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

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____ Н. Ф. Ржевська
«____»_____ 20__ р.

**ДИПЛОМНА РОБОТА**
ВИПУСКОВОЇ КАФЕДРИ ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА
ЗА СПЕЦІАЛЬНІСТЮ 291 «МІЖНАРОДНІ ВІДНОСИНИ, СУСПІЛЬНІ КОМУНІКАЦІЇ ТА РЕГІОНАЛЬНІ СТУДІЇ»
ЗА ОСВІТНЬО-ПРОФЕСІЙНОЮ ПРОГРАМОЮ
«МІЖНАРОДНА ІНФОРМАЦІЯ»

**Тема: «ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ ЯК ЗАГРОЗА НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ»**

Виконавець: студент 4 курсу, 409 групи, Політаєв Андрій Євгенійович

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

Нормоконтролер _____ _____
(Підпис) (ПІБ)

**ЗМІСТ**

## Перелік умовних позначень

ВВС - БРИТАНСЬКА КОМПАНІЯ СУСПІЛЬНОГО ТЕЛЕРАДІОМОВЛЕННЯ;

ЗМІ - ЗАСОБИ МАСОВОЇ ІНФОРМАЦІЇ;

ООН - ОРГАНІЗАЦІЯ ОБ'ЄДНАНИХ НАЦІЙ;

ОАД - ОРГАНІЗАЦІЯ АМЕРИКАНСЬКИХ ДЕРЖАВ;

ОІС - ОРГАНІЗАЦІЯ ІСЛАМСЬКОГО СПІВРОБІТНИЦТВА;

СААРК - АСОЦІАЦІЯ РЕГІОНАЛЬНОГО СПІВРОБІТНИЦТВА ПІВДЕННОЇ АЗІЇ;

ОБСЄ - ОРГАНІЗАЦІЯ З БЕЗПЕКИ І СПІВРОБІТНИЦТВА В ЄВРОПІ;

РНБО - РАДА НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ;

ШОС - ШАНХАЙСЬКА ОРГАНІЗАЦІЯ СПІВРОБІТНИЦТВА;

СЗР - СЛУЖБА ЗОВНІШНЬОЇ РОЗВІДКИ;

СБУ - СЛУЖБА БЕЗПЕКИ УКРАЇНИ;

ЄС - ЄВРОПЕЙСЬКИЙ СОЮЗ;

КТК - КОНТРТЕРОРИСТИЧНИЙ КОМІТЕТ;

ЗСУ - З ЗБРОЙНІ СИЛИ УКРАЇНИ.

# ВСТУП

Сьогодні проблема інформаційного тероризму починає привертати все більше уваги в сучасній політичній науці. Це пов'язано, в першу чергу, з технічним прогресом, який постійно прискорюється наростаючою інформатизацією суспільства і переходом світової цивілізації в інформаційну епоху. Сучасне суспільство немислимо без комунікацій, все життя середнього європейця, американця, та й вже багатьох українців щільно «зав'язана» на інформації. Порушення роботи інформаційних систем неминуче тягне за собою втрату почуття реальності, хаос, як суспільний, так і економічний занепад.

**Актуальність** вибору теми обґрунтовується тим, що найближче майбутнє характеризується неухильно зростаючою роллю інформаційної компоненти. Як індустрія, що забезпечує існування цивілізації, так і вся система громадської безпеки будуть перебувати в прямій залежності від інформаційних систем. Передбачити негативні наслідки терористичної атаки на інфосферу представляється практично неможливим, а наслідки таких атак можуть бути катастрофічними. Саме через слабкість своїх позицій у порівнянні з міццю сучасної держави терористи готові використовувати найжорстокіші методи боротьби та можливості для здійснення масових вбивств, заподіяння величезної економічної шкоди. Вони дуже швидко ставлять на озброєння своєї терористичної діяльності новітні досягнення сучасної науки і військової думки. Тероризм сам по собі не в змозі досягти багато чого, але він може запустити механізми складних і руйнівних соціальних явищ. Інформаційні канали це свого роду ключові артерії сучасного суспільства. Тому й не дивно, що саме вони можуть стати мішенню №1 для міжнародних терористів.

Питання про стратегічні цілі розвитку держави набуває, як раніше говорили, доленосного характеру. По суті мова йде про вироблення принципово нової парадигми життєдіяльності. Мабуть, і до України можна віднести роздуми Папи іонна Павла II про те, що зараз у світі торжествує «культура смерті», то треба забезпечити торжество «культури життя». Останнє неможливо без встановлення нового світопорядку, який повинен бути більш гуманним, справедливим і безпечним. Процес глобалізації призвів до того, що тероризм став значно небезпечнішим, ніж раніше. Так вважає Пол Піллар, один з провідних фахівців Central Intellegence Agency в області тероризму. Він вважає, що процес глобалізації призвів до зміни стратегії тероризму.

Все більш масштабним соціально-політичним явищем, що представляє серйозну загрозу безпеці і життєво важливим інтересам як особистості, так і суспільства і держави, стає тероризм.

Терористична діяльність як складне, багатоаспектне і вкрай негативне соціально-політичне явище давно переросла рамки національних кордонів і перетворилася на масштабну загрозу для безпеки всього людства.

**Мета дослідження** полягає у розкритті інформаційного тероризму як загрози національній безпеці України.

Відповідно до поставленої мети **завданнями** роботи будуть:

- розкрити основні підходи до визначення поняття «інформаційний тероризм»;

- проаналізувати сутність та зміст поняття національної безпеки;

- з’ясувати причини і джерела ескалації інформаційного тероризму;

- розкрити види, суб’єкти інформаційного тероризму;

- дослідити протидію інформаційному тероризму в рамках міжнародних організацій та форумів;

- визначити періодизацію та види терористичних атак на інформаційний простір України;

- розкрити нормативно-правову базу протидії інформаційному тероризму в Україні;

- висвітлити співробітництво України з міжнародними організаціями у сфері протидії інформаційному тероризму;

**Об'єктом** дослідження є національна безпека України.

**Предметом** дослідження є інформаційний тероризм, форми його прояву та наслідки для національної безпеки України.

При дослідженні даного питання були використані такі **методи** як порівняльно-правовий, метод аналізу, формально-логічний і ряд інших методів.

**Загальнотеоретичною базою** дослідження послужили праці: В.Н. Цигичко, Г. Л. Смолян, Д. С. Черешкін, С. А. Охріменко, Г. А. Черней, А. Б. Антопольський, А. А. Кононов та інші.

**Структура** роботи складається зі вступу, трьох розділів, висновку та списку літератури.

# РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ФЕНОМЕНУ ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ У КОНТЕКСТІ ЗАГРОЗ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ

## 1.1. Основні підходи до визначення поняття «інформаційний тероризм»

Тероризм, як будь-яке негативне соціальне явище відчуває постійні зміни. У зв'язку з виниклими на сучасному етапі потенційними можливостями використання при скоєнні злочинів новітніх інформаційних технологій, телекомунікаційних систем і засобів, кіберпростору, з'явився новий найбільш небезпечний вид тероризму, якого одні називають кібертероризмом або електронним тероризмом, інші – інформаційним тероризмом.

Як відомо, в даний час серйозна підготовка до скоєння злочинів терористичної спрямованості, як правило, вимагає активного використання інформаційних ресурсів, в тому числі і з метою забезпечення широкої середовищної підтримки злочинних акцій. Для цього, наприклад, ще в кінці минулого і початку нинішнього століття міжнародними терористами, що діяли в Чеченській Республіці, було сформовано спеціальний підрозділ. Створене сепаратистським ідеологом М. Удуговим так зване «інформаційне агентство «Кавказ-центр»», відкрило однойменний сайт в мережі Інтернет. Це агентство займалося поширенням дезінформації про успіхи терористів і великі втрати федеральних сил з метою сформувати у світової громадськості і керівництва іноземних держав негативне ставлення. У цій злочинній акції використовувалися понад 100 фінансованих терористами сайтів російською, англійською, арабською, французькою та іншими мовами.

Лідерами терористів були створені інформаційні центри в Азербайджані, Грузії, Україні, Литві, Фінляндії, Туреччині та Польщі. Кібертероризм являє собою серйозну загрозу для людства, порівняну з ядерною, бактеріологічною і хімічною зброєю; причому ступінь цієї загрози в силу своєї новизни не до кінця ще усвідомлена і вивчена. Досвід світової спільноти в цій галузі з усією очевидністю свідчить про безсумнівну уразливість будь-якої держави, тим більше що кібертероризм не має державних кордонів, кібертерорист здатний в рівній мірі загрожувати інформаційним системам, розташованим практично в будь-якій точці земної кулі [2, с.146].

Цей термін вперше був запропонований ще в 80-х минулого століття старшим науковим співробітником Інституту безпеки і розвідки (англ. Institute for Security and Intelligence) Баррі Колліном, який використовував його в контексті тенденції до переходу тероризму з фізичного у віртуальний світ, зростаючого перетину і зрощення цих світів. Він визначив його як використання комп'ютерних і телекомунікаційних технологій в терористичних цілях. У Вікіпедії комп'ютерний тероризм (кібертероризм) також визначається як використання комп'ютерних і телекомунікаційних технологій (насамперед, Інтернету) в терористичних цілях [5].

В даний час в науковій літературі не існує загальновизнаного визначення поняття «інформаційний тероризм» («кібертероризм»).

Одні автори під кібертероризмом розуміють сукупність протиправних дій, пов'язаних із замахом на життя людей, деструктивними діями щодо матеріальних об'єктів, спотворенням об'єктивної інформації або рядом інших дій з використанням інформаційних засобів, що сприяють нагнітанню страху і напруженості в суспільстві з метою отримання переваги при вирішенні політичних, економічних або

соціальних завдань. Інші оцінюють його як навмисну атаку на інформацію, оброблювану комп'ютером, комп'ютерну систему або мережу, що створює небезпеку для життя і здоров'я людей, якщо такі дії були здійснені з метою порушення громадської безпеки, залякування населення або провокації військового конфлікту.

З юридичної точки зору, слід також розмежовувати поняття інформаційного тероризму та використання інформації в терористичних цілях. У засобах масової інформації часто допускають підміну даних понять, розглядаючи пропагандистську діяльність в терористичних цілях як інформаційний тероризм.

Крім того, не всі вчені розглядають поняття «інформаційний тероризм», «кібертероризм (комп'ютерний тероризм)» як синоніми, надаючи їм різний сенс.

Інформаційний тероризм вони визначають як використання інформаційних засобів в терористичних цілях, а також дезорганізація автоматизованих інформаційних систем, що створює небезпеку загибелі людей, заподіяння майнової шкоди або настання інших суспільно небезпечних наслідків, якщо вони здійснені з метою порушення громадської безпеки, залякування населення або надання впливу на прийняття рішень органами влади, а також загроза вчинення зазначених дій в тих же цілях.

Основною ознакою кібертероризму (комп'ютерного тероризму) вони бачать атаки на комп'ютерні сети, апаратно-програмні комплекси державних, оборонних установ, важливих, особливо важливих та інших об'єктів з метою дезорганізації їх роботи і саботажу, або загрози заподіяння фізичної шкоди за допомогою комп'ютерних засобів вчиненням подібних атак при невиконанні пред'явлених терористами певних вимог (наприклад, виведення інформаційно-телекомунікаційної

мережі організації з ладу, знищення персональних даних клієнтів банків, виведенням з ладу «оцифрованих» заводів і енергетичних об'єктів в терористичних цілях або отримання викупу з метою фінансування тероризму).

Крім того є і таких вчені, які вважають, що це поняття придумали і роздувають в медіапросторі власники об'єктів виробництва засобів інформаційної безпеки в рекламних цілях.

На нашу думку, такий підхід до даної проблеми в корені не відповідає сучасним реаліям використання інформаційно-телекомунікаційних засобів в практиці не тільки терористичних організацій, а й терористів-одинаків і виходить від цього явища надмірної небезпеки.

Одні вчені і практики схильні вважати його самостійною формою тероризму, такий же, як і політичний, ідеологічний, релігійний, національний, етнічний і т.д., інші розглядають його як спосіб здійснення зазначених форм тероризму. Дослідження показує, що і ті, і інші доводи мають під собою теоретичні та практичні підстави, так як в практиці такий вид тероризму в чистому вигляді зустрічається рідко.

У кримінальному законі інформація є предметом злочинів, представлених у Кримінальному кодексі України (злочинів у сфері комп'ютерної інформації), було криміналізовано нове діяння – шахрайство у сфері комп'ютерної інформації. Це свідчить про підвищення уваги законодавця до інформаційної сфери, у зв'язку була створена нова норма для її захисту. Однак загроза, яку несуть з собою хакерські групи, набагато серйозніше. Вона не може бути порівнянна з тими зусиллями, які робить законодавець. Якщо раніше хакери і хакерські групи були зацікавлені лише в демонстрації своїх умінь, то тепер їх більше цікавить матеріальна складова питання, яка не завжди пов'язана з правомірними діями. Як

відомо, в даний час терористичні угруповання (такі як Аль-Каїда) активно використовують навички хакерських груп для досягнення своїх злочинних цілей.

20 жовтня 1969 р. вперше два комп'ютери, один з яких знаходився в комп'ютерному центрі Каліфорнійського університету в Лос-Анджелесі (UCLA), а інший – в Стенфордському дослідницькому інституті в Південній Каліфорнії, почали «розмовляти» між собою. З плином часу комп'ютери стали найзручнішим засобом зберігання інформації, а інтернет найдешевшим засобом її передачі. І, звичайно ж, цей факт не залишився без уваги організованих злочинних груп, включаючи терористичні угруповання. Терористам комп'ютерна мережа необхідна для зберігання, обміну та отримання інформації. Якщо раніше діяльність терористів більшою мірою була зосереджена в реальному просторі, то в даний час ми можемо спостерігати зміну області дій.

Говорячи про комп'ютерну мережу, необхідно торкнутися теми хакерських груп. Джеффрі Карр виділяє 2 види таких груп: державні та недержавні хакери. Велику небезпеку становлять, звичайно ж, недержавні хакери. По-перше тому, що суспільно небезпечні діяння (особливо злочинні) вони можуть вчиняти як щодо іноземної держави, так і щодо тієї держави, громадянином якої вони є. По-друге, такі хакерські групи можуть бути залучені в діяльність терористичних угруповань. У цьому випадку жоден урядовий веб-сайт, жодна комп'ютерна система не можуть бути гарантовано захищені від кібератак. Підтверджуючим прикладом може служити використання терористами секретної інформації, отриманої з підрозділів ООН, внаслідок чого був убитий Іранський фізик-ядерник.

Однак зупиняти свою увагу виключно на кібертероризмі було б неправильно. Засоби масової інформації та масова інформація взагалі є потенціалом для використання їх терористами. Існують різні точки зору на

тему, хто кого використовує і чи використовує взагалі. Наприклад, В. Лакер зазначає, що терористичні групи залежні від публічності, тобто терористи не прямо, а побічно використовують ЗМІ, при цьому ЗМІ не вважають себе використаними, оскільки виконують свій обов'язок перед суспільством, анонсуючи події. Також приблизно вважає Б. Хоффмат, пояснюючи, чому США за останні 30 років частіше, ніж інші країни, ставали жертвою терористичних актів. «Гласність плюс можливості американських ЗМІ, - пише Б.Хоффман, — представляють терористам привабливі і відносно легкодоступні шанси для самопредставлення на цілий світ».

Малоймовірно, що таке використання ЗМІ характерне лише для США. Інтернет рясніє заголовками про те, що ЗМІ всіляко покриває терористів. Анонсуючи події, канал ВВС дуже рідко використовує у своїх репортажах слова «терорист», «терористичний акт», пояснюючи це тим, що в Статуті для продюсерів ВВС записано: «...неупередженість лежить в основі всієї діяльності ВВС. Всі програми і служби ВВС повинні бути відкритими для думок, справедливими і демонструють повагу до істини». Ось чому журналісти корпорації в своїх репортажах намагаються обходитися без слова «терорист». У зв'язку з проголошеним в США правом кожного на вільне поширення та отримання інформації діяльність ЗМІ визначає лише інститут саморегуляції, для прикладу, представлений вище Статут для продюсерів ВВС.

Існують і інші версії про взаємодію ЗМІ та терористичних угруповань. Таким чином, ми можемо говорити про навмисне використання ЗМІ не стільки для виправдання і популяризації своєї діяльності, скільки для анонсування саме тієї інформації, яка вигідна терористам для досягнення своїх цілей.

Однак під ЗМІ розуміється періодичне друковане видання, мережеве видання, телеканал, радіоканал, телепрограма, радіопрограма, відеопрограма, кінохронікальна програма, інша форма періодичного поширення масової інформації під постійним найменуванням (назвою). Малоймовірно, що листівки можна визнати періодичним друкованим виданням, хоча вони також потрапили в сферу використання терористами.

З цього можна зробити висновок про те, що поставити знак рівності між інформаційним тероризмом і негативною діяльністю ЗМІ ми не можемо. Таким чином, інформаційний тероризм слід розуміти як використання мережі інтернет або іншої інформаційної мережі, а також ЗМІ або іншої інформації як відомостей незалежно від форми їх подання з метою негативного впливу на органи влади та (або) населення або досягнення інших терористичних цілей (включаючи фінансування, обмін даними та ін).

При цьому основними ознаками інформаційного тероризму є: використання ЗМІ (іншої інформації як відомостей незалежно від їх подання), а також мережі інтернет або локальної інформаційної мережі; спеціальна мета – негативний вплив на органи влади і (або) населення, а також інші терористичні цілі, що включають фінансування, обмін даними та ін.

Враховуючи те, що за даними «Глобального індексу тероризму за 2020 рік» і супроводжуючого його рейтингу країн світу за рівнем тероризму, представленого Інститутом економіки і миру спільно з Інститутом Меріленда, Україна займає 10-е місце з 158 країн, це повинно спонукати законодавця зробити крок вперед і вжити інші кримінально-правові заходи з метою підвищення ефективності боротьби, включаючи профілактику і попередження тероризму взагалі.

## 1.2. Національна безпека: сутність та зміст

Розкриття поняття «національна безпека» являє собою відомі складності в силу його багатозначності.

«Національна безпека, підкреслює, зокрема, голова Комітету Палати Представників Конгресу США Д. Мосс, - це таке важковизначне поняття, що ніхто не може дати його дефініцію... будучи протягом 16 років головою підкомітету, я не міг знайти когось, хто міг дати мені визначення». Поняття «безпека» в українській мові безпосередньо пов'язане з поняттям «небезпека». Так, В.І. Даль визначає безпеку як «відсутність небезпеки, збереження, надійність». С.І. Ожегов трактує безпеку як «стан, при якому не загрожує небезпека, є захист від небезпеки».

Не буде перебільшенням твердження, що всі люди, держава і суспільство в цілому вважають забезпечення безпеки найважливішою своєю потребою. Потреба в безпеці розглядається як один з першорядних мотивів діяльності людей і спільнот. У науковій літературі сьогодні утвердилося таке розуміння проблем небезпек і безпеки, при якому все коло проблем, пов'язаних з цими процесами, концентрується в понятті «національна безпека».

Вперше термін «національна безпека» вжив у своєму посланні до Конгресу США в 1904 р. президент США Т. Рузвельт. У посланні йшлося про приєднання до США зони Панамського каналу, причому ця акція обґрунтовувалася інтересами «національної безпеки» США.

Наприкінці Другої світової війни саме уряд США підтримав теоретичні дискусії з питань національної безпеки та прийняття відповідних нормативних правових актів. Основи забезпечення національної безпеки США закладені в законі від 26 липня 1947 р. «Про

національну безпеку». В. Манілов вважає, що цей закон визначив систему національної безпеки як інтеграцію питань внутрішньої, зовнішньої і військової політики в інтересах виваженого підходу до проблем використання різних військових і невійськових засобів.

У нашій країні термін «національна безпека» вперше використаний в Законі України «Про інформацію». У даному документі сказано: «національна безпека розуміється як стан захищеності національних інтересів від внутрішніх і зовнішніх загроз, що забезпечує прогресивний розвиток особистості, суспільства і держави». Це визначення збігається з визначенням «безпека» в Законі «Про безпеку», так як сукупність життєво важливих інтересів особистості, суспільства, держави і становить національні інтереси.

Ключовим у понятійному комплексі «національна безпека» є поняття «нація». Формулювань останнього існує не менше, ніж формулювань самого поняття «безпека». Наприклад, воно може розглядатися в наступних значеннях: як сукупність громадян держави, як сукупність представників одного етносу. Р. Г. Абдулатіпов стверджує, що «у нас не склалися інші традиції: націями ми називали етнічні утворення. У нас стоїть проблема вибору: нація як етнос або нація як держава».

Якщо раніше найбільш поширеним було визначення нації як історично стійкої спільності людей, що виникає на базі спільності мови, території, економічного життя і психічного складу, що виявляється в спільності культури, то зараз все більшого визнання набуває визначення нації як єдності громадянського суспільства і держави. Суспільство як складова частина нації власне і підкреслює поліетнічність всякої нації. Стрижнем нації є держава. К. Дейч коротко і однозначно визначає націю як народ, що володіє державою. Змістовно поняття нації близьке до поняття країни.

Щоб піти від неоднозначного розуміння категорії «національна безпека» деякі дослідники пропонують використовувати поняття державна безпека. Ця розбіжність інтересів не визнавалася в Концепції державної безпеки Радянського Союзу, яка декларувала повний їх збіг. Однобокість і наступна з неї деструктивність Концепції державної безпеки призвели до необхідності звернутися до Концепції національної безпеки. Суб'єктами і об'єктами концепції національної безпеки є: особистість з її правами і свободою, суспільство з його матеріальними і духовними цінностями, держава з його конституційним ладом, суверенітетом і територіальною цілісністю.

Принциповою відмінністю концепції національної безпеки від державної безпеки є докорінна зміна системи пріоритетів: головне – особистість, потім суспільство, і тільки потім – держава. Таким чином, поняття «національна безпека», передбачає під нею такий стан суспільства (держави), при якому воно, будучи складною соціальною системою, зберігає свою цілісність, стійкість і здатність до ефективного функціонування і розвитку, а також можливість надійного захисту своїх інтересів від будь-яких внутрішніх і зовнішніх впливів, як антропогенного, так і техногенного характеру.

Під загрозами національній безпеці розуміються явища і дії, що ускладнюють або роблять неможливою реалізацію життєво важливих інтересів особистості, суспільства і держави. Загрози національної безпеки вельми різноманітні і можуть класифікуватися залежно від тих чи інших підстав.

Найбільш важливою підставою класифікації, на нашу думку, є джерело нанесення шкоди, природні явища і техногенні фактори і антропогенні (людина і різні системи). У свою чергу, антропогенні джерела можна розділити в залежності від їх місцезнаходження на

зовнішні і внутрішні. Загрози політичного, економічного, техногенного, соціального, терористичного та інформаційного характеру можуть бути як зовнішніми, так і внутрішніми. Поряд з цим існують загрози, що мають тільки зовнішнє або внутрішнє джерело. Наприклад, військова має яскраво виражений зовнішній характер.

Забезпечення національної безпеки України - цілеспрямована діяльність державних і недержавних (громадських) інститутів, громадян щодо виявлення та попередження загроз безпеці особистості, суспільства і держави, а також захисту національних інтересів України.

Система забезпечення національної безпеки по-різному представляється в законодавстві. Як зазначає у своїй роботі і. б. Кардашова «процес формування системи забезпечення національної безпеки України ускладнений відсутністю чіткої концепції її розвитку з визначенням цілей, національних інтересів, методів і засобів досягнення».

Система забезпечення національної безпеки є механізм, що дозволяє перетворити прийняту державою стратегію в галузі національної безпеки в скоординовану діяльність конкретних відомств, громадських об'єднань і громадян на основі чинного законодавства. Так, Бабаєв В. К. пропонує під механізмом забезпечення національної безпеки розуміти «єдність організаційно оформлених державою спеціальних органів, які відповідно до інтересів людини, суспільства і держави вирішують завдання забезпечення безпеки країни і в цих цілях здійснюють в строго визначених формах державне керівництво і практично реалізують у своїй діяльності функції забезпечення національної безпеки».

Керує системою забезпечення національної безпеки України Президент України - Верховний головнокомандувач. Особливістю системи забезпечення національної безпеки в Україні є безпосереднє підпорядкування Президенту ряду державних органів виконавчої влади.

Він є головою Ради безпеки, який здійснює підготовку рішень глави держави з питань захищеності життєво важливих інтересів особистості, суспільства і держави від внутрішніх і зовнішніх загроз, проведення єдиної державної політики в галузі забезпечення національної безпеки України, у забезпеченні національної безпеки України беруть участь всі гілки державної влади. Законодавча визначає компетенцію органів забезпечення національної безпеки в державній системі, законодавчо формулює правові засади забезпечення національної безпеки, визначає правовий статус учасників суспільних відносин; передбачає юридичну відповідальність за неправомірну поведінку осіб, які є суб'єктами права.

Судова влада є гарантом захисту конституційних прав і свобод громадян; визнає і відновлює суб'єктивне право; визначає заходи державного впливу на правопорушення. І, нарешті, виконавча влада здійснює безпосереднє Державне управління у сфері національної безпеки.

У структуру системи забезпечення національної безпеки входять також сили і засоби, що здійснюють комплекс заходів спрямованих на захист життєво важливих інтересів особистості, суспільства і держави. Сили забезпечення безпеки включають в себе: Збройні Сили, органи безпеки, органи внутрішніх справ, зовнішньої розвідки, забезпечення безпеки органів законодавчої, виконавчої, судової влади та їх вищих посадових осіб, податкової служби; внутрішні війська та інші державні органи забезпечення безпеки, що діють на підставі законодавства. До засобів забезпечення національної безпеки належать матеріальні, технічні, майнові та ресурсні об'єкти, що безпосередньо використовуються для забезпечення національної безпеки.

Таким чином, під системою забезпечення національної безпеки слід розуміти сукупність взаємодіючих суб'єктів, сил, органів і засобів національної безпеки, що забезпечують на основі чинного законодавства

та в рамках єдиної державної політики України сталий розвиток, реалізацію та захист національних інтересів. Законодавець виділяє основні функції системи безпеки: виявлення і прогнозування внутрішніх і зовнішніх загроз життєво важливим інтересам об'єктів безпеки, здійснення комплексу оперативних і довготривалих заходів щодо їх попередження і нейтралізації; створення і підтримання в готовності сил і засобів забезпечення безпеки; управління силами і засобами забезпечення безпеки в повсякденних умовах і при надзвичайних ситуаціях; участь у заходах щодо забезпечення безпеки за межами України відповідно до міжнародних договорів та угод, укладених або визнаних Україною. На основі проведеного аналізу, можна зробити наступні висновки:

1. Національна безпека - стан захищеності національних інтересів від внутрішніх і зовнішніх загроз, що забезпечує прогресивний розвиток особистості, суспільства і держави.

2. Система забезпечення національної безпеки є складним комплексним механізмом, що вимагає пізнання місця і ролі кожного з елементів цієї системи для досягнення рівня національної безпеки сприяє прогресивному розвитку України.

# РОЗДІЛ 2. ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ ЯК ОДНА З ФОРМ СУЧАСНОГО ТЕРОРИЗМУ

## 2.1. Причини і джерела ескалації інформаційного тероризму

Сьогодні багато фахівців-террологів говорять про зростаючу ескалацію тероризму, розуміючи під цим терміном розвиток тероризму, який прогресує в часі і по території; перехід до більш гострих форм протистояння сучасному суспільству, при яких наступні руйнівні впливи тероризму інтенсивніше, ніж попередні.

Найбільш значущим фактором ескалації тероризму є його постійне фінансування по різних каналах. Для протидії фінансуванню тероризму сьогодні зроблено досить багато: розроблена і постійно вдосконалюється правова база, налагоджуються міжнародні канали взаємодії, здійснюється контроль за сумнівними активами. В даному напрямку дуже корисним і в певному сенсі інноваційним нам представляється американський досвід зі створення Служби внутрішніх доходів.

Наприклад, ефективним елементом інфраструктури контролю за фінансовими потоками є Закон США «про боротьбу з відмиванням грошей», що передбачає ряд додаткових заходів щодо посилення фінансового контролю з боку держави.

Відповідно до цього нормативного акту фінансова операція, а також операції з перевезення, переказу, відправлення платіжних документів розглядаються як «відмивання» грошей, якщо особа, яка здійснює ці операції:

- незаконно перевозить кредитно-грошовий інструмент з однієї держави в іншу або навмисно сприяє такій незаконній діяльності;

- знає, що такий документ забезпечує отримання незаконних доходів;

- знає, що операція необхідна для приховування справжнього характеру, місцезнаходження, джерела доходів, володіння або розпорядження ними;

- знає, що операція здійснюється для ухилення від виконання вимог закону в частині подання звіту про операцію.

Закон зобов'язує банки повідомляти в право-охоронні органи про всі підозрілі операції на суму понад 5 тисяч доларів (а за операціями з цінними паперами на суму понад 3 тисячі доларів). Ознаки «підозрілості» угоди і процедура дій банківського службовця в розглянутих випадках детально описуються відповідною інструкцією Міністерства фінансів. Обов'язковою вимогою є наявність у кожної банківської установи спеціальної програми по боротьбі з відмиванням грошей. Особливому контролю підлягають повторювані операції, пов'язані з продажем банківських чеків, поштових переказів або дорожніх чеків, на суму понад 3 тисячі доларів кожна, а також операції з переведення в готівку повторюваних чеків.

Прийняття аналогічного закону в Україні дозволить вирішити і ще одну проблему - отримання корупційних доходів з подальшим виведенням коштів в офшори.

Крім фінансової підтримки, псевдоісламські організації масовими тиражами видавали і поширювали літературу екстремістського спрямування, довершуючи ідеологічну обробку через власні освітні структури. Відсутність священнослужителів, які мають ісламську освіту, змушувала місцеві релігійні громади відправляти молодь на навчання в зарубіжні ісламські університети, де вони знайомилися з канонами «чистого», або «істинного» ісламу. Дозвіл хаджу до святих місць,

розташованих в Саудівській Аравії, і знайомство з іншими підходами до здійснення ісламських обрядів сприяють наростанню протиріч з ісламом.

Якщо говорити про національні, українські фактори ескалації тероризму, то слід згадати про тенденцію поширення терористичних організацій в республіках Середньої Азії. Дана детермінанта має кумулятивний ефект через тісні економічні та міграційні зв'язки України з державами даного регіону. Разом з потоком мігрантів на територію України потрапляють емісари терористичних організацій, які вміло використовують багатонаціональність і багатоконфесійність України для розпалювання расової та релігійної ворожнечі.

Наступною детермінантою, яку ніяк не можна скидати з рахунків, є участь деяких громадян України у збройних формуваннях на боці забороненої в Україні Ісламської держави. Подібні елементи, повертаючись додому, організовують «сплячі терористичні осередки», несучи ідеологію політичного екстремізму і насильства.

Вагомим фактором ескалації тероризму в регіоні є територіальна близькість до осередків збройних конфліктів в країнах ближнього і далекого зарубіжжя, насамперед на Близькому Сході. Перераховані вище обставини свідчать, що тероризм сьогодні реалізується в якості позасистемного геополітичного гравця як один з осередків міжнародного тероризму.

Послабити негативний вплив міграційного чинника сьогодні представляється можливим, використовуючи сучасні інформаційні технології, а саме: створення інтегрованого банку даних, що включає біометричні параметри мігрантів, їх участь в релігійних об'єднаннях, політичних партіях і т. д.

Досліджуючи проблему ескалації тероризму, слід підкреслити, що серйозну заклопотаність, поряд з глобалізацією і диверсифікацією,

викликає його професіоналізація. Терорист сьогодні - не екзальтований юнак з «пекельною машиною», а холоднокровний професіонал, який підготовлений і володіє навичками диверсійної діяльності. І шляхи, по яких такі професіонали приходять в терористичні організації, теж різні: це можуть бути і релігійні фанатики, і ветерани локальних конфліктів, і військовослужбовці, з різних причин (економічних, соціальних, політичних) залишилися не при справах, особливу групу джерел складають професійні терористи, підготовлені спецслужбами для ведення підривної і диверсійної діяльності.

Яскравим прикладом представників останньої групи був Усама бен Ладен, підготовлений і профінансований для протидії угрупованню радянських військ в Республіці Афганістан, який створив Аль-Каїду (організація терористичного спрямування – заборонена в Україні), спадкоємцем якої стала Ісламська держава. Вже сьогодні аналітики низки європейських держав говорять про високий професійний рівень терактів останніх років у Парижі, Каннах, Брюсселі, Лондоні, Каліфорнії.

В якості істотного фактора зростання терористичної загрози глобального масштабу виступає пропаганда в соцмережах, що вербує «наречених джихаду» з числа мешканок інших країн, яка ведеться професійними психологами, що враховують всі нюанси особистості майбутньої «нареченої».

На загальноприйнятій практиці тероризм - це ідеологія насильства і практика впливу на прийняття рішення органами державної влади, органами місцевого самоврядування або міжнародними організаціями, пов'язані з залякуванням населення і (або) іншими формами протиправних насильницьких дій.

Разом з тим тероризм дуже часто використовується спецслужбами різних держав як акція прикриття різних операцій, в яких не можуть бути

задіяні збройні сили даної держави, або терористи фінансуються ззовні з метою дестабілізації обстановки, ведення підривної і диверсійної діяльності, схиляння до прийняття вигідних політичних та економічних рішень. Таким чином, багато держав сьогодні розглядають тероризм як альтернативну форму війни.

На думку деяких вчених, тероризм кінця XX - початку XXI століття докорінно відрізняється від того, який мав місце досі, – і цілями, і методами, і засобами, і типом виконавців. Це диктує необхідність вироблення інших методів боротьби.

Сучасний терор сформувався значною мірою під впливом двох процесів – сучасної глобалізації та демографічного вибуху. В даний час великий вплив, крім наростання після 2018 року загальносвітової економічної кризи, надає і демографічний фактор. Населення планети збільшилося до 7 млрд осіб, насамперед за рахунок зростання населення в країнах Африки та Азії.

Даний фактор, поряд з економічним, багато в чому пояснює причини того, що відбувається на планеті найбільшого переселення народів (перше масштабне планетарне переселення було 40 тис.років тому).

У розвинених регіонах світу в наявності тенденція депопуляції, виродження, яка досягне максимуму до 2030 року. У багатьох європейських сімей або зовсім немає дітей, або одна дитина, в той час як в ряді країн Азії, Африки, Латинської Америки, в мусульманському світі наростає інша тенденція – до збільшення народжуваності. Там 7-8 дітей в сім'ї - це норма.

Перш за все це стосується Африки, де чисельність населення вже перевищує мільярд і прогнозується його подальший щорічний приріст в 4%, в результаті чого до 2050 року населення континенту подвоїться

(найбільше в Нігерії – до 290 млн осіб, Ефіопії – до 174 млн осіб, Конго – до 128 млн осіб, Єгипті – до 130 млн осіб).

У той час як чисельність населення в Китаї (1,4 млрд осіб) і Індії (1,6 млрд осіб), за прогнозами, буде збільшуватися повільніше, ніж сьогодні. Загальне зростання населення в країнах, що розвиваються тягне за собою нездатність держав забезпечити людей соціальними послугами, продовольством, роботою. При цьому слід враховувати, що групи людей у віці від 15 до 25 років складають там половину населення, і саме серед них наростає невдоволення своїм матеріальним становищем.

Більш того, знижується ймовірність поліпшення їх становища в майбутньому. Градус цього невдоволення зростає, оскільки всі мають можливість бачити рівень життя Заходу і порівнювати з власним становищем. Подібне порівняння, як правило, не на користь їхньої країни.

При цьому величезна армія безробітної молоді з країн третього світу постійно поповнюється резервом терористичних груп, якими легко маніпулюють агенти збройових монополій, які отримують надприбутки.

Роль каталізатора в зростанні невдоволення відіграють безцеремонні і жорсткі спроби Заходу нав'язати своє сприйняття світу, свої цінності, традиції, спосіб мислення і поведінки, а також спроби насильницького насадження державного ладу і устрою, моделі демократії західного зразка, неоліберальної моделі розвитку. У даній ситуації терор є відповідною реакцією, проявом невдоволення фактичною узурпацією влади некомпетентними правителями, корупцією, тяжким матеріальним становищем, відчаєм, правовим нігілізмом.

І все ж основною рушійною силою, як уже зазначалося вище, є явне неприйняття диктату ззовні, неприйнятних схем політичного та економічного устрою, чужої філософії, поведінкової моделі, способу мислення.

У той же час специфікою сучасного тероризму є те, що він поширюється за власною важко передбачуваною логікою і носить демонстративний характер, навмисно здійснюючись у вигляді страхітливих варварських акцій. При цьому існує реальна небезпека використання терористами «брудної» атомної бомби, біологічної та бактеріологічної зброї, впровадження в системи комунікацій та інфраструктуру.

Поряд з цим істотний деструктивний потенціал таять в собі спроби Заходу різними способами використовувати тероризм в своїх корисливих інтересах шляхом розпалювання конфліктів, зіштовхування між собою етнічних, національних і релігійних груп. Саме через подібні дії західних держав, і перш за все США, з'явилося таке утворення, як Ісламська держава.

Ніколи до цього терористи не володіли настільки значними фінансовими ресурсами і не брали під контроль настільки великі території.

Все частіше фахівці розглядають тероризм як особливу форму війни. Відомо, що військова доктрина України серед загроз військовій безпеці особливо виділяє наступні загрози терористичного профілю:

- міжнародний тероризм;

- протиправну діяльність екстремістських націоналістичних, релігійних, сепаратистських і терористичних рухів, організацій і структур, спрямовану на порушення єдності і територіальної цілісності України, дестабілізацію внутрішньополітичної обстановки в країні;

- створення, підготовку, постачання та діяльність незаконних формувань;

- незаконне поширення (обіг) на території України коштів, які можуть бути використані для здійснення терористичних актів та інших протиправних дій.

Аналіз цього документа дозволяє стверджувати, що з точки зору військово-політичної безпеки сучасна держава розглядає тероризм як загрозу військового характеру, так що ще однією детермінантою сучасної ескалації терроризму є можливість досягнення геополітичних цілей за допомогою терористичних організацій, в результаті чого уникається відкрита військова експансія. Саме тому різні спецслужби охоче фінансують сепаратистські та опозиційно-терористичні об'єднання по всій земній кулі.

В якості підсумкового висновку слід зазначити, що сучасна ескалація тероризму – складна, багатоаспектна проблема, що характеризується рядом факторів, кожен з яких при виході з поля зору органів державної влади, місцевого самоврядування та громадськості здатний підштовхнути ситуацію в бік зростання терористичної активності, збільшення числа терактів і зростання кількості їх жертв. Тому саме своєчасне виявлення детермінант ескалації тероризму є основою його ефективної профілактики та подальшої нейтралізації.

## 2.2. Види, суб’єкти інформаційного тероризму

Суб'єкти тероризму являють собою широку систему державних і недержавних структур, що знаходяться між собою в складних відносинах взаємодії і протиборства. Нерідкі випадки, коли терористичні організації управляються, субсидуються різними державами або політичними організаціями. Вважаємо, що всі суб'єкти тероризму можуть бути розділені на наступні види:

- держави, що підтримують окремі терористичні організації або використовують терористичні акції в своїх політичних інтересах;

- недержавні терористичні організації, що здійснюють суспільно небезпечні посягання в політичних цілях;

- злочинні організації, що використовують терор як один із засобів досягнення неполітичних цілей;

- терористи-одинаки.

До числа суб'єктів терористичної діяльності можуть бути віднесені також спецслужби деяких іноземних держав і їх підрозділи, призначені для здійснення терористичних акцій. Йдеться насамперед про держави з антидемократичними, авторитарними режимами або про країни, що перебувають у гострому протиборстві зі своїми зовнішньополітичними противниками, які ведуть боротьбу зі «своєю» політичною опозицією в середовищі емігрантів у зарубіжних країнах.

Другу групу суб'єктів утворюють недержавні організації, що безпосередньо реалізують терористичні акції в політичних цілях. Необхідно відзначити, що для них, як правило, характерні такі риси:

- наявність програми, яка проголошує в якості основного засобу досягнення своїх цілей терор;

- чітка організаційно-функціональна будова;

- сувора конспірація;

- здійснення заходів з планування та організації терористичних актів;

- створення центрів підготовки терористів;

- зв'язок із зарубіжними екстремістськими кримінальними структурами.

У період найвищої активності терористичні організації являють собою не розрізнені групи змовників, як це траплялося в минулому, а складні структури з внутрішнім поділом праці, майстернями, складами, друкарнями, лабораторіями, госпіталями, конспіративними квартирами та

ін. Вони активно впроваджують своїх агентів в різні ланки державного апарату, промислових і фінансових корпорацій.

До даної групи суб'єктів можна віднести наступні організації:

- Міжнародні та національні терористичні організації, в числі яких може бути виділений ряд підгруп:

1) Праві терористичні організації профашистської, расистської, іншої реакційної спрямованості «Сірі вовки» (Туреччина), «військово-спортивна група Гофмана» і деякі інші неонацистські організації (ФРН), «расистсько-національний фронт» (Англія); Ку-клукс-клан, «арійські нації» (США);

2) Лівацькі, ультрареволюційні терористичні організації «Червоні бригади» (Італія), «фракції Червоної Армії», «антиімперіалістичний осередок опору імені Наді Шебадах» (ФРН), «Деф-Сол» (Туреччина), «Сендеро Луміносо» і «революційний рух Тупака Амуру» (Латино-американські), «Японська Червона Армія» (Японія) і т. д.;

3) Націоналістичні-сепаратистські «Ірa» (Англія), «ЕТА» (Іспанія), «Чорний вересень» (Палестинська), «Фронт національного визволення Корсики» (Франція), «Тигри визволення Таміл І лама» (Шрі-Ланка) та ін.;

4) Релігійно-політичні терористичні «Хамас» (Палестина, Ізраїль), «Хезболлах» (Ліван), «Брати-мусульмани» (Єгипет, Сирія, Саудівська Аравія), «озброєна Ісламська група» (Алжир, Франція), «Аум Сінріке» (Японія) та ін.;

- Екстремістські організації антиконституційної спрямованості всередині окремих країн, що використовують насильство як основний метод політичної боротьби і допускають застосування тероризму (подібні організації існують, наприклад, в даний час не тільки в традиційних районах поширення тероризму, але також в Росії і ряді інших країн СНД).

Виступаючи в якості складного соціально-політичного феномена, тероризм може бути класифікований в залежності від методів, цілей, суб'єктів, використовуваних засобів, ідеологічної основи і за іншими критеріями.

Залежно від використовуваних методів прийнято виділяти «фізичний» і «психологічний» терор.

«Фізичний» терор пов'язаний із застосуванням безпосереднього насильства до індивідів. Воно може характеризуватися позбавленням особи (групи осіб) життя, нанесенням тілесних ушкоджень, обмеженням волі та ін.

«Психологічний» терор може виражатися в досягненні страхітливого ефекту шляхом руйнування матеріальних об'єктів (підприємств, установ, комунікацій та ін), знищення (пошкодження) майна держави, громадських та інших організацій, приватних осіб. Крім того, до «психологічного» терору може бути віднесено морально-психологічне насильство, здійснюване шляхом шантажу, погроз та інших дій з метою примусити державу, її органи та інші суб'єкти виконувати вимоги терористів.

За переслідуваним цілям в наукових джерелах виділяються політичний, неполітичний (корисливо-економічний) тероризм; акти терору, вчинені на грунті ірраціональної мотивації психічно хворими особами.

Залежно від характеристик об'єкта терористичного впливу прийнято розмежовувати «селективний» терор, тобто спрямований на конкретних державних, громадських діячів, громадян, їх майно і «масовий» («сліпий»).

У разі «масового» терору суспільно небезпечні посягання здійснюються щодо будь-якої безлічі людей в громадських місцях (вулиці, парки, вокзали, об'єкти транспорту, на виробничих підприємствах та ін.).

У числі загальновизнаних критеріїв класифікацій розглянутого феномена важливе місце займає характер використовуваних засобів, в залежності від яких виділяють «традиційний» і «технологічний» тероризм.

До «традиційного» відносять застосування насильства, знищення або пошкодження матеріальних об'єктів, засноване на використанні широко поширених, давно відомих людству засобів ураження, в тому числі вогнепальної, холодної, метальної зброї, вибухових речовин та інших.

«Технологічний» тероризм характеризується застосуванням нових засобів ураження, створених з використанням передових технологій - радіоактивних, хімічних речовин, отрут, біологічних культур та ін.

Таким чином, в умовах нарощування в світі процесів глобалізації та формування інформаційного суспільства тероризм став виступати в якості самостійного чинника, здатного загрожувати державній цілісності країн і дестабілізувати міжнародну обстановку. Зростає ступінь впливу сучасного тероризму не тільки на складові внутрішньої політики окремих держав, а й на міжнародну безпеку. При цьому особливо гостро питання забезпечення інформаційної безпеки як однієї з важливих складових національної безпеки постає в контексті появи транснаціональної (транскордонної) комп'ютерної злочинності та кібертероризму. Загроза кібератак є цілком реальною, і пов'язані з нею ризики оцінюються фахівцями як високі.

При цьому можна виділити наступні основні його види:

1) інформаційно-психологічний тероризм – контроль над ЗМІ з метою поширення дезінформації, чуток, демонстрації потужності терористичних організацій; вплив на операторів, розробників, представників інформаційних і телекомунікаційних систем шляхом насильства або загрози насильства, підкупу, введення наркотичних і психотропних засобів, використання методів нейролінгвістичного

програмування, гіпнозу, засобів створенні ілюзій, мультимедійних засобів для введення інформації в підсвідомість і т. д.;

2) інформаційно-технічний тероризм – нанесення шкоди окремим фізичним елементам інформаційного середовища держави; створення перешкод, використання спеціальних програм, що стимулюють руйнування систем управління, або, навпаки, зовнішнє терористичне управління технічними об'єктами (в т. ч. літаками), біологічні та хімічні засоби руйнування елементної бази і т. д.; знищення або активне придушення ліній зв'язку, неправильне адресування, штучне перевантаження вузлів комутації і т. д.

Очевидно, що кібератаки, виходячи з цілей і методів інформаційного впливу, можуть бути віднесені до одного з видів інформаційного тероризму. Деструктивні впливи ж при цьому завжди буде здійснюватися із застосуванням кіберпростору.

Існує багато способів, за допомогою яких терористичні групи використовують можливості новітніх інформаційних технологій та глобальну мережу Інтернет у своїх цілях [4-7]:

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

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

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

- збір, в т. ч., вимагання грошей для підтримки терористичних рухів;

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

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

- залучення в терористичну діяльність нових членів, в тому числі нічого непідозріваючих співучасників, наприклад хакерів, яким не відомо до якої кінцевої мети приведуть їх дії;

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

- семантичні атаки, метою яких є злом сторінок і подальше розміщення (без помітних слідів злому) на них завідомо неправдивої інформації. Подібним атакам, як правило, піддаються найбільш часто відвідувані інформаційні сторінки, змісту яких користувачі повністю довіряють;

- виведення з ладу або зниження ефективності функціонування структурних елементів інформаційно-телекомунікаційних систем шляхом: застосування спеціальних програмних і апаратно-програмних засобів на основі програмного коду (програмні та апаратні закладки, комп'ютерні віруси, мережеві черв'яки і т. п.); масової розсилки електронних листів (одна з форм «віртуальної блокади»); DOS-атак, проведення яких аналогічно технології масової розсилки електронних листів, що призводить до уповільнення роботи обслуговуючого сервера або повного припинення зовнішнього доступу до його ресурсів.

Таким чином, на відміну від традиційного тероризму, який не загрожував суспільству як такому і не зачіпав основ його життєдіяльності, сучасний високотехнологічний тероризм здатний продукувати системну кризу в будь-якій державі з високорозвиненою інформаційною інфраструктурою. Розвиток соціальних мереж супроводжується все більш широким використанням їх можливостей для здійснення інформаційного протиборства, зростанням координації, масштабів і складності дій його учасників, в якості яких найчастіше виступають як держави, так і окремі організовані групи, в т.ч. терористичні. Об'єктом кібератак все частіше стають інформаційні ресурси, виведення з ладу або утруднення функціонування яких може завдати протилежній стороні значної економічної шкоди або викликати великий суспільний резонанс.

## 2.3. Протидія інформаційному тероризму в рамках міжнародних організацій та форумів

Перш за все, активна боротьба з тероризмом ведеться в рамках Організації Об'єднаних Націй. Вона була створена в 1945 році, і в даний час включає 193 держави. Її місія і роль визначається Статутом ООН.

У доповіді групи високого рівня щодо загроз, викликів і змін містяться наступні напрямки діяльності ООН по боротьбі з тероризмом:

- стримування, заохочення соціальних і політичних прав, боротьба з організованою злочинністю, зменшення масштабів убогості і безробіття і запобігання розпаду держав;

- зусилля по боротьбі з екстремізмом і нетерпимістю, в тому числі за допомогою освіти і сприяння публічним обговоренням;

- розробка більш дієвих інструментів для глобального співробітництва в боротьбі з тероризмом Доповідь групи високого рівня по загрозам, викликам і змінам.

Деякі дослідники вважають, що вже принципи міжнародного права, що містяться в Статуті ООН, забороняють державам вдаватися до терористичної діяльності. Наприклад, у резолюції 748 (1992) від 31 березня 1992 р., Рада Безпеки ООН визначила, що відповідно до принципу, викладеного в п. 4 ст. 2 Статуту ООН (згідно з яким держави утримуються від загрози силою або її застосування в міжнародних відносинах), «кожна держава зобов'язана утримуватися від організації, заохочення терористичних актів в іншій державі, сприяння таким актам або участі в них, а також потурання в межах своєї території організованої діяльності, спрямованої на вчинення таких актів, коли подібні акти пов'язані з загрозою силою або її застосування». Інші принципи міжнародного права так само, в тій чи іншій мірі, сприяють координації діяльності держав у боротьбі з тероризмом.

Величезне значення має робота контртерористичного комітету в рамках Ради Безпеки ООН. Він був створений в 2001 році на основі положень резолюцій 1373 (2001) і 1624 (2005) Ради Безпеки. КТК сприяє зміцненню потенціалу держав-членів у боротьбі з тероризмом, як на національному, так і на міжнародному рівні.

Резолюція 1373 (2001) від 28 вересня 2001 року, закликає до здійснення ряду заходів, спрямованих на зміцнення можливостей держав-членів в області боротьби з тероризмом:

- запровадити кримінальну відповідальність за фінансування тероризму та не надавати фінансову підтримку терористичним групам;

- заблокувати кошти осіб, замішаних у терористичних актах;

- вести обмін інформацією, співпрацювати з іншими урядами в розслідуванні, видачі та переслідуванні осіб, замішаних в таких актах;

- встановити в національному законодавстві відповідальність за сприяння тероризму.

Резолюція 1624 (2005) пропонує, в тому числі, заборонити підбурювання до вчинення терористичних актів.

КТК використовує такі методи роботи як відвідування країн (з метою відстеження досягнутого прогресу), технічну допомогу, доповіді країн (необхідні в якості інструменту для діалогу між країнами-членами), передові методи і спеціальні наради (допомагають у поліпшенні координації зусиль) Рада Безпеки контртерористичний комітет. Існування численних терористичних організацій зумовило створення спеціальних підрозділів КТК, що координують окремі угруповання.

Затверджено комітет Ради Безпеки відповідно до резолюцій 1267(1999) і 1989 (2011) з організації Аль-Каїда і пов'язаних з нею осіб і організацій, так як складною залишається ситуація афгано-пакистанської зони.

У резолюціях цього Комітету містяться такі вимоги як:

- негайне заморожування фінансових активів зазначених осіб та організацій;

- недопущення в'їзду на свою територію або проїзду через неї;

- запобігання постачанням зброї та пов'язаних з ним матеріальних цінностей зазначеним особам комітет Ради Безпеки , заснований резолюціями 1267(1999) і 1989(2011) з організації «Аль-Каїда» і пов'язаним з нею особам і організаціям.

Комітет Ради Безпеки, заснований резолюцією 1988(2001) стосується діяльності організації «Талібан» або пов'язаних з ним у створенні загрози миру, стабільності і безпеки в Афганістані містить аналогічні вимоги, тобто заморожування активів, заборона на поїздки і збройове ембарго комітет Ради Безпеки, заснований резолюцією 1988 (2011).

Важливий внесок у систему протидії фінансуванню тероризму вносить група розробки фінансових заходів боротьби з відмиванням грошей. Вона була створена в 1989 році за рішенням країн «Великої сімки» і є основним міжнародним інститутом, що займається розробкою і впровадженням міжнародних стандартів у цій сфері.

Не можна недооцінювати важливу роль Інтерполу, міжнародної організації кримінальної поліції, створеної в 1923 році.

Інтерпол включився в боротьбу з тероризмом в 1985 році. На засіданні 54-ї Генеральної Асамблеї у Вашингтоні було прийнято рішення про створення спеціальної групи, яка займеться «координацією боротьби з міжнародним тероризмом».

У 1998 р. Генеральний секретаріат Інтерполу приймав Керівництво по співпраці в боротьбі з тероризмом, в якому описані практичні заходи, які можуть бути вжиті для вдосконалення співпраці в боротьбі з міжнародним тероризмом. 27 жовтня 1998 р. резолюцією Генеральної Асамблеї Інтерполу прийнята Декларація по боротьбі з тероризмом.

Також істотний внесок у боротьбу з тероризмом вносять регіональні міжнародні організації. Боротьба з тероризмом ведеться в рамках Ради

Європи, південно-азіатської асоціації регіонального співробітництва (СААРК), Організації Американських держав (ОАД), Організації Ісламського співробітництва (ОІС). Для забезпечення координації своїх дій в СНД був заснований Антитерористичний центр, а також прийнята відповідна програма по боротьбі з міжнародним тероризмом.

Таким чином, співробітництво в боротьбі з тероризмом здійснюють як універсальні міжнародні організації, такі як контртерористичний комітет в рамках ООН, Інтерпол та ін., так і регіональні організації.

# РОЗДІЛ 3. ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ І НАЦІОНАЛЬНА БЕЗПЕКА УКРАЇНИ

## 3.1. Періодизація та види терористичних атак на інформаційний простір України

У сучасному світі міжнародний тероризм досяг такого рівня, що став представляти реальну загрозу існування всього людства. В умовах глобалізації, коли стираються кордони, створюються транснаціональні корпорації, інформаційні потоки, що впливають на свідомість різних соціальних груп, стають все більш інтенсивними і практично не контрольованими з боку держави, немає такої держави в світі, яка б на 100% убезпечила себе, громадян і суспільство від проявів тероризму.

Україна, в силу свого геополітичного розташування, території, клімату, земель сільськогосподарського призначення, розвитку промисловості, наукового потенціалу та військово-промислового комплексу, постійно відчуває політичний, економічний та інформаційний вплив з боку розвинених країн Євросоюзу, США і особливо Росії.

Прагнення Росії домогтися економічного краху України, багатонаціональний склад українського народу і не продумана політика керівництва України в економічній, політичній і соціальній областях дозволяють припустити високу ймовірність організації терористичних актів на території України.

Для правильного аналізу суспільно-політичної ситуації та вироблення рекомендацій щодо недопущення виникнення терористичних організацій і припинення терористичних актів, необхідно чітко розуміти зміст таких понять як «тероризм», «терор» і «терористичний акт».

В даний час налічується понад 200 визначень поняття «тероризм». Це обумовлено як розширенням кількості країн, в яких почали відбуватися терористичні акти, так і специфічними національними особливостями здійснення терористичних актів в цих країнах. Крім того, це пояснюється по-перше, ідеологічною тенденційністю: визначаючи ті чи інші політичні дії як терористичні, політологи і політики керуються своїми ідейними симпатіями і антипатіями. По-друге, тероризм зачіпає різні аспекти життєдіяльності людей: юридичні, історичні, психологічні, технологічні. Його важко відокремити від таких понять, як «злочин», «насильство», «війна», «агресія». З одного боку, це ускладнює процедуру аналізу, а з іншого — сприяє більш повному розумінню феномена тероризму.

Так, під тероризмом розуміється насильство або загроза його застосування щодо фізичних осіб або організацій, а також знищення (пошкодження) або загроза знищення (пошкодження) майна та інших матеріальних об'єктів, створюють небезпеку загибелі людей, заподіяння значної майнової шкоди або настання інших суспільно небезпечних наслідків, здійснювані з метою порушення громадської безпеки, залякування населення, або надання впливу на прийняття органами влади рішень, вигідних терористам, задоволення їх неправомірних майнових і (або) інших інтересів; посягання на життя державного або громадського діяча, вчинене з метою припинення його державної чи іншої політичної діяльності або з помсти за таку діяльність; напад на представника іноземної держави або співробітника міжнародної організації, що користуються міжнародним захистом, а так само на службові приміщення або транспортні засоби осіб, які користуються міжнародним захистом, якщо це діяння скоєно з метою провокації війни або ускладнення міжнародних відносин.

Держдепартаментом США використовується наступне визначення тероризму: це навмисне політично мотивоване насильство, що застосовується субнаціональними групами або таємними державними агентами проти небойових цілей, як правило, спрямоване на вплив на громадськість.

У свою чергу, закони Сполученого Королівства Великобританії та Північної Ірландії визначають тероризм як застосування серйозного насильства (або загроза його застосування) проти будь-якої особи; заподіяння серйозної шкоди (або загроза його заподіяння) майну; створення серйозного ризику здоров'ю або безпеці суспільства, серйозне втручання в забезпечення життєдіяльності суспільства або підрив електронних систем, якщо ця дія відбувається з метою вплинути на уряд, залякати суспільство (або його частину) з політичних, релігійних або ідеологічних підстав.

Більш яскраво, радикально і масштабно тероризм проявляється в країнах Середньої Азії та Близького Сходу. Експерти відзначають, що в даний час збережеться високий і всезростаючий рівень насильства на етнічному і націоналістичному грунті. Палестинці і курди, сикхи і таміли, ірландські католики і валлійці, вірмени та азербайджанці будуть збирати і плекати свої образи.

В Україні, згідно закону України «Про боротьбу з тероризмом», тероризм – це суспільно небезпечна діяльність, яка полягає у свідомому, цілеспрямованому використанні насильства шляхом захоплення заручників, підпалів, убивств, тортур, залякування населення та органів влади або вчинення інших посягань на життя чи здоров'я ні в чому не винних людей або погрози вчинення злочинних дій з метою досягнення злочинних задумів.

Проаналізувавши безліч визначень тероризму, можна встановити наступні характерні риси:

- Залякування.
- Використання нічим не обмеженого насильства.
- Публічність загрози вчинення терористичного акту.
- Політична та ідеологічна мотивація.
- Терористи розраховують головним чином на психологічний ефект своїх дій, а не на військово-стратегічну перемогу.

Для більш чіткого визначення тероризму як політичного явища необхідно зрозуміти взаємозв'язок понять «тероризм» і «терор». Багато дослідників висловлюють точку зору, згідно з якою суб'єктами терору є державні структури, а тероризму — неурядові групи. При цьому зброєю терору є репресії, а зброєю тероризму терористичні акти.

Відповідно до закону України «Про боротьбу з тероризмом» терористичний акт – це злочинна дія у вигляді використання зброї, організації вибуху, підпалу, або інших дій, відповідальність за які передбачена статтею 258 Кримінального кодексу України.

Комплексно проаналізувавши існуючі поняття тероризму, можна уявити більш точне його визначення: тероризм — це використання насильства для досягнення ідеологічних і політичних цілей шляхом примусу державних органів, окремих громадян до вчинення тих чи інших дій на користь терористів, запобігання реалізації останніми загроз у вигляді терористичних актів по відношенню до певних осіб або соціальних груп.

Необхідно відзначити, що зрозуміти природу тероризму багато в чому дозволяє аналіз таких понять як екстремізм і радикалізм. Під екстремізмом більшість експертів розуміють агресивну поведінку (настрій) особистості, найбільш істотними зовнішніми проявами, якого є:

нетерпимість до думки опонента, орієнтованого на загальноприйняті в даному суспільстві норми; схильність до прийняття крайніх (силових) варіантів вирішення проблеми; неприйняття консенсусу як цінності і ділового інструменту щоденної діяльності; неприйняття особистості і її самої як цінності.

Як соціально-політичне явище екстремізм являє собою одну з форм політичної боротьби, яка характеризується запереченням сформованих державних, суспільних інститутів і структур, прагненням підірвати і знищити їх стабільність для досягнення власних владних устремлінь. Для політичного екстремізму тероризм є способом досягнення і утримання влади незаконним, насильницьким шляхом з усіма супутніми цьому наслідками. В рамках права і справедливості цивілізованим шляхом досягнення влади виступає законний спосіб її придбання. Тероризм є насильницьким злочинним методом досягнення і утримання влади для всіх сил національного, релігійного, політичного екстремізму. Політичні екстремісти також мають радикальні погляди і переконання, так багато з них належать до незаконних і заборонених політичних організацій. Однак якщо вони не застосовують насильство для здійснення своїх задумів, то не можуть бути віднесені до терористів. У своїх діях екстремісти можуть використовувати різні методи: від ненасильницьких, таких, як пропаганда (гасла, заклики, виступи в пресі і на зборах), масові виступи і страйки, до різного ступеня легітимності насильницьких (організовані заворушення, страйки, громадянська непокора, терористичні акти, методи партизанської війни).

На думку експертів, екстремізм являє собою ідеологічний і емоційний фундамент тероризму, становить його суть і зміст. Екстремістські ідеї характеризуються агресивним настроєм, нетерпимістю, одновимірністю, схильністю до прийняття крайніх варіантів вирішення

проблем. Вони визначають засоби, методи, масштаби і об'єкт терористичної діяльності.

Поряд з екстремізмом тероризм часто плутають з радикалізмом. Радикал (від латинського radix - корінь) - прихильник корінних, рішучих заходів. У літературі радикалізм найчастіше визначають як тактику (способи і методи дій), що сповідує крайні заходи. Радикальними можуть бути ідейно-політичні течії, кардинально (радикально) відхиляються від норм і цінностей, прийнятих в суспільстві. Тому індивідів або організації слід вважати радикальними, якщо вони проводять яскраві акції протесту, сповідують корінні і загальні зміни в суспільстві, викликають негативну реакцію при владі. Залежно від ступеня терпимості і демократичності самого суспільства і державної системи, радикальними можуть вважатися не тільки блокування доріг, захоплення будівель, а й збір підписів протесту, пікети та інші мирні публічні акції.

Визначити поріг радикальності дозволяє не стільки самовідчуття тієї чи іншої групи, скільки негативне, нетерпиме ставлення з боку суспільства або, принаймні, державної влади.

Аналіз соціально-політичної ситуації в Україні показує, що приводом до виникнення терористичних організацій може служити проведення урядом антинародної політики, значне погіршення економічної ситуації, масове порушення прав і свобод громадян.

Поки суспільно-політична ситуація в Україні така, що не існує передумов до створення терористичних організацій громадянами України. Водночас існує реальна загроза організації терористичних актів з боку диверсійно-розвідувальних груп Російської Федерації, а також громадян України, які відстоюють інтереси Російської Федерації та зацікавлені у знищенні України як незалежної держави.

### 3.2. Нормативно-правова база протидії інформаційному тероризму в Україні

Аналіз підходів до сутності, ознак, концепції та еволюції інформаційного тероризму; виявлення основних соціально-культурних та інформаційних передумов розвитку інформаційного тероризму в контексті розвитку глобалізаційних процесів сучасності; з'ясування основних причин використання терористичними угрупованнями інформаційно-комунікативних технологій; визначення загальних політико-правових та морально-етичних принципів обмеження діяльності засобів масової інформації у контексті боротьби з терористичними проявами; –прояв зовнішньої агресії та збройний конфлікт на Сході України дають підстави для розгляду та аналізу сучасного стану вітчизняного організаційно-правового механізму протидії інформаційному тероризму в Україні. Тому тематика дослідження є сучасною та актуальною.

Сьогодні ні світова спільнота в особі компетентних організацій таких ка ООН, ОБСЄ тощо, ні українське законодавство не дають чіткого визначення інформаційному тероризму. Це, в свою чергу, гальмує і обмежує організаційно-правові можливості компетентних органів у боротьбі з цим актуальним злочинним явищем. Катастрофічною є відсутність чітко вираженого ієрархічного державного механізму протидії інформаційному тероризму в Україні.

Існування цивілізованого світу завжди супроводжувалося якоюсь надбудовою управління, формуючи при цьому за допомогою певних механізмів політику державного управління, в тому числі політику регулювання на загрози національній безпеці. –З плином часу змінюються умови «політичної гри» і ці механізми державного управління вимагають модернізації. У зв'язку з цим, а також з урахуванням постійно зростаючої і

змінюючої вигляд загрози тероризму також вимагають постійного перегляду і удосконалення заходів з підвищення ефективності реагування на загрози національній безпеці. Сьогодні у світі, в тому числі і в Україні, широкомасштабного поширення набуває проблема інформаційного тероризму, як сучасна і одна з основних загроз інформаційній безпеці будь-якої країни, регіону, світу. Питання вироблення ефективного механізму державного управління інформаційною сферою, аналіз дієвості громадських організацій у сфері запобіганню терористичних і екстремістських проявів, а також міжнародне співробітництво з цього питання сьогодні є вкрай актуальними для України, особливо в контексті забезпечення безпеки людини, суспільства і держави.

Організаційно-правовий механізм протидії інформаційному тероризму в Україні має складатися з:

- суб'єктів, що безпосередньо організовують, забезпечують і здійснюють боротьбу з інформаційним тероризмом;
- правові норми повноважень, наділених цих суб'єктів;
- форм і методів діяльності цих суб'єктів, спрямованих на попередження, виявлення, блокування і нейтралізацію проявів інформаційного тероризму.

Перша складова - суб'єкти боротьби з тероризмом визначені Законом України «Про боротьбу з тероризмом» [1]. Закон також визначає Антитерористичний центр при Службі безпеки України, як головний координуючий орган, що відповідає за боротьбу з тероризмом в Україні. На Антитерористичний центр при Службі безпеки України покладається:

- розробка концептуальних основ і програм боротьби з тероризмом, рекомендацій, спрямованих на підвищення ефективності заходів з виявлення та усунення причин і умов, що сприяють вчиненню

терористичних актів та інших злочинів, що здійснюються з терористичною метою;

- збір у встановленому порядку, узагальнення, аналіз і оцінка інформації про стан і тенденції поширення тероризму в Україні та за її межами;
- організація і проведення антитерористичних операцій і координація діяльності суб'єктів, які ведуть боротьбу з тероризмом або залучаються до конкретних антитерористичних операцій;
- організація і проведення командно-штабних і тактико-спеціальних навчань і тренувань;
- участь у підготовці проектів міжнародних договорів України, підготовка та надання в установленому порядку пропозицій щодо вдосконалення законодавства України у сфері боротьби з тероризмом, фінансування проведення суб'єктами, які ведуть боротьбу з тероризмом, антитерористичних операцій, здійсненням заходів щодо запобігання, виявлення та припинення терористичної діяльності;
- взаємодія зі спеціальними службами, правоохоронними органами іноземних держав та міжнародними організаціями з питань боротьби з тероризмом.

Досвід минулих років свідчить про те, що підхід до аналізу вітчизняного антитерористичного законодавства умовно можна розділити на два етапи: до 2014 року, коли антитерористичні операції в Україні мали переважно точковий характер, і після 2014 року, коли в Україні проводилася масштабна антитерористична операція на сході країни, яка переросла в квітні 2018 року у військову операцію об'єднаних сил.

Первісна редакція Закону України «Про боротьбу з тероризмом« передбачала проведення антитерористичних операцій, –як комплексу скоординованих дій відповідних спецслужб і правоохоронних органів на

певній території, обмеженого за часом і засобами протидії. Але вже починаючи з 2014 року Закон зазнав істотних змін – на сьогоднішній день в нього внесено більше 15 змін і доповнень. Це дозволило розглядати проведення антитерористичної операції не тільки як діяльність спецслужб і правоохоронних органів, а впровадити цілий комплекс заходів, реалізація яких покладається на безліч органів виконавчої влади, органів державної влади та органів місцевого самоврядування в межах їх повноважень. Суттєвим стало те, що тепер антитерористична операція може здійснюватися одночасно з відсіччю збройної агресії в порядку статті 51 Статуту Організації Об'єднаних Націй та/або в умовах введення воєнного або надзвичайного стану відповідно до Конституції України та законодавства України. Вперше прописаний правовий механізм, що дозволяє залучати Збройні Сили України та підрозділи спеціального призначення по боротьбі з тероризмом з метою усунення загрози державній безпеці. Відсутність чіткої законодавчої регламентації застосування Збройних Сил України в кризових ситуаціях зумовила врегулювання всіх аспектів можливості їх практичної участі у справі боротьби з тероризмом. Тим більше, що питання застосування зброї і бойової техніки, особливо щодо повітряних, морських і річкових суден, є досить гострим, що яскраво показало їх обговорення в засобах масової інформації.

З метою захисту громадян, держави і суспільства від терористичних загроз в районі проведення тривалої антитерористичної операції, як виняток, Закон дозволяє здійснювати і визначає правову процедуру превентивного затримання осіб, причетних до терористичної діяльності, на термін понад 72 години, але не більше ніж на 30 діб.

Закон також встановлює відповідальність організаціям, що здійснюють терористичну діяльність і процедуру їх притягнення до

відповідальності. Як наслідок, внесення змін до Закону зумовило можливість розвитку інформаційної складової протидії тероризму, тобто підготувало підґрунтя для підвищення ефективності протидії інформаційному тероризму, поглибленню та конкретизації організаційно-правових механізмів у цій сфері.

На жаль, сам головний антитерористичний документ держави (Закон України «Про боротьбу з тероризмом») в частині реагування на інформаційну загрозу терористичних проявів (тобто реагування на інформаційний тероризм) досі не змінився. Детермінанта інформаційного тероризму в ньому випливає з кореляційного зв'язку поняття технологічного тероризму, який відбувається з терористичною метою із застосуванням засобів електромагнітного впливу, комп'ютерних систем і комунікаційних мереж, прямо або побічно створюють загрозу або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій і представляють небезпеку для персоналу, населення і навколишнього середовища, або створюють умови для аварій і катастроф техногенного характеру. А статтями 15 і 17 Закону обумовлені фактори взаємодії осіб, які залучаються до проведення антитерористичної операції з представниками громадськості, а також вводяться критерії на заборону висвітлення в ЗМІ інформації про форми і методи проведення антитерористичної операції.

Іншими словами, в головному законі країни у сфері протидії тероризму ми спостерігаємо слабку детермінацію і, як наслідок, малоефективне загальне нормативне визначення повноважень, суб'єктів по боротьбі з тероризмом для здійснення ними практичних дій у справі боротьби з інформаційним тероризмом. Натомість вітчизняний нормотворець виділяє окремий Закон України «Про основні засади забезпечення кібербезпеки України» [2]. У ньому наводиться поняття

кібертероризму - терористична діяльність, здійснювана в кіберпросторі або з його використанням. Розглядаючи Закон далі, бачимо, що кіберпростір – це середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворена в результаті функціонування спільних (об'єднаних) комунікаційних систем і забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

Отже, особливе значення серед нормативно-правових актів щодо забезпечення інформаційної безпеки України має Стратегія національної безпеки України [5], яка спрямована на реалізацію до 2020 року визначених нею пріоритетів державної політики національної безпеки. Аналіз документа вказує на те, що Національна система кібербезпеки повинна, перш за все, забезпечувати взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ і організацій, які є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури.

Наступним важливим нормативно-правовим актом є Воєнна доктрина України, що є «системою поглядів на причини виникнення, сутність і характер сучасних військових конфліктів, принципи та шляхи запобігання їх виникненню, підготовку держави до можливого військового конфлікту, а також на застосування військової сили для захисту державного суверенітету, територіальної цілісності, інших життєво важливих національних інтересів» [7].

Документ грунтується на результатах аналізу і прогнозування військово-політичної обстановки і високої готовності сил до оборони. До

військово-політичних викликів, здатних перерости в загрозу застосування військової сили проти України, серед інших віднесено цілеспрямований інформаційний (інформаційно-психологічний) зовнішній вплив з використанням сучасних інформаційних технологій, спрямовані на формування негативного міжнародного іміджу України, а також на дестабілізацію внутрішньої соціально-політичної обстановки, загострення міжетнічних і міжконфесійних відносин всередині України, або її окремих регіонах і місцях компактного проживання національних меншин.

Серед основних завдань військової політики України визначено: удосконалення державної інформаційної політики у військовій сфері; попередження та ефективну протидію інформаційно-психологічним впливам іноземних держав, спрямованим на підрив обороноздатності, порушення суверенітету і територіальної цілісності України, дестабілізацію внутрішньої соціально-політичної обстановки, провокування міжетнічних і міжконфесійних конфліктів в Україні.

Ще одним значущим нормативним правовим актом, що опосередковано охоплює проблеми протидії інформаційному тероризму, що супроводжуються збройним протистоянням, є концепція розвитку сектору безпеки і оборони України [8]. Нею визначено, що основною метою реформування та розвитку сектору безпеки і оборони є формування та підтримання можливостей, що дозволить гарантовано забезпечити адекватне та гнучке реагування на весь спектр загроз національній безпеці України, раціонально використовуючи наявні в державі можливості та ресурси. Серед основних завдань сектору безпеки і оборони визначено забезпечення інформаційної та кібербезпеки.

У березні 2019 року Президентом України була затверджена Концепція боротьби з тероризмом в Україні [9]. Концепція спрямована на вдосконалення загальнодержавної системи боротьби з тероризмом з

урахуванням сучасних терористичних загроз національній безпеці України та прогноз їх розвитку. Також в концепції наводиться визначення об'єктів можливих терористичних посягань, до яких також відноситься «...інформаційний простір і його компоненти...». Важливим завданням, що виділяється в документі, є удосконалення інституційного механізму координації діяльності суб'єктів по боротьбі з тероризмом.

Виходячи з вищевикладеного та беручи до уваги той факт, що організаційно-правовий механізм протидії інформаційному тероризму повинен складатися з суб'єктів боротьби з інформаційним тероризмом, правових норм, форм і методів їх діяльності, на жаль, сьогодні в Україні можна спостерігати кілька розпилений та дезорієнтований в просторі і між компетентними органами комплексний підхід до вирішення завдання боротьби з інформаційним тероризмом.

Плачевно усвідомлювати той факт, що спостерігаючи постійні процеси глобалізації світу, рушійною силою яких є потужний інформаційний прогрес поняття інформаційного тероризму навіть не закріплено на законодавчому рівні, хоча, на мою думку, являє собою головну інформаційну загрозу для держави. Логіка вказує на те, що при координаційній ролі РНБО України вибудовувати організаційно-правовий механізм протидії інформаційному тероризму необхідно Антитерористичному центру при Службі безпеки України, як державному інституту, який відповідає за це. Практичне втілення цього антитерористичного законодавства, на жаль, про це мовчить. Разом з тим, розглядаючи сучасний стан розробленості та впровадження організаційно-правового механізму протидії інформаційному тероризму в Україні, аналіз інформаційно-психологічного та інформаційно-технічного його двох аспектів бачимо досить насичену, хоча і не структуровану «картину державного управління позначеними цими процесами». Все це вимагає

наукового пошуку напрямів формування системи забезпечення інформаційної безпеки України в контексті протидії інформаційному тероризму.

### 3.3. Співробітництво України з міжнародними організаціями у сфері протидії інформаційному тероризму

Боротьба з тероризмом є глобальною і зачіпає всі країни світу, без винятку. В 21 столітті тероризм активізувався, став більш масштабним, і є головною загрозою століття. Найбільшою загрозою в сучасному світі є загроза застосування ядерної зброї або інших засобів масового ураження, дія яких відіб'ється не тільки на окремій території будь-якої держави, а й на світ в цілому. Дана тема є актуальною, і вимагає найтіснішого міжнародного співробітництва в пошуку найбільш оптимальних і дієвих вирішень даної проблеми.

Міжнародне співробітництво важливе і в плані того, що тероризм в кожній країні має свої специфічні риси, знаннями про які володіють тільки представники регіону, в якому відбувається терор. Тому інформування інших держав про специфіку терору в тій чи іншій країні дозволяє іншим державам своєчасно вживати заходів і протидіяти терору.

Сьогодні міжнародне співробітництво з протидії терору відбувається на 3-х рівня:

1. Універсальному, яке відбувається під егідою Організації Об'єднаних Націй. На цьому рівні розробляються загальні принципи з міжнародного співробітництва, головне завдання яких забезпечити мир і захист прав людини. Перші міжнародні акти, що стосуються протидії тероризму були розроблені в 20-30 роки 20 століття. У 1937 році в Женеві було схвалено Конвенцію про попередження тероризму та покарання за

нього та Конвенцію про створення Міжнародного кримінального суду [1]. В даний час створена різнобічна система співробітництва держав по боротьбі з тероризмом на чолі егіди ООН, в якій прийняті 16 Конвенцій і угод про захист від тероризму на землі, в повітрі і на морі. Україна є учасником більшості конвенцій.

2. Регіональному, де Міждержавна взаємодія відбувається на основі наступних об'єднань (Ліга арабських держав, Організація Американських Держав, організація ісламського співробітництва, Організація африканської єдності, Співдружність Незалежних Держав, Європейський союз, Шанхайська організація співробітництва (ШОС) та інші). Головне завдання на даному рівні полягає в протистоянні тероризму, сепаратизму і політичному екстремізму [9]. Правова база даних об'єднань обширна, також проводяться спільні військові навчання держав-членів ШОС, в яких зусилля України визнані найбільш пріоритетними у сфері діяльності ШОС.

3. Двосторонньому, де присутні ряд міжнародних договорів по боротьбі з тероризмом між Російською Федерацією і Швецією, Великобританією, Норвегією, Індією, Бразилією і багатьма іншими країнами. Україна активно бере участь у створенні даних угод, а також розробляє проекти зі створення загальної системи протидії новим загрозам тероризму на основі норм міжнародного права.

Практика видання численних наказів, вказівок, рішень, постанов робить сформовану нормативну документацію неозорою і непридатною для регулювання процесу міжнародного співробітництва. В даному нормативному акті дано визначення тероризму, а саме: «тероризм - ідеологія насильства і практика впливу на прийняття рішення органами державної влади, органами місцевого самоврядування або міжнародними організаціями, пов'язані з залякуванням населення та (або) іншими

формами протиправних насильницьких дій» [2]. У Законі відображені основні моменти, що стосуються міжнародного співробітництва України в галузі боротьби з тероризмом. Ця норма повністю відповідає Резолюції 1624 Ради Безпеки ООН 2005 року, спрямована на залучення антитерористичних зусиль на міжнародному рівні.

Однак на міжнародному рівні в нормативно-правовій системі немає загальновизнаного визначення поняттю «тероризм», але виділені специфічні ознаки, такі як: насильство, протидія закону в основному із застосуванням зброї, наявність безвинних жертв, якщо це насильство йде проти ряду держав, то додається і міжнародний елемент. Протягом часу тероризм набув додаткових характерних ознак, наприклад, транскордонність і соціальна стійкість, це сталося в результаті терактів що почастішали, з наявністю великої кількості жертв, які вже не стали екстраординарними явищами в житті суспільства і держави. Зросла частота терористичних актів вказує на неефективність методів боротьби з даною проблемою [7]. Розглянемо основні проблеми в міжнародному співробітництві з боротьби з терором на сучасному етапі.

Тероризм в сучасному світі технологічний, жорстокий і масштабний. За 2019 рік у багатьох країнах було скоєно безліч терактів різної величини. Головним чином це країни Ірак, Афганістан, Нігерія, Сирія, Пакистан і Ємен. Дані держави не можуть самостійно протистояти терористичним актам, кількість яких зростає швидше, ніж заходи по боротьбі з ними. Після того, як в Сирії вдалося перемогти «Ісламську державу» групи терористів почали проникати в країни Центральної Азії, Південно-Східної Азії, Європи, і важливо знайти спосіб протистояти цьому явищу. Успішна боротьба з тероризмом можлива, що було доведено операціями російських збройних Сил в Сирії і прогрес, досягнутий в рамках дипломатичних зусиль Росії, Ірану і Туреччини при врегулюванні сирійського конфлікту.

Найважливішою умовою такого успіху є багатосторонній формат: широке міжнародне співробітництво, залучення всіх сторін, зацікавлених у стабілізації становища в кризових регіонах. Саме в Сирії, можна вважати, що був проведений перший етап до створення по-справжньому ефективних міжнародних механізмів боротьби з тероризмом [6].

Але головна проблема полягає в тому, що міжнародне співробітництво здійснюється відокремлено, обмеженою кількістю країн, через небажання країн включатися в даний процес, а також те, що дослідження проблеми, навчання і напрямок правоохоронної діяльності, розробка і випробування технічних або оперативних методів боротьби з тероризмом, а також удосконалення законодавства на міжнародному рівні відбувається із запізненням, тільки після того, як відбуваються великі міжнародні терористичні акти, що є звичайно ж, не допустимим і не ефективним механізмом боротьби [5].

Ще одним з головних недоліків у сфері міжнародної діяльності з протидії тероризму є те, що навіть за наявності угоди, договору або іншого нормативного акта між окремими регіонами або країнами співпраця не здійснюється належним чином, а саме з наступних причин:

- різні держави трактують терористичний акт відповідно до свого законодавства, тому для однієї країни вироблені дії будуть визнані як, тероризм, а для іншої держави , як прояв боротьби за незалежність або свободу;

- захист власних інтересів країни ставиться на першорядний рівень, ніж міжнаціональний;

- брак кваліфікованих кадрів, що мають досвід роботи з розробки заходів протидії тероризму;

- обмін інформацією відбувається не оперативно, через відсутність єдиної системи для обміну даними;

- потрібні нові засоби і способи для збору даних про терористів і їх плани;

- відсутність покарань до країн, які не надають інформацію про терор на їх території

- дефіцит економічних коштів у держави, для здійснення міжнародної співпраці на належному рівні.

На підставі викладеного, для вирішення вищевказаних проблем у сфері розвитку міжнародного співробітництва по боротьбі з тероризмом важливо організувати наступні заходи:

- розробити систему контролю та моніторингу за рішеннями у сфері боротьби з терором;

- спонсорувати держави, які мають бажання брати участь у процесі міжнародного співробітництва в галузі боротьби з міжнародним тероризмом, але не мають фінансових можливостей на організацію даного процесу;

- визначити санкції до держав, які не виконують свої зобов'язання в рамках укладених угод або міжнародних актах з протидії тероризму;

- об'єднати зусилля щодо захисту інформаційного простору держав регіону від поширення ідей тероризму та екстремізму;

- підготовка кваліфікованих кадрів.

Підводячи підсумок, необхідно підкреслити, що головне завдання в 21 столітті по боротьбі з тероризмом полягає в тому, щоб сприяти країнам у подоланні розбіжностей, які існують в даний момент і знайти єдиний підхід у сфері міжнародно-правового співробітництва.

# ВИСНОВКИ

Таким чином, можна зробити висновки. Тероризм, як будь-яке негативне соціальне явище відчуває постійні зміни. У зв'язку з виниклими на сучасному етапі потенційними можливостями використання при скоєнні злочинів новітніх інформаційних технологій, телекомунікаційних систем і засобів, кіберпростору, з'явився новий найбільш небезпечний вид тероризму, якого одні називають кібертероризмом або електронним тероризмом, інші – інформаційним тероризмом. Кібертерор - страшна річ. Кібертерористи можуть нанести дуже великих збитків навіть не користуючись фізичною силою. Але разом із кібертероризмом розвивається сфера його протидії. Новітні можливості країн світу вже вміють уникати, протидіяти та нейтралізовувати кібератаки. Важлива ціль держави та органів безпеки - розробити такі умови, аби наші генії комп'ютерних наук не шукали грошей порушуючи закони, а допомогали нашим фахівцям боротись із цим злом.

Як відомо, в даний час серйозна підготовка до скоєння злочинів терористичної спрямованості, як правило, вимагає активного використання інформаційних ресурсів, в тому числі і з метою забезпечення широкої середовищної підтримки злочинних акцій. Для цього, наприклад, ще в кінці минулого і початку нинішнього століття міжнародними терористами, що діяли в Чеченській Республіці, було сформовано спеціальний підрозділ. Створене сепаратистським ідеологом М. Удуговим так зване інформаційне агентство «Кавказ-центр», відкрило однойменний сайт в мережі Інтернет. Це агентство займалося поширенням дезінформації про успіхи терористів і великі втрати федеральних сил з метою сформувати у світової громадськості і керівництва іноземних держав негативне ставлення. У цій злочинній акції використовувалися

понад 100 фінансованих терористами сайтів російською, англійською, арабською, французькою та іншими мовами. Лідерами терористів були створені інформаційні центри в Азербайджані, Грузії, Україні, Литві, Фінляндії, Туреччині та Польщі. Кібертероризм являє собою серйозну загрозу для людства, порівнянну з ядерною, бактеріологічною і хімічною зброєю; причому ступінь цієї загрози в силу своєї новизни не до кінця ще усвідомлена і вивчена. Досвід світової спільноти в цій галузі з усією очевидністю свідчить про безсумнівну уразливість будь-якої держави, тим більше що кібертероризм не має державних кордонів, кібертерорист здатний в рівній мірі загрожувати інформаційним системам, розташованим практично в будь-якій точці земної кулі.

Цей термін вперше був запропонований ще в 80-х минулого століття старшим науковим співробітником Інституту безпеки і розвідки (англ. Institute for Security and Intelligence) Баррі Колліном, який використовував його в контексті тенденції до переходу тероризму з фізичного у віртуальний світ, зростаючого перетину і зрощення цих світів. Він визначив його як використання комп'ютерних і телекомунікаційних технологій в терористичних цілях. У Вікіпедії комп'ютерний тероризм (кібертероризм) також визначається як використання комп'ютерних і телекомунікаційних технологій (насамперед, інтернету) в терористичних цілях.

Перш за все, активна боротьба з тероризмом ведеться в рамках Організації Об'єднаних Націй. Вона була створена в 1945 році, і в даний час включає 193 держави. Її місія і роль визначається Статутом ООН.

У доповіді групи високого рівня щодо загроз, викликів і змін містяться наступні напрямки діяльності ООН по боротьбі з тероризмом:

- стримування, заохочення соціальних і політичних прав, боротьба з організованою злочинністю, зменшення масштабів убогості і безробіття і запобігання розпаду держав;

- зусилля по боротьбі з екстремізмом і нетерпимістю, в тому числі за допомогою освіти і сприяння публічним обговоренням;

- розробка більш дієвих інструментів для глобального співробітництва в боротьбі з тероризмом Доповідь групи високого рівня по загрозам, викликам і змінам.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Віктор В. В. «Лівий» тероризм на Заході: історія і сучасність / В. В. Віктюк, С. Ф. Есфіров. - М.: Наука, 1987. - 315 с.

2. Воробйов І. М. Збройний конфлікт: боротьба з диверсійно-терористичною діяльністю противника / І.М. Воробйов, В. А. Кисельов // Військова думка. – 2006. – № 1. – С. 34 – 40.

3. Воробйов І. М. Організація боротьби з диверсійно-терористичними формуваннями противника в операції / І.М. Воробйов, В. А. Кисельов // Там само. – 2006 – № 2. – С. 2 – 8.

4. Воробйов І. М. Протидиверсійний і протитерористичний захист військ в операції і бою / і.м. Воробйов, В. А. Кисельов // Там само. – 2006. – № 3. – С. 29 – 34; № 4. – С. 48 – 53.

5. Гайдук Е.Г. Тероризм в сучасному суспільстві: структура, основні види і цілі / Е. Г. Гайдук // сучасне право. – 2002. – № 1. – С. 11 – 16.

6. Жарінов К. Тероризм і терористи: іст. довід. / К. Жарінов - Мінськ: Харвест, 1999. - 604 с.

7. Про боротьбу з тероризмом: закон України від 20.03.2003 р. № 638-IV // Відомості верхів. Ради України. – 2003. – № 25. - Ст. 180.

8. Князь І. С. До питання протидії можливим терористичним проявам в територіальних та внутрішніх водах України / І. В.Князь, П. Б. Волотівський, Ю. Л. Домніцький // Наука і оборона. – 2008. – № 1. - С. 20-24.

9. Кожушко О. Сучасний тероризм. Аналіз основних напрямків / О. Кожушко . - Мінськ: Харвест, 2000. - 447 с.

10. Про ратифікацію Конвенції Ради Європи Про запобігання тероризму: закон України від 31.07.2006 р. № 54-V // Відомості верхів. Ради України. – 2006. – № 39. - Ст. 340.

11. Кулик С. Система і сили протидії морському тероризму в Чорноморському регіоні / С. Кулик, Д. Штибликов // Чорноморська безпека. – 2006. – № 2. – С. 65 – 70.

12. Литвинов Н. Д. Міжнародний тероризм / Н. Д. Литвинов. - СПб.: Пітер, 2002. - 286 с.

13. Надьон О. Правовий аналіз передумов виникнення загрози тероризму в Україні / О. Надьон // Право України. – 2003. – № 3. – С. 24 – 28.

14. Возженіков А. В. Міжнародний тероризм. Боротьба за геополітичне панування / А.В. Возженіков, М. А. Виборнов, А. Ю. Гончаров; під ред. А. В. Возженікова. - М.: Ексмо, 2007. - 528 с.

15. Сельцовський П.А. Різновиди і форми тероризму в сучасних умовах / П. А. Сельцовський // соціально-гуманітарне знання. – 2003. – № 4.– С. 301 – 307.

16. Требін М.П. Тероризм в XXI столітті / М. П. Требін. - Мінськ: Харвест, 2004. - 816 с.

18. Горбунов, Ю.С. Тероризм і правове регулювання протидії йому / Ю. С. Горбунов. - М.: Молода Гвардія, 2008. - 464 с.

19. Дікаєв, С.У. Терор, тероризм і злочини терористичного характеру / С.У. Дікаєв. - М.: Юридичний центр Прес, 2006. - 464 с.

20. Девіс, Лі Тероризм і насильство / Лі Девіс. - М.: Русич, 1998. - 496 с.

21. Єфімов, Ігор Грядущий. Минуле,сьогодення і майбутнє міжнародного тероризму / Ігор Єфімов. - М.: Абетка-класика, 2008. - 368 с.

22. Жарінов, К. В. Тероризм і терористи. Довідник / К. В. Жарінов. - Москва: Вогні, 1999. - 608 с.

23. Журавель, Валерій 2006 р. Протидія тероризму / Валерій Журавель, Наталія Король, Олександр Полуєв. - М.: ТОМ, 2007. - 252 с.

24. Зубков, В.А. Російська Федерація в міжнародній системі протидії легалізації (відмиванню) злочинних доходів і фінансуванню тероризму / В. А. Зубков, С. К. Осипов. - Москва: Вогні, 2007. - 752 с.

25. Іванов, В. Н. Сучасний тероризм / В.Н. Іванов. - М.: РАГС, 2006. - 262 с.

26. Іванов, І.Є. Психологія тероризму. Попередження та припинення терористичних актів / І.Є Іванов. - М.: Камея, 2005. - 125 с.

27. Іконніков-Галицький, Анджей Самогубство імперії. Тероризм і бюрократія. 1866-1916 / Анджей Іконніков-Галицький. - М.: сучасна інтелектуальна книга, 2013. - 352 с.

28. Іконніков-Галицький, Анджей Самогубство імперії. Тероризм і бюрократія. 1866-1916 / Анджей Іконніков-Галицький. - М.: сучасна інтелектуальна книга, Лімбус прес, 2016. - 368 с.

29. Іслам проти тероризму. - Москва: Вогні, 2003. - 200 с.

30. Казарін, О.В. Методологія захисту програмного забезпечення. Наукові проблеми безпеки та протидії тероризму / о.в. Казарін. - М.: МЦНМО, 2009. - 464 с.

31. Кассіс, В. Тероризм без маски / В Кассіс, Л. Колосов. - М.: Молода Гвардія, 1983. - 176 с.

32. Каптан, В. В. Протидія тероризму. Навчальний посібник / В.В. Кафтан. - М.: Юрайт, 2015. - 262 с.

33. Кілясханов, Х.Ш. ОБСЄ в боротьбі з тероризмом / х. Ш. Кілясханов. - М: Юнити-Дана, Закон і право, 2013. - 524 с.

34. Кіршин, Ю. Концепція воєн і боротьби з міжнародним тероризмом демократичних держав / Ю.Кіршин. - М.: Видавництво Клинцовской міської друкарні, 2002. - 220 с.

35. Кожушко, Євген. Аналіз основних напрямків / Євген Кожушко . - М.: Харвест, 2000. - 448 с.

36. Кокошин, А.А. Замітки про проблему ядерного тероризму в сучасній світовій політиці / А.А. Кокошин. - М.: Едиториал УРСС, 2004. - 580 с.

37. Колегаєва, Т. П.; Тероризм І Екстремізм-Загроза Xxi Століття. Бібліографічний Список літератури: моногр. / Т. П. Колегаєва;. - Москва: Вогні, 2010. - 901 с.

38. Коряковцев, В.В. Коментар до Федерального закону «Про легалізацію (відмивання) доходів, одержаних злочинним шляхом, і фінансування тероризму» / В.В Коряковцев, К. В. Пітулько. - М: Питер, 2003. - 432 с.

39. Коряковцев, В.В. Коментар до Федерального закону «Про боротьбу з тероризмом» (постатейний Науково-практичний) / В. В. Коряковцев, К. В. Пітулько. - М: Питер, 2003. - 416 с.

40. Кошель, П. Історія російського тероризму / П.Кошель. - Москва: Гостехиздат, 1995. - 376 с.

41. Крусанов, Павло Діюча модель пекла. Нариси про тероризм і терористів / Павло Крусанов. - М.: АСТ, Астрель-СПб, 2004. - 224 с.

42. Кузнєцов, Д.В. Події 11 вересня 2001 року і проблема міжнародного тероризму в дзеркалі громадської думки / Д. В. Кузнєцов. - М.: Либроком, 2009. - 400 с.

43. Ліллі, Пітер Брудні угоди. Таємна правда про світову практику відмивання грошей, міжнародну злочинність і тероризм / Пітер Ліллі. - М.: Фенікс, 2005. - 400 с.

44. Лукін, В. Н. Глобалізація і міжнародний тероризм / В. Н. Лукін. - М.: Наука, 2006. - 496 с.

45. Лукоянов, Едуард «Хочеться якогось культурного тероризму і бажано прямо зараз» / Едуард Лукоянов. М.: трансліт, вільне марксистське видавництво, 2013. - 162 с.45. Лукоянов, Едуард «Хочеться

якогось культурного тероризму і бажано прямо зараз» / Едуард Лукоянов. М.: трансліт, вільне марксистське видавництво, 2013. - 162 с.

46. Маркович, І.В. Біологічна зброя. Проблеми поширення, тероризму, політика протидії / І.В. Маркович, А.Є. Симонова. - Москва: Вогні, 2011. - 240 с.

47. Міжнародний тероризм. Боротьба за геополітичне панування. - М.: Ексмо, 2007. - 528 с.

48. Мішин, Б.І. Антитерор. Дидактичний матеріал з профілактики тероризму та надання першої медичної допомоги. 5-11 класи / Б.І. Мішин, В. В. Абатурова, А.В. Легкобитов. - М.: Вентана-Граф, 2014. - 954 с.

49. Мішин, Б. І. Антитерор. Заходи з профілактики тероризму. Набір плакатів для оформлення кабінету ОБЖ. 5-11 класи / Б.І Мішин, В.В. Абатурова, А.В Легкобитов. М.: Вентана Граф, 2014. - 891 с.49. Мішин, Б. І. Антитерор. Заходи з профілактики тероризму. Набір плакатів для оформлення кабінету ОБЖ. 5-11 класи / Б.І. Мішин, В. В. Абатурова, А.В Легкобитов. - М.: Вентана-Граф, 2014. - 891 с.

50. Моджорян, Л. А. Тероризм. Правда і вигадка: моногр. / Л.А. Моджорян. М.: Юридична література, 1983. - 208 с.

51. Моджорян, Л.А. тероризм: правда і вигадка / Л. А. Моджорян. - М.: Книга на вимогу, 2012. - 244 с.

52. Мохаддам, Фаталі Тероризм з точки зору терористів. Що вони переживають і думають і чому звертаються до насильства / Фаталі Мохаддам. М.: Форум, 2011. - 288 с.

53. Нікітін, А.І. Конфлікти, тероризм, миротворчість / А.І. Нікітін. - М.: Навона, 2009. - 232 с.

54. Нуждин, Лев Нуждин / Лев Нуждин. - М.: Ікар, 2014. - 276 с.