RAND Europe*. URL: <https://www.rand.org/randeurope/research/projects/the-cost-of-terrorism-in-europe.html> (Last accessed: 05.10.2022)

149. The impact of COVID-19 pandemic on terrorism, counter-terrorism and countering violent extremism. *Un.org*. December 2020. URL: [https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted\\_paper\\_the-impact-of-the-covid-19-pandemic-on-counter-te.pdf](https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted_paper_the-impact-of-the-covid-19-pandemic-on-counter-te.pdf) (Last accessed: 10.10.2022)

150. The Islamic State's Doctrine for Information Warfare. *The International Centre for the Study of Radicalisation (ICSR)*. 2017. URL: <https://icsr.info/wp-content/uploads/2017/02/ICSR-Report-Media-Jihad-The-Islamic-State%E2%80%99s-Doctrine-for-Information-Warfare.pdf> (Last accessed: 30.09.2022)

151. The use of the Internet for terrorist purposes. United Nations New York, 2012. 144 p. *United Nations Office on Drugs and Crime (UNODC)*. URL: [https://www.unodc.org/documents/terrorism/Publications/Use\\_of\\_Internet\\_for\\_Terrorist\\_Purposes/ebook\\_use\\_of\\_the\\_internet\\_for\\_terrorist\\_purposes.pdf](https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/ebook_use_of_the_internet_for_terrorist_purposes.pdf) (Last accessed: 18.10.2022)

152. The US is losing the propaganda war against al-Qaeda and other enemies, defence chief Donald Rumsfeld has said. *BBC News*. 17.02.2006. URL: <http://news.bbc.co.uk/2/hi/americas/4725992.stm> (Last accessed: 02.10.2022)

153. The Weaponization of social media. How social media can spark violence and what can be done about it. *MERCY CORPS*. November 2019. URL: [https://www.mercycorps.org/sites/default/files/2020-01/Weaponization\\_Social\\_Media\\_FINAL\\_Nov2019.pdf](https://www.mercycorps.org/sites/default/files/2020-01/Weaponization_Social_Media_FINAL_Nov2019.pdf) (Last accessed: 14.10.2022)

154. Tiana Gaudette, Ryan Scrivens, Vivek Venkatesh. The Role of the Internet in Facilitating Violent Extremism: Insights from Former Right-Wing Extremists. *ResearchGate GmbH*. July 2020. URL: [https://www.researchgate.net/publication/342992254\\_The\\_Role\\_of\\_the\\_Internet\\_in\\_Facilitating\\_Violent\\_Extremism\\_Insights\\_from\\_Former\\_Right-Wing\\_Extremists](https://www.researchgate.net/publication/342992254_The_Role_of_the_Internet_in_Facilitating_Violent_Extremism_Insights_from_Former_Right-Wing_Extremists) (Last accessed: 27.10.2022)

155. Tim Hume, Lindsay Isaac and Paul Cruickshank. French terror attacker threatened Euro 2016 in Facebook video, source says. *Cable News Network (CNN)*. 14.06.2016. URL: <http://edition.cnn.com/2016/06/14/europe/french-policeman-terror-attack/> (Last accessed: 24.10.2022)

156. Tom Risen. Twitter, Facebook, YouTube Grapple With Islamic State Censorship. *U.S. News & World Report L.P.* 05.09.2014. URL: <https://www.usnews.com/news/articles/2014/09/05/twitter-facebook-youtube-navigate-islamic-state-censorship> (Last accessed: 02.11.2022)

157. Ukraine: Revoke Ban on Dozens of Russian Web Companies. *Human Rights Watch*. 16.05.2017. URL: <https://www.hrw.org/news/2017/05/16/ukraine-revoke-ban-dozens-russian-web-companies> (Last accessed: 18.10.2022)

158. What Islamists Are Doing and Saying on COVID-19 Crisis? *Wilson Center*. 14.05.2020. URL: <https://www.wilsoncenter.org/article/what-islamists-are-doing-and-saying-covid-19-crisis> (Last accessed: 11.10.2022)

159. Without internet, phone, Osama depended on couriers: NYT. *TwoCircles.net* (TCN). 08.05.2011. URL: [http://twocircles.net/2011may08/without\\_internet\\_phone\\_osama\\_depended\\_couriers\\_nyt.html](http://twocircles.net/2011may08/without_internet_phone_osama_depended_couriers_nyt.html) (Last accessed: 15.10.2022)

### **Інформаційні ресурси**

160. 2020 in review: New Europol threat assessment on IS and al-Qaeda's battle for relevance. *European Union Agency for Law Enforcement Cooperation (Europol)*. 13.08.2021. URL: <https://www.europol.europa.eu/media-press/newsroom/news/2020-in-review-new-europol-threat-assessment-and-al-qaeda%e2%80%99s-battle-for-relevance> (Last accessed: 07.11.2022)

161. ABDUL MOHSEN ABDALLAH IBRAHIM AL CHAREKH. UNITED NATIONS SECURITY COUNCIL. URL: [https://www.un.org/securitycouncil/sanctions/1267/aq\\_sanctions\\_list/summaries/individual/abdul-mohsen-abdallah-ibrahim-al-charekh](https://www.un.org/securitycouncil/sanctions/1267/aq_sanctions_list/summaries/individual/abdul-mohsen-abdallah-ibrahim-al-charekh) (Last accessed: 19.10.2022);

AQSA MAHMOOD. UNITED NATIONS SECURITY COUNCIL. URL: [https://www.un.org/securitycouncil/ru/sanctions/1267/aq\\_sanctions\\_list/summaries/individual/aqsa-mahmood](https://www.un.org/securitycouncil/ru/sanctions/1267/aq_sanctions_list/summaries/individual/aqsa-mahmood) (Last accessed: 19.10.2022); OMAR ALI HUSSAIN. UNITED NATIONS SECURITY COUNCIL. URL: [https://www.un.org/securitycouncil/ru/sanctions/1267/aq\\_sanctions\\_list/summaries/individual/omar-ali-hussain](https://www.un.org/securitycouncil/ru/sanctions/1267/aq_sanctions_list/summaries/individual/omar-ali-hussain) (Last accessed: 19.10.2022)

162. A Counter-Terrorism Agenda for the EU: Anticipate, Prevent, Protect, Respond. *European Commission*. 09.12.2020. URL: [https://home-affairs.ec.europa.eu/system/files/2020-12/09122020\\_communication\\_commission\\_european\\_parliament\\_the\\_council\\_eu\\_agenda\\_counter\\_terrorism\\_po-2020-9031\\_com-2020\\_795\\_en.pdf](https://home-affairs.ec.europa.eu/system/files/2020-12/09122020_communication_commission_european_parliament_the_council_eu_agenda_counter_terrorism_po-2020-9031_com-2020_795_en.pdf) (Last accessed: 05.10.2022)

163. Amarnath Amarasingam, Shiraz Maher, Charlie Winter. How Telegram Disruption Impacts Jihadist Platform Migration (FULL REPORT). *Centre for Research and Evidence on Security Threats (CREST)*. 08.01.2021. URL: <https://crestresearch.ac.uk/resources/how-telegram-disruption-impacts-jihadist-platform-migration/> (Last accessed: 02.10.2022)

164. BBC Monitoring. 23.11.2017. URL: <https://monitoring.bbc.co.uk/product/c1dnnj2k> (Last accessed: 02.10.2022)

165. Broadening the GIFCT Hash-Sharing Database Taxonomy: An Assessment and Recommended Next Steps. *Global Internet Forum to Counter Terrorism (GIFCT)*. July 2021. URL: <https://gifct.org/wp-content/uploads/2021/07/GIFCT-TaxonomyReport-2021.pdf> (Last accessed: 05.10.2022)

166. Digital Markets Act: Commission welcomes political agreement on rules to ensure fair and open digital markets. *European Commission*. 25.03.2022. URL: [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_22\\_1978](https://ec.europa.eu/commission/presscorner/detail/en/IP_22_1978) (Last accessed: 19.10.2022)

167. Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment. *European Commission*. 23.04.2022. URL: [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_22\\_2545](https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545) (Last accessed: 19.10.2022)

168. Christchurch Call story. *CHRISTCHURCH CALL*. URL: <https://www.christchurchcall.com/about/the-christchurch-call-story/> (Last accessed: 31.10.2022)

169. Civil Society Empowerment Programme (CSEP). *European Commission*. URL: [https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran/civil-society-empowerment-programme\\_en](https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran/civil-society-empowerment-programme_en) (Last accessed: 31.10.2022)

170. Content Regulation in the Digital Age. Submission to the United Nations Special Rapporteur on the Right to Freedom of Opinion and Expression by the Association for Progressive Communications (APC). *The Office of the High Commissioner for Human Rights*. February 2018. URL: <https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/ContentRegulation/APC.pdf> (Last accessed: 05.10.2022)

171. Countering illegal hate speech online 5th evaluation of the Code of Conduct. *European Commission*. June 2020. URL: [https://ec.europa.eu/info/sites/default/files/codeofconduct\\_2020\\_factsheet\\_12.pdf](https://ec.europa.eu/info/sites/default/files/codeofconduct_2020_factsheet_12.pdf) (Last accessed: 17.10.2022)

172. Current Approaches to Terrorist and Violent Extremist Content among the Global Top 50 Online Content-Sharing Services. *Organisation for Economic Co-operation and Development (OECD)*. 14.08.2020. URL: [https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CD/EP\(2019\)15/FINAL&docLanguage=En](https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CD/EP(2019)15/FINAL&docLanguage=En) (Last accessed: 04.10.2022)

173. EU Internet Forum: Bringing together governments, Europol and technology companies to counter terrorist content and hate speech online. *European Commission*. 03.12.2015. URL:



[https://ec.europa.eu/commission/presscorner/detail/en/IP\\_15\\_6243](https://ec.europa.eu/commission/presscorner/detail/en/IP_15_6243) (Last accessed: 15.10.2022)

174. From traditional to online media: Best practices and perspectives/Ed. By M. Stone; Vienna: OSCE Representative on Freedom of the Media, 2013. 126 p. The Representative on Freedom of the Media. *Organization for Security and Cooperation in Europe (OSCE)*. URL: <https://www.osce.org/files/f/documents/5/b/102311.pdf> (Last accessed: 26.11.2022)

175. Global Internet Forum to Counter Terrorism. *Global Internet Forum to Counter Terrorism (GIFCT)*. URL: <https://gifct.org/> (Last accessed: 05.10.2022)

176. Hash-sharing database. *Global Internet Forum to Counter Terrorism (GIFCT)*. URL: <https://gifct.org/tech-innovation/> (Last accessed: 05.10.2022)

177. Implementing the European Agenda on Security – New measures to combat terrorism and illicit trafficking of firearms and use of explosives. *Commission européenne*. 02.12.2015. URL: [https://ec.europa.eu/commission/presscorner/detail/fr/MEMO\\_15\\_6219](https://ec.europa.eu/commission/presscorner/detail/fr/MEMO_15_6219) (Last accessed: 09.10.2022)

178. Incitement to Terrorism through the Media: UNODC organizes workshop on anti-terror law for Journalists, Security Agencies. *United Nations Office on Drugs and Crime (UNODC)*. URL: [https://www.unodc.org/nigeria/en/incitement-to-terrorism-through-the-media\\_-unodc-organizes-workshop-on-anti-terror-law-for-journalists--security-agencies.html](https://www.unodc.org/nigeria/en/incitement-to-terrorism-through-the-media_-unodc-organizes-workshop-on-anti-terror-law-for-journalists--security-agencies.html) (Last accessed: 10.10.2022)

179. ONLINE JIHADIST PROPAGANDA - 2020 IN REVIEW. *European Union Agency for Law Enforcement Cooperation (Europol)*. 2021. URL: [https://www.europol.europa.eu/cms/sites/default/files/documents/online\\_jihadist\\_propaganda\\_2020\\_in\\_review\\_0.pdf](https://www.europol.europa.eu/cms/sites/default/files/documents/online_jihadist_propaganda_2020_in_review_0.pdf) (Last accessed: 07.11.2022)

180. Online Jihadist Propaganda 2021 in review. Publications Office of the European Union, Luxembourg. *European Union Agency for Law Enforcement Cooperation (Europol)*. 2022. URL:

[https://www.europol.europa.eu/cms/sites/default/files/documents/Online\\_Jihadist\\_Pr opaganda\\_2021\\_in\\_review.pdf](https://www.europol.europa.eu/cms/sites/default/files/documents/Online_Jihadist_Pr opaganda_2021_in_review.pdf) (Last accessed: 17.10.2022)

181. OSCE furthers international discussion on terrorist use of Internet and related challenges on designation of illicit content online and gaps in regulatory frameworks. *Organization for Security and Cooperation in Europe (OSCE)*. 12.03.2021. URL: <https://www.osce.org/secretariat/481120> (Last accessed: 21.10.2022)

182. OSCE supports regional efforts to tackle the digital dimensions of violent extremism in Central Asia. *Organization for Security and Cooperation in Europe (OSCE)*. 12.12.2019. URL: <https://www.osce.org/secretariat/441991> (Last accessed: 18.20.2022)

183. Stop the virus of disinformation the risk of malicious use of social media during COVID-19 and the technology options to fight it. *United Nations Interregional Crime and Justice Research Institute (UNICRI)*. November 2020. URL: <https://unicri.it/sites/default/files/2020-11/SM%20misuse.pdf> (Last accessed: 10.10.2022)

## SUMMARY

At the beginning of the 21st century, international terrorism acquired the features of a global threat to international security. The active development of information communication technologies and digitalization processes covered all spheres of social life and directly affected the activities of maintenance: the development of digital technologies radically changed the information tools of terrorists, who quickly adapted to technological innovations. Thus, social media (social networks, messengers, online platforms, etc.) came to replace traditional mass media (press, television, radio), which were previously used by terrorists mainly as a source of informing the community about terrorist acts and their consequences. The latter has become a real weapon in the hands of extremist and terrorist organizations, which have understood all the advantages of the online environment to achieve their own goals (the efficiency of conveying information to the world community, focusing global attention, online communication with supporters, low costs of using social media, publicizing significant array information, user anonymity, etc.). The issue of combating media terrorism — a special type of information terrorism, which consists in the systematic and purposeful use of social media for the purpose of destabilizing the situation, psychological influence on mass consciousness (spreading feelings of anxiety, worry, fear and panic among the population, ensuring manipulative influence) — was on the agenda.

Social media perform informative, propaganda, and tactical functions for terrorist organizations:

- the spread of propagandistic sentiments and ensuring manipulative influence;
- the spread of panic and fear among the world community;
- ensuring a permanent presence in the online space, self-promotion;
- support of military operations;
- data collection;
- recruitment and training of supporters, exchange of experience;
- expansion of the financial support base of terrorist organizations.

Social media influence the acceleration of the evolutionary processes and practices of terrorists. In turn, the extremist content of terrorist organizations disseminated in the media affects the kindling of interest among a certain circle of participants in violent ideologies, forms a base of supporters, and provides psychological and manipulative pressure on the population. Such mechanisms and directions of interaction between terrorist organizations and the media can be clearly traced on the example of the activities in the media space of the most powerful terrorist organizations – IS and Al-Qaeda, which managed to effectively use modern information communication technologies, create their own media structures, adapt to the media environment, and ensure a constant presence in the online space. The function of terrorist organizations in the information space proved the relevance and importance of the influence of social media for ensuring a competitive propaganda war. At the same time, the directions, and tools, features of the use of social media by IS and Al-Qaeda are actively influenced by their ideological guidelines, goals, and objectives. The analysis of the activities of these terrorist organizations in the media space provides an opportunity to establish distinctive and common features (taking into account the clear difference between the ideology of terrorist organizations, their target audience, channels for the distribution of media content, its actual content, etc.), which must be taken into account when developing a strategy and mechanisms for combating media terrorism.

A significant contribution to the development of mechanisms for combating media terrorism was made by the international organizations of the UN, the EU, and the OSCE, which formed legal and technical mechanisms to prevent the spread of extremist and terrorist content in social media, to prevent the involvement of representatives of the younger generation through the Internet to participate in extremist and terrorist organizations, etc.

These issues are on the agenda in most countries of the world, where legislative initiatives have already been initiated, and various programs and projects have been developed and implemented. It is important to use and further improve already existing experiences, tools, and mechanisms of combating media terrorism.