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

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувачка випускової кафедри
_____ Ніна РЖЕВСЬКА
«____»_____2022 р.

КВАЛІФІКАЦІЙНА РОБОТА
ЗДОБУВАЧА ВИЩОЇ ОСВІТИ ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА
СПЕЦІАЛЬНОСТІ 291 «МІЖНАРОДНІ ВІДНОСИНИ, СУСПІЛЬНІ
КОМУНІКАЦІЇ ТА РЕГІОНАЛЬНІ СТУДІЇ» ОСВІТНЬО-ПРОФЕСІЙНОЇ
ПРОГРАМИ «МІЖНАРОДНА ІНФОРМАЦІЯ»

Тема: «ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ В СУЧАСНИХ МІЖНАРОДНИХ ВІДНОСИНАХ»

Виконавець: здобувачка вищої освіти 4 курсу, 409 Б групи Барвінська Марія Андріївна

Керівник: к. політ. н., доцент кафедри міжнародних відносин, інформації та регіональних студій Поведа Олександр Петрович

Нормоконтролер _____ Валентина ЄМЕЦЬ
(підпис)

КИЇВ, 2022

ЗМІСТ

ВСТУП……..……..…….……..3
РОЗДІЛ 1. ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ В СУЧАСНИХ МІЖНАРОДНИХ ВІДНОСИНАХ: ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ…….....……...…6
1.1. Поняття міжнародного інформаційного тероризму…….……...…..6
1.2. Види та причини інформаційного тероризму……...11
РОЗДІЛ 2. ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ: РОЗРОБКА СТРАТЕГІЇ ПРОТИДІЇ…….……19
2.1. Міжнародні інституційні механізми протидії інформаційному тероризму…….……..…17
2.2. Міжнародно-правове забезпечення боротьби з актами інформаційного тероризму……...…21
РОЗДІЛ 3. УДОСКОНАЛЕННЯ МЕТОДІВ ПРОТИДІЇ ІНФОРМАЦІЙНОМУ ТЕРОРИЗМУ…….……...……..…30
3.1. Сучасний стан державно політики у сфері інформаційної безпеки в Україні……...…….……...…30
3.2. Основні напрями вдосконалення системи забезпечення інформаційної безпеки в контексті протидії інформаційному тероризму……..…..…..……38
ВИСНОВКИ…….…….…46
СПИСОК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ…….....…..48

ВСТУП

Актуальність теми дослідження. Процес глобалізації включає розвиток глобальної економіки, науки та інформаційного простору. Розвиток міжнародних комунікаційно-інформаційних мереж відіграє ключову роль у забезпеченні цілісності сучасного світу. Протягом останнього десятиліття особлива увага як на законодавчому, так і на доктринальному рівнях приділялася правовій базі забезпечення безпеки інформаційного простору проти різноманітних викликів і загроз, зокрема інформаційної війни, інформаційного тероризму та інформаційної злочинності. Це пов'язано із глобальними процесами інформатизації та прогресом інформаційних технологій. Тероризм характеризується масштабами терористичних актів, високим рівнем організації та фінансування, різким збільшенням технічного та технологічного оснащення (терористичні організації, такі як Хезболла, ХАМАС та ІДІЛ, мають складну структуру, уряд, теле- та радіостанцію), що веде до виникнення нових його форм. Крім того, з кожним роком зростає кількість терористичних злочинів.

Незважаючи на тенденцію до цілісності та єдності, все ще існують серйозні відмінності майже в кожній сфері людського існування у світі (економіка, культура, соціальні умови тощо). Активний вплив тероризму на суспільно-політичні процеси нині є постійним і значним деструктивним явищем. Проблема тероризму, будучи відносно незалежною, постає як частина глобального спустошення, що має значний вплив на суспільно-політичні процеси на світовому, регіональному та національному рівнях. Дослідження та вирішення цього питання зумовлює необхідність міждисциплінарного зближення природничих, соціальних і науково-технічних знань, а також обґрунтованого міжнародного співробітництва у розробці та реалізації комплексних цільових програм. На тлі сучасного розвитку національних і міжнародних фінансово-економічних, соціально-культурних, політичних, технологічних процесів тероризм формується як самостійний фактор, що має значний вплив на політичну ситуацію у світі, регіонах і країнах. Ефективний спосіб створення

цілеспрямованої конфліктної ситуації, реалізації певної політичної поведінки та виправдання політичної та економічної експансії. На жаль, поняття «інформаційна війна» сьогодні як ніколи актуальне.

У класичному розумінні інформаційна війна - це форма інформаційного протистояння, комплекс заходів щодо впливу на суспільну свідомість, зміни поведінки людей і встановлення цілей, які не відповідають їхнім інтересам. Раніше вважалося, що інформація лише забезпечує інформування людей про події та факти навколишнього світу. Інформація розглядалася як корисний ресурс, призначений для підтримки людей. У сучасних умовах інформаційна війна розглядається військовими теоретиками як якісно новий вид боротьби, активний контрнаступ в інформаційному просторі, а інформація як потенційна зброя і зручна ціль. Інформаційна війна розглядає інформацію як окремий об'єкт або зброю, яка не завдає фізичної шкоди, але може призвести до реальної війни. Інформаційна зброя, як правило, не спрямована на заподіяння втрат робочій силі противника. Вона не руйнує фізично людські, матеріально-технічні та інші ресурси, а підриває основи організаційних та управлінських механізмів. На даний час боротьба з тероризмом є однією з актуальніших проблем сучасного суспільства. Пояснення сучасного тероризму в контексті глобалізації можливе лише в контексті полісистемного та багатоаспектного підходів, що дозволить врахувати якомога більшу кількість умов та факторів. Враховуючи особливу соціальну загрозу, дослідження цього явища мають велике значення та актуальність. Дослідженням проблеми займаються як українські, так і зарубіжні вчені, вивчаючи вплив інформаційного тероризму на сучасне суспільство.

Це питання вивчали такі українські вчені: Балицький В.В., Богуцький П.П., Авдошин І.В., Слюсаревський М.М., Майоров В.В., Горбулін В.П., Задорожній О.В. та ін. Зарубіжні вчені: Додонов О.Г., Жайворонок О.І., Сідненко Г.Ф., М.Я. Девост, Б.Х. Хоутон, Н.А. Полла.

Метою дослідження є дослідження проблеми боротьби з інформаційним тероризмом як елемента національної безпеки, визначення генезису поняття інформаційного тероризму, комплексний аналіз практики та особливостей

міжнародної боротьби з цим явищем, визначення сутності поняття інформаційного тероризму.

Для досягнення цієї мети визначено наступні **завдання дослідження:**

– вивчення історії та розвитку поняття «інформаційний тероризм»;

– аналіз феномену інформаційного тероризму як засобу впливу на сучасне інформаційне поле;

– розкрити сучасний стан державної політики України та основні напрями розвитку системи інформаційної безпеки;

– аналіз міжнародно-правового забезпечення та інституційних механізмів у боротьбі з інформаційним тероризмом.

Об'єктом дослідження є міжнародні відносини у сфері протидії інформаційному тероризму.

Предметом дослідження є особливості міжнародного досвіду та вітчизняної практики, на прикладі України, способи і шляхи протидії інформаційному тероризму.

Методологічною основою роботи є сукупність загальних і спеціальних методів політології. Під час написання дослідження використовувалися різноманітні загальнотеоретичні та спеціально-наукові методи та підходи для вивчення предмета дослідження. Основними методами дослідження були історичний - у вивченні та з'ясуванні умов виникнення поняття інформаційного тероризму; метод формально використовувався при аналізі законодавства іноземних держав щодо боротьби з терористичними нападами; порівняльний метод дослідив відповідальність за тероризм на міжнародному та національному рівнях. Крім цих методів, використовуються також системний аналіз, логічний метод та структурно-функціональний метод.

Практичне значення роботи: робота мас теоретико-практичне значення і може бути використана у якості матеріалів для підготовки лекцій з дисциплін, орієнтованих на вивчення тематики інформаційного тероризму.

Структура кваліфікаційної роботи: робота складається зі вступу, трьох розділів, висновків та списку використаних інформаційних джерел.

РОЗДІЛ 1. ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ В СУЧАСНИХ МІЖНАРОДНИХ ВІДНОСИНАХ: ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ

1.1. Поняття міжнародного інформаційного тероризму

Тероризм, який спочатку виник як національне явище, тепер є загрозою для всього світового співтовариства, про що свідчить різноманітність міжнародних документів, які певним чином вирішують питання, пов'язані з визначенням явища, контрзаходами та судовими процесами. Тероризм, як і всі негативні соціальні явища, зазнає постійних змін. Завдяки новим інформаційним технологіям, телекомунікаційним системам та інструментам, використанню кіберпростору, на цьому етапі з'явився новий, найнебезпечніший вид тероризму, який одні називають електронним тероризмом або кібертероризмом, інші – інформаційним кібертероризмом. Інформаційний тероризм становить серйозну загрозу для людства на рівні з ядерною, бактеріологічною та хімічною зброєю; до того ж масштаби цієї небезпеки через її новизну ще до кінця не відомі та не вивчені. Досвід світового співтовариства в цій сфері чітко свідчить про беззаперечну вразливість будь-якої держави, тим більше, що кібертероризм не має державних кордонів, кібертероризм може продовжувати загрожувати інформаційним системам, розташованим практично в будь-якій точці світу [6, с. 146].

Наразі всі діючі терористичні та екстремістські організації мають власні веб-сайти у всесвітній мережі. Зазвичай вони містять детальний огляд політичних і соціальних мотивів, що призвели до створення терористичних та екстремістських організацій, інформацію про ідеологічні та політичні цілі, які вони переслідували, інформацію про найвідоміші акції, біографії засновників і «героїв», а також огляд актуальних новин. Сучасні релігійно-екстремістські та терористичні організації все частіше використовують глобальний інформаційний

простір як «прес-центр» для закликів терористів, бойовиків, релігійних радикалів, повстанців [3, с. 110].

Створені антисоціальні сайти зроблені на високому професійному рівні з великою кількістю візуальної інформації: фото, аудіо та відео файлів, створених для полегшення сприйняття інформації та залучення додаткової підтримки та фінансування. На цих сайтах часто міститься інформація про тактику та засоби терористичних актів, види отруйних і вибухових речовин, основи роботи з вибуховими речовинами, виготовлення саморобних вибухових пристроїв, методи змови [16].

Екстремістські та терористичні організації намагаються використовувати комунікаційні можливості всесвітньої мережі для залякування суспільства, поширення антисоціальної інформації та пропаганди своїх злочинних ідей. На міжнародному рівні роками намагаються пояснити існування тероризму, який часто впливає на фізичну цілісність, життя, здоров'я людей тощо.

Визначення тероризму загалом є суперечливим і складним, і через насильство та жорстокість, притаманні тероризму, цей термін став сильно стигматизованим у суспільному вживанні. Вперше він був виголошений у 1790-х роках для позначення терору, який використовували революціонери проти своїх супротивників під час Французької революції. Якобінська партія Максиміліана Робесп'єра здійснила «панування терору», закликаючи до масових страт за допомогою гільйотини. Хоча тероризм у цьому сенсі є актом державного насильства проти своїх внутрішніх ворогів, починаючи з 20-го століття цей термін найчастіше використовується для позначення прямого чи непрямого насильства проти урядів з метою впливу на політику чи повалення існуючого режиму.

Інформаційний тероризм – це явище, яке безпосередньо впливає на психіку та мислення, щоб виробити необхідні судження та думки, які так чи інакше керують поведінкою людей [11]. На практиці під інформаційним тероризмом зазвичай розуміють насильницьку пропаганду, що впливає на психіку, що не дозволяє людям критично оцінити отриману інформацію. Перш за все, інформаційний тероризм з усією інформацією негативно впливає на людей,

державу та суспільство. Його метою є послаблення конституційного ладу держави. Це здійснюється будь-якими доступними способами, від агентів іноземних спецслужб до іноземних і державних ЗМІ [87].

У деяких країнах тероризм, як і інформаційний тероризм, не має правового поняття. Проте, безсумнівно, розвиток такої концепції передусім визначить, де саме на національному рівні займають місце злочини, пов'язані з тероризмом. Дослідники М. Дж. Девост, Б. Х. Хоутон і Н. А. Поллард визначають інформаційний тероризм як навмисне зловживання цифровими інформаційними системами, компонентами або мережами таких систем або мереж для сприяння терористичним актам або операціям. Дороті Деннінг, професор комп'ютерних наук Джорджтаунського університету та провідний експерт з кібербезпеки та кіберзлочинності, у своїй книзі «Атака або загроза: Інтернет як засіб впливу на зовнішню політику» пише влучний вислів: «Дані атаки на комп'ютери, мережі чи інформацію, проводяться з єдиною метою - змусити уряд переслідувати соціальні та політичні цілі» [81, с. 192].

За даними Є.А. Роговського, згідно з цим визначенням, можна назвати два види кібертероризму:

1) безпосереднє здійснення терористичних процесів з використанням комп'ютерних мереж і комп'ютерів;

2) використання кіберпростору терористичними угрупованнями для комунікаційних та організаційних цілей та для вимагання, але не для прямих терористичних атак [5, с. 113].

Перший вид відповідає поєднанню термінів «кіберпростір» і «тероризм» і передбачає навмисний напад на комп'ютерні мережі або інформацію, комп'ютери, комп'ютерні програми, що ними обробляються, що спричиняє смерть, значну шкоду майну чи іншу небезпеку для населення. Наприклад, прослуховування керівництва інфраструктури чи військового об'єкта з метою загрози аварії (катастрофи), порушення громадської безпеки, впливу на прийняття громадських рішень чи залякування громадськості [20, с.36]. Перший вид кібертероризму – це так звані «інформаційні» злочини проти конституції

(неконституційне оскарження, загрози конституційним свободам і правам особи і громадянина, погрози інформаційній політиці, поширення жахливих чуток тощо).

Другий вид кібертероризму – використання терористичними групами інформаційного простору для комунікаційних та організаційних цілей (але не для прямих терористичних атак), військової, теоретичної, богословської пропаганди, а також вербування нових членів та встановлення зв'язків між осередками. На даний момент у науковій літературі не існує загальноприйнятого визначення поняття «кібертероризм» [30].

Тероризм є багатогранним, складним і мінливим явищем. Феноменом тероризму займаються вчені різних дисциплін (політологи, соціологи, психологи та ін.). Звісно, повне вивчення цього негативного явища та його наслідків, а також профілактика можливі лише після встановлення особи, відповідальної за соціальний розвиток понятійного апарату [8, с. 231].

Також важливо подбати про розуміння поняття інформаційного простору. Інформаційний простір – це сукупність результатів смислової діяльності людини. Багаторівнева структура, що акумулює результати компанії з використанням конкретних компонентів інформаційно-комунікаційної системи [24].

У власній «реляційній теорії інформаційного простору» М. Слушаревський розглядає інформаційний простір як стан (і результат) споживання інформації та постійної взаємодії, тобто інформаційний простір як простір для обробки інформації. При цьому, якщо хтось сприймає інформацію, то існування інформації можна вважати можливим, тобто обов'язковою умовою обробки інформації є наявність «джерела – приймача» у системі зв'язку. Передбачається, що параметри інформаційного простору визначаються психологічними та часовими характеристиками інформаційного процесу, а також соціально-психологічними характеристиками споживачів інформації. Тому цю категорію рекомендується характеризувати не за обсягом виробництва інформації чи обсягом поширення інформації, а за її інтенсивністю та споживанням. Тому категорія інформаційного простору сповнена власних теорій – змісту спілкування та соціальної психології, відокремленої від географії та інших рівнів, і починає

відігравати самостійну функцію. Центром інформаційного простору є суб'єкт, який в процесі своєї діяльності збирає, створює, зберігає та передає всю необхідну інформацію. Такими суб'єктами можуть бути соціальні групи або окремі особи, організації, компанії або навіть державні установи, тобто всі користувачі будь-яких інформаційних технологій [72, с. 340].

Характеристика терористичних актів в інформаційній сфері:

- прихований характер підготовки та здійснення таких дій – відсутність явного втручання та проявів;

- розмах атак – завданням є знищення великої кількості об'єктів;

- синхронізація атак – може виконуватися на кілька об'єктів одночасно;

- відстань – джерело нападу може бути за межами країни, де стався напад;

- інтернаціональність – шкода може поширитися на кілька або багато країн [33, с. 41].

Тероризм не є статичним явищем; воно завжди співвідноситься із соціальними змінами (технічне та інформаційне обладнання, озброєння тощо).

Тероризм стоїть у контексті процесів, що відбуваються в різних сферах діяльності держави та суспільства. Відповідно, інформаційний тероризм (кібертероризм) – це цілеспрямована атака на інформаційні системи, інформаційно-телекомунікаційні мережі та компоненти таких систем чи комп’ютерних мереж, програмно-технічні комплекси оборонних і державних органів, що мають особливе значення, та інші об’єкти, у тому числі людей. Порушення та саботування їхньої роботи, залякування населення, дестабілізація влади чи вплив на прийняття рішень, або погроза такими діями з тією ж метою, якщо такі дії призвели до смерті чи інших тяжких наслідків [89, с. 57].

Це визначення враховує обидва види кібертероризму: безпосереднє вчинення терористичних актів засобами масової інформації та використання кіберпростору терористичними групами для безпосереднього нападу на інформаційні системи, телекомунікаційні та інформаційні мережі або компоненти цих систем, або терористичні мережі. Сьогодні форми та методи захисту від

інформаційного тероризму на основі нових мережевих технологій значно підвищили ефективність та результативність, а також масштаби цієї діяльності.

По-перше, набір може здійснюватися дистанційно. Оскільки відповідні матеріали доступні майже скрізь в Інтернеті, традиційний особистий контакт стає застарілим. У той же час це полегшує завдання підбору персоналу, щоб якомога ширша аудиторія дізналася про існування та цілі організації.

По-друге, сучасні форми дистанційного рекрутингу є більш ефективними, оскільки рекрутер має можливість «підготувати» велику кількість людей, які проживають у своєму регіоні, своїй країні, а також у віддалених куточках світу. Сучасні мережеві технології, такі як відеоігри та Інтернет, підвищують здатність терористичних груп просувати та поширювати свої ідеї, у тому числі шляхом адаптації змісту та форми повідомлення до певної аудиторії [98].

1.2. Види та причини інформаційного тероризму

Інформаційний тероризм – це абсолютно нова терористична діяльність, спрямована на використання сучасних інформаційних технологій для руйнування або пошкодження громадської інфраструктури (критичної інфраструктури, яка може бути вразливою до антитерористичних атак тощо). Характеризується маніпулюванням свідомістю людини шляхом активного використання психологічних впливів [91].

У результаті широкого використання нових інформаційних технологій змінилися як засоби збройної боротьби, так і стратегія і тактика сучасної війни з урахуванням нових вразливих місць. Ці нові концепції безпосередньо пов’язані з тим, що швидкий розвиток кіберпростору може відкрити додаткові можливості для якісного розвитку озброєння та військової техніки, але це також може призвести до нових проблем і вразливостей. У сучасному світі маючи менше інформації про поле бою, інформація обробляється повільніше і рішення приймаються менш ефективно. Зрозуміло, що терористи, використовуючи новітні технічні досягнення, значно розширили свої деструктивні можливості, що

дозволяє їм привертати увагу громадськості, постійно тримати людей в страху та впливати на їхній психологічний стан. Сьогодні майже всі цифрові пристрої, які використовуються для обробки та зберігання інформації, є об’єктами терористичних атак. Залежність таких процесів від різних сфер застосування інформаційно-телекомунікаційних систем постійно зростає. Ефективність найсучасніших засобів збройної боротьби визначається насамперед умінням вести бойові дії та якістю автоматизованих систем управління та зв'язку. Існує ряд методів та інструментів впливу на такі системи шляхом дезактивації певних структурних елементів, ключових операторів або маніпулювання інформацією, що міститься в них, на користь супротивника [12, с. 165].

У той же час сам конфлікт може вступити у фазу конфронтації, а не відкритого збройного конфлікту, якщо змусити одну сторону повірити і визнати, що вона більше не може розраховувати на ефективне використання своєї зброї у війні. У будь-якому випадку сторона з найкращою стратегією та тактикою ведення військових дій (інформаційної війни) в інформаційному просторі в сучасних умовах має значні переваги.

В якості інформаційної зброї можуть виступати різні пристрої: високоточна зброя для знищення управління або радіоелектронної боротьби, джерела потужних електромагнітних імпульсів, програмні віруси та ін. Критерієм віднесення до «інформаційної зброї» може бути лише ефективність зброї у вирішенні завдань інформаційної війни. Операції з використанням індивідуальних радіоелектронних засобів, інформаційного озброєння (військова наступальна операція з використанням інформації) може здійснюватися окремо та в поєднанні, до або в підтримку традиційних наступальних дій. У будь-якому випадку метою інформаційно-наступальної операції є забезпечення «інформаційної переваги» в конфлікті шляхом впливу на засоби збору, обробки та зберігання інформації та на персонал, який керує технологіями та приймає рішення [27, с. 110].

Наразі не існує класифікації інформаційної зброї та чіткого визначення цього терміну. Варто додати, що інформаційна зброя традиційно повинна пропагувати військову перевагу, усувати фізичні масові ураження, орієнтуватися

на високоточні та найбільш ефективні засоби впливу. Важливо розділяти інформаційну зброю на оборонну та наступальну. Інформаційна оборонна зброя вирішує проблему інформаційної оборонної війни та відповідних контрзаходів. До таких чинників відносять:

- Пристрої, що впливають на компоненти електронних пристроїв та їх живлення для тимчасової або необоротної втрати працездатності окремих компонентів електронних систем.

- Інструменти забезпечення впливу та демонтажу модулів керування та зміни алгоритму за допомогою спеціального електронного програмного забезпечення на програмному ресурсі.

- Засоби впливу на процес передачі інформації з метою припинення або переривання роботи підсистем алгоритмів передачі інформації та обміну інформацією.

- Засоби пропаганди та дезінформації для зміни інформації систем управління, створення віртуальної ситуації, відмінної від реальної, зміни людських цінностей, шкоди духовно-моральному життю ворога.

- Пристрої, призначені для психіки і підсвідомості людини для зниження і придушення її волі, тимчасової втрати працездатності [26].

Не можна сказати, що ця класифікація охоплює всі види інформаційної зброї, які можуть з’явитися в майбутньому. Проте всі відомі практичні розробки, які зараз здійснюються, повністю висвітлені. Інформаційну зброю будь-якого виду можна класифікувати за кількома ознаками: одно- та багатоцільова чи універсальна; короткі та тривалі дії; індивідуальна, групова або масова поразка; за типом медіа. Вивчаючи, аналізуючи та розуміючи різні погляди на одне з найнебезпечніших і найскладніших для прогнозування сучасних явищ – інформаційний тероризм та вплив глобалізації на державотворення – ми можемо виділити та визначити його основні види.

Види тероризму:

- інформаційний та психотероризм – використання ЗМІ для поширення неправдивої інформації, чуток, терористичними організаціями; Погрози

насильством, хабарництво, поширення наркотиків і психотропних речовин, використання методів нейролінгвістичного програмування, гіпнозу, засобів створення ілюзій, мультимедійних засобів введення інформації в підсвідомість тощо.

- ІТ-тероризм – знищення окремих елементів національного інформаційного середовища, зведення бар'єрів, застосування спеціальних процедур для руйнування системи управління або, навпаки, зовнішній тероризм, що контролює та знищує технічні засоби, біологічне та хімічне руйнування, руйнування або активне придушення ліній зв'язку, неправильна адресація, штучне перевантаження вузлів комутації тощо.

- Когнітивний тероризм – легітимація насильницьких способів досягнення незаконних терористичних цілей шляхом впливу на емоційні та поведінкові елементи суспільства, створення суспільної свідомості, радикальних соціальних стереотипів, соціальних ідей та концепцій, а також підсвідоме та емоційне сприяння легалізації насильства. Вражає нестійкі, переважно емоційні погляди, особливо молодих людей, які через екстремальні та радикальні дії розуміють навколишній світ і себе. Це призводить до таких когнітивних концепцій, як радикалізм, екстремізм, фанатизм, шовінізм і фундаменталізм.

- Мережевий тероризм (кібертероризм) – масові, скоординовані дії великих соціальних мереж (автономних приватних чи неурядових організацій) з деструктивним терористичним впливом (релігійні секти, державні організації, рухи, недержавні організації, комерційні організації).

- Соціально-комунікаційний тероризм – руйнування соціальної бази спеціально розробленими програмами, які вчать людей сприймати і вірити у будь-яку інформацію (широке поширення та маніпулювання громадською думкою, свідомістю, репрезентація через фізіологічні та психологічні закони сприйняття). Використовується певний текст, певний ритм і модуляція мовлення. Маніпулювання свідомістю здійснюється шляхом занурення людей у контрольоване поле інформації, створення вигаданої картини світу. Основою формування віртуального інформаційного поля є обман [29].

Слід зазначити, що для України, де соціальна інформатизація ще на стадії зародження, а джерела інформації знаходяться в руках приватних компаній, основна загроза інформаційного тероризму йде ззовні, а не зсередини. В основному його створили іноземні та міжнародні терористи та інші злочинні групи та організації. Передумовою поширення інформаційного тероризму є неспроможність державних адміністрацій створити ефективні механізми протидії інформаційним загрозам. Особливо це помітно в контексті збройного конфлікту на сході України. Тому вдосконалення механізму боротьби з інформаційним тероризмом дозволить Україні вийти на новий рівень якості свого інформаційного законодавства та прискорить розробку ефективних заходів протидії цьому негативному явищу [69, с. 60]. Боротьба з тероризмом – це діяльність із запобігання, виявлення, припинення та мінімізації наслідків терористичної діяльності.

В. Ліпкан запропонував розумне визначення терміну, а саме: «Боротьба з тероризмом»:

- система організаційно-правових, режимних, оперативних, науково-дослідних, інженерно-бойових та інших заходів, що вживаються спеціально уповноваженими органами для запобігання, виявлення та припинення тероризму. Нейтралізація терористичних правопорушень та пост-терористичних ситуацій, розкриття злочинів цієї категорії, встановлення винних та покарання;

- комплекс економічних, політичних, правових, психологічних, організаційно-технічних заходів, спрямованих на запобігання (пом'якшення) факторів, що сприяють тероризму, запобігання, придушення та реєстрація тероризму, виявлення (розслідування, переслідування та притягнення до відповідальності) терористів, моніторинг їх поведінки;

- діяльність щодо запобігання, виявлення та придушення терористичних актів;

- підготовка та здійснення заходів, спрямованих на ліквідацію тероризму як деструктивного, та соціально небезпечного явища, у тому числі здійснення політичної, правової, соціально-економічної, інформаційної, виховної,

організаційної, оперативно-розшукової, розвідувальної та контррозвідувальної діяльності, спеціально спрямованої на протидію тероризму.

У цьому контексті виділяємо основні характеристики інформаційного тероризму:

- специфічний вид психологічної та/або кіберзлочинності;

- використання засобів масової інформації, комп'ютерних та інших мереж, інформаційно-комунікаційних систем тощо;

- використання інформаційного тероризму має психологічний вплив на населення та важливі інформаційні інфраструктури;

- відповідно до Закону України «Про боротьбу з тероризмом», технологічний тероризм може бути перетворений на ядерну, хімічну, бактеріальну (біологічну) та іншу зброю масового ураження або її компоненти, інші шкідливі для здоров’я людини речовини, електромагнітні пристрої.

- залякування для досягнення бажаного ефекту;

- мета – залучити багато людей за допомогою реклами та агітації [56].

РОЗДІЛ 2. ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ: РОЗРОБКА СТРАТЕГІЇ ПРОТИДІЇ

2.1. Міжнародні інституційні механізми протидії інформаційному тероризму

У свідомості суспільства природа інформаційного тероризму розкривається через використання або загрозу різних форм навмисного насильства проти цивільного населення або держави (особи чи групи осіб) у політичних чи релігійних цілях. Тероризм залишається серйозною загрозою, тому обов’язково потребує відповідних дій і заходів. Питання полягає в тому, які стратегії та правила слід використовувати в боротьбі з тероризмом і хто повинен стежити за дотриманням цих правил.

Боротьба з тероризмом не може бути ефективною без якісної правової підтримки. Система правової допомоги у боротьбі з терористичними правопорушеннями має бути побудована таким чином:

- Перша група нормативних актів – закони та інші нормативні акти, що визначають теорію антитерористичної безпеки та антитерористичної стратегії та є основою для боротьби з терористичними актами.

- Друга група – комплекс антитерористичних та пов'язаних з ними заходів, спрямованих на захист інтересів країни, суспільства та окремих осіб, груп і об'єднань, аналіз загрози терористичної діяльності.

- Третя група законів міститиме нормативні акти Служби безпеки України, Національної поліції та інших правоохоронних органів, що відображатимуть тактичні аспекти боротьби з тероризмом та іншими терористичними актами.

У сфері боротьби з інформаційним тероризмом дослідження будуть зосереджені на розробці державної політики та вивчення позитивного досвіду інших країн, вжиття заходів щодо боротьби з тероризмом та забезпечення організаційної основи для досліджень. Держави повинні відігравати набагато активнішу роль у забезпеченні чітких і справедливих правил інформаційної

співпраці, як у сфері цивільного права. Необхідна адекватна координація між законодавцями та правоохоронними органами, щоб створити міцну правову основу для розвитку інформаційного середовища, а не обмежувати цей розвиток надмірним регулюванням.

Проблема тероризму стала пріоритетною у Європейському Союзі з моменту прийняття Стратегії безпеки в 2003 році, з середини 1980-х років розширювалися заходи боротьби з тероризмом, зміцнювалися антитерористичні відносини зі Сполученими Штатами. Нині існує три загальні підходи до протидії тероризму з трьох різних точок зору [77].

Перший підхід базується на регуляції з боку поліції та слідства, що є найбільш поширеним у Європі. Він відображає кримінально-правове уявлення про тероризм, згідно з яким тероризм є повторюваним явищем, яке неможливо усунути, але може бути переслідувано за допомогою особливих методів правозастосування.

Другий підхід розглядає тероризм як соціальну хворобу і прагне визначити його першопричини, наприклад середовище, в якому процвітають терористичні групи та від якого вони отримують підтримку. Цей підхід передбачає розробку довгострокових стратегій усунення або виправлення соціальних дисбалансів.

Третій підхід полягає в тому, щоб розглядати тероризм через призму військової аналогії, що передбачає використання сили для запобігання катастрофі (у тому числі в країнах, що приховують або планують створення терористичних організацій) і фізичного знищення такого керівництва. У таких надзвичайних ситуаціях, як глобальний терор, такий підхід може означати повномасштабну війну.

У Китаї, наприклад, Постійний комітет Всекитайського збору народних представників розглядає перший антитерористичний закон, який вимагатиме від будь-якої іноземної високотехнологічної компанії, яка бажає надавати послуги в Китаї, надавати суспільству ключі шифрування.

У 2004 році керівники центрів боротьби з тероризмом у США, Великобританії та Австралії оголосили про намір створити єдину розвідувальну

мережу для «запобігання Аль-Каїді та її союзним силам у всьому світі». Це призвело до створення Глобальної контртерористичної мережі, до якої входять США, Національний центр боротьби з тероризмом, Об'єднаний центр аналізу тероризму у Великобританії, Національний центр поширення загроз в Австралії та Об'єднаний центр поширення загроз у Канаді.

У квітні 2007 року тодішній прем'єр-міністр Тоні Блер оприлюднив зовнішньополітичну доктрину Великобританії, оголосивши про створення підрозділу, відповідального за стратегії протидії ідеології Аль-Каїди та іншим формам екстремістської пропаганди ворожих режимів, який отримав назву RICU (Дослідницький, інформаційно-комунікаційний підрозділ). Мережа поінформованості про радикалізацію (RAN), створена Комісією ЄС, функціонує з вересня 2011 року для покращення реакції Європейського Союзу на радикалізацію.

Роль таких об'єднань також полягає в обміні передовим досвідом та розробці рекомендацій і методологій для професіоналів, які працюють у цій галузі.

Тематика запобігання інформаційному тероризму охоплює громадські організації, об'єднання та громадян, які підтримують органи державної влади та місцевого самоврядування у здійсненні антитерористичних заходів. Звичайно, більшість завдань, пов'язаних з інформаційною боротьбою з тероризмом, може і повинна вирішувати держава, але ми повинні визнати, що повний мережевий контроль держави може викликати в тому числі і певне невдоволення й опір з боку громадян, навіть коли здійснюється для досягнення благородних, соціально значущих цілей.

Крім того, абсолютизація держави в боротьбі з тероризмом в інформаційній сфері створює умови для використання її складових у формуванні авторитарних засад суспільного розвитку та перетворення їх у тоталітаризм. Аналіз вітчизняної та зарубіжної практики показує, що активне залучення неурядових організацій до національної антитерористичної системи значно підвищує ефективність її роботи.

Для ефективних дій проти руйнівного впливу тероризму мають бути запущені певні суспільно-політичні процеси.

Це включає всі три рівні правового сегменту політичної системи:

- нормативний рівень – закони, принципи та стандарти;

- власне організації антитерористичного спрямування;

- концептуальний рівень (ідеологія).

Заходи повинні бути об'єктивними, закріпленими в міжнародному праві і конкретними, а саме:

- Політичні заходи – досягнення компромісу щодо глобалізаційних процесів, у тому числі формалізації багатополярної світової системи, встановлення механізмів більш раціонального розвитку цивілізації, балансу ресурсів.

- Розвиток правових міжнародних систем вирішення глобальних і регіональних соціально-політичних конфліктів.

- Розробка системи інформаційно-психологічної безпеки, яка не допускає непрямих інформаційних механізмів і психологічних воєн; запровадження гнучких критеріїв контролю озброєнь (у тому числі ядерної зброї шляхом заборони ядерного залякування як засобу просування політичних інтересів).

- Усунення економічних передумов через ліквідацію непрямих каналів фінансування терористичних організацій та їх союзників [41].

Світова спільнота визнає, що війна з тероризмом в кінцевому підсумку не означатиме локальної перемоги. У цьому сенсі терор можна повністю ліквідувати в будь-який момент. Тому чітко визначити природу цієї війни практично неможливо. Однак у сучасному світі існують два основних напрямки розвитку безпеки: посилення антитерористичного захисту та запобігання терористичних атак.

Це включає не лише збільшення правоохоронних сил, боротьбу з тероризмом та посилення впливу розвідувальних служб, а й заходи щодо запобігання наслідкам глобальних та національних катастроф, спричинених терористичними атаками [95].

2.2. Міжнародно-правове забезпечення боротьби з актами інформаційного тероризму

На початку 21 століття тероризм став однією з найбільших загроз міжнародній безпеці. Процеси глобалізації призвели до інтернаціоналізації тероризму, трансформації його ідеологічної та інституційної основи, розширення форм і методів його існування. У зв'язку з цим одним із нагальних завдань кожної держави було вивчення низки організаційно-правових та інших заходів на національному рівні з метою їх удосконалення, необхідності поглиблення двостороннього та регіонального співробітництва та активізації діяльності всередині країни у боротьбі з тероризмом. Особливого значення набуває також питання боротьби з фінансуванням тероризму, створення відповідної нормативно-правової бази для контролю за надходженням коштів до громадських, неприбуткових організацій, офшорних зон тощо.

Важливим питанням у боротьбі з тероризмом є створення відповідної законодавчої бази та існування ефективної системи протидії на національному та міжнародному рівнях. Багато країн ухвалили спеціальні антитерористичні закони. У Великобританії, наприклад, правоохоронні та розвідувальні органи у боротьбі з тероризмом підпадають під дію двох основних законів – Про тероризм (2000 р.) та Про боротьбу з тероризмом (2001 р.) [37]. Стан і особливості сучасного етапу світового розвитку багато в чому характеризуються тим, що світова спільнота вимушена боротися з появою принципово нових загроз життю окремих суспільств, держав та їх громадян. У найбільш зловісній формі це проявляється у такому явищі, як тероризм, який використовує інформаційне суспільство у своєму розвитку, активніше ніж інші соціально небезпечні явища [100].

Оскільки тероризм як соціальне явище є вкрай негативним, а інформатизація як явище і процес зачіпає найширші верстви суспільства, цілком закономірно поставити пріоритетним питання вивчення природи тероризму, засобів та способів поширення терористичної ідеології, здійснення шантажу та політичного тиску. Бурхливий розвиток інформаційних технологій значно

розширив можливості терористичних структур не тільки для розробки нових технічних засобів терористичної діяльності, а й для створення та широкого використання технологій маніпулювання свідомістю населення в терористичних цілях.

Як згадувалося раніше, терористичні атаки мають різні політичні цілі, і тому їх можна вважати більш серйозними, ніж кримінальні злочини. Крім того, кримінальне право може бути надто слабкою «зброєю» у боротьбі з тероризмом, оскільки для знищення терористичної інфраструктури та мереж потрібні дипломатія, широкий спектр соціальних, інформаційних, культурних та економічних заходів, а також кримінальне право.

Обмеження кримінального законодавства мають сенс у громадянському суспільстві, де стримування є важливим фактором, але це може бути не так для високотехнологічної терористичної організації. Тому тероризм можна вважати великою небезпекою, оскільки це набагато більше, ніж злочин, він прагне досягти своїх цілей, навіть доходячи до самопожертви в деяких ситуаціях. Сама по собі кримінальна відповідальність не може бути універсальною платформою для протидії тероризму.

Інтерпол (Паризька конференція, 1979 р.) був першою міжнародною організацією, яка посилається на поняття кіберзлочинності. «Природа кіберзлочинності є міжнародною, як і зв'язок між різними країнами за допомогою телефону, супутника тощо. Міжнародним організаціям, особливо Інтерполу, потрібно приділяти більше уваги цьому.» Держави-члени Інтерполу брали участь в опитуванні щодо кіберзлочинності в Парижі 7-11 грудня 1981 року в рамках першого комп'ютерного семінару Інтерполу з кіберзлочинності. Це був перший крок до глобальної гармонізації кримінального законодавства щодо кіберзлочинності.

У 1982 році ОЕСР вирішила створити в Парижі комітет експертів для вивчення концепції кіберзлочинності та аналізу необхідності реформи кримінального законодавства. Підсумком роботи комітету є Огляд правової політики ОЕСР 1986 р. Держави-учасниці визначили міру, до якої такі дії можуть

бути притягнені до відповідальності. «Фальсифікація комп'ютерних документів, пошкодження комп'ютерних даних і програм, несанкціоноване проникнення та несанкціонований доступ чи перехоплення комп'ютерних систем» [65].

У 1985 році Рада Європи призначила Комітет експертів з боротьби з кіберзлочинністю. Рекомендації були розроблені виключно для національних законодавців, які займаються міжнародною злочинністю (Рекомендація R (89) 9-1989). Ця рекомендація містила основний рекомендований перелік кіберзлочинів і додатковий список. Крім того, 11 вересня 1995 р. Рада Європи прийняла додаткові рекомендації щодо процесуального права у сфері інформаційних технологій. Ці рекомендації містили 7 розділів: обшук та затримання; технологічний моніторинг; обов'язки щодо співпраці зі слідчими органами; електронні докази; використання шифрування; дослідження статистики; міжнародне співробітництво [5].

Проте в деяких країнах, особливо в Австрії, США, Польщі, Швейцарії, Швеції та інших, не існує єдиного (спеціального) антитерористичного законодавства. У цих країнах законодавство про боротьбу з тероризмом включає ряд законодавчих актів. В Ірландії, наприклад, національне законодавство про боротьбу з тероризмом міститься в Кримінальних кодексах 1939-1998 років. Наразі Бундестаг приймає власний закон про кримінальну відповідальність за терористичні правопорушення (законопроект про кримінальне правосуддя та терористські злочини). Прийняття цього закону допоможе Ірландії приєднатися до низки конвенцій ООН проти тероризму. У Фінляндській Республіці антитерористичне законодавство включає окремі статті Кримінального кодексу, спрямовані на боротьбу з протиправною антигромадською діяльністю, а також низку законів про безпеку цивільної авіації, морського транспорту, збереження та використання ядерних матеріалів тощо [94].

У Словаччині Кримінальний кодекс є основним антитерористичним правовим актом. У Швейцарії найважливішими правовими актами, що регулюють діяльність спеціальних організацій з боротьби з тероризмом та його фінансуванням, є Кримінальний кодекс, Федеральний закон «Про заходи внутрішньої безпеки» та низка постанов уряду.

У Сполучених Штатах немає всеосяжного закону, який би був зосереджений виключно на боротьбі з тероризмом. Події 11 вересня 2001 р. спонукали керівництво країни вдосконалити нормативно-правову базу протидії тероризму та виправити недоліки федерального законодавства. З цією метою прийнято низку нормативно-правових актів щодо розширення повноважень правоохоронних органів щодо розслідування терористичних злочинів та посилення боротьби з відмиванням грошей.

Вищезазначені закони передбачають: створення Міністерства внутрішньої безпеки та Групи оцінки ризиків біотероризму як головного антитерористичного органу; виконання конвенцій ООН про боротьбу з тероризмом; вжиття низки заходів для фінансового стимулювання розвитку антитерористичних технологій; порядок відшкодування шкоди, заподіяної терористичними актами; та посилення заходів щодо захисту кордонів та віз, запровадження системи біометричного контролю при в'їзді до США [50, с. 226].

У листопаді 2001 року федеральний уряд Німеччини ухвалив закон про боротьбу з міжнародним тероризмом (другий антитерористичний пакет федерального уряду). Його основна мета – внести зміни до більшості положень німецького закону про захист громадянства та Кодексу про проживання іноземців, щоб закріпити додаткові повноваження та збільшити повноваження правоохоронних органів щодо захисту населення. Законом передбачено внесення змін до 14 законів і підзаконних актів. Одним із ключових моментів цього пакету є прийняття закону, який передбачає пом'якшення покарання співучасникам за наявності достовірної інформації про інші заплановані злочини. Наприклад, німецькі правоохоронні органи завчасно шукають інформацію для підготовки до можливих терористичних атак, розкривають секретні локації розміщення та заарештовують екстремістів, які переховуються в Німеччині [50, с 227]. У 2016 році внесено зміни до Закону «Про Федеральну розвідувальну службу» (BND), якими розширюються її повноваження. Зокрема, передбачено надання права щодо зняття інформації з телекомунікаційних каналів на території ФРН, у т.ч. й прослуховування громадян країни (до цього BND не мала повноважень

здійснювати такі заходи на території країни), зберігати інформацію про користувачів Інтернету та передавати її до партнерських спецслужб. Водночас, законом передбачено посилення контролю з боку уряду та парламенту за діяльністю спецслужби.

В Індії згідно із законом, прийнятим у березні 2001 року, злочини, пов’язані з тероризмом або підбурюванням до тероризму, караються позбавленням волі на строк до п’яти років, у деяких випадках єдиною мірою покарання є смертна кара. Відповідно до закону, ухваленого у 2001 році, поліції дозволено затримувати підозрюваних на 90 днів без пред’явлення обвинувачення, а рішення суду дозволяє продовжити термін утримання під вартою ще на 90 днів.

Федеральний закон Об'єднаних Арабських Еміратів про боротьбу з тероризмом передбачає ув'язнення або страту будь-кого, хто організовує, спонсорує або керує терористичними групами. Особи, які займаються вербуванням, підготовкою чи іншим навчанням учасників терористичних груп, можуть бути засуджені до довічного або тривалого ув'язнення. Закон визначає «акт тероризму» як будь-яку дію чи бездіяльність, що призводять до індивідуального або колективного акту проти глав держав або уряду, урядових установ чи посадових осіб міжнародних урядових організацій та членів їхніх сімей. Термін «терористичний злочин» включає дії, які завдають шкоди державній або приватній власності, рухомому майну або природним ресурсам.

У Франції внесено поправки до низки законів, які доповнюють перелік правопорушень, які можуть бути віднесені до терористичних (зокрема екологічний тероризм – забруднення атмосфери, ґрунту, води тощо шкідливими для здоров'я людей або дикої природи речовинами). У справах за статтею «Тероризм» позовна давність становить 30 років.

Тому, виходячи з уже встановленого в міжнародних конвенціях визначення тероризму та в рамках норм і законів, прийнятих більшістю країн, світове співтовариство має вийти на новий рівень міжнародного співробітництва як ключового інструменту спільної боротьби з тероризмом.

Можна сказати, що питанню обміну інформацією в рамках ООН з тих пір приділено належної уваги і що норми міжнародного права, які його регулюють, досягають значного прогресу, зокрема завдяки зусиллям деяких органів ООН.

Прикладом явних результатів його практичної роботи щодо зміцнення антитерористичної співпраці на регіональному рівні буде робота Контртерористичного центру СНД (АТЦ СНД). Це спеціальна постійна філія СНД, завдання якої щодо обміну інформацією досить широкі, зокрема:

- Аналіз інформації про ситуацію, динаміку та тенденції розвитку міжнародного тероризму та інших проявів екстремізму в СНД та інших країнах.

- Створення єдиної бази даних органів безпеки, спецслужб та інших компетентних органів держав-учасниць СНД [45].

12 грудня 2016 року на засіданні Ради Безпеки Організації Об'єднаних Націй було прийнято резолюцію № 2322 (одним з авторів є Україна), яка закликає держави до укріплення та розширення міждержавної взаємодії та взаємодопомоги у сфері боротьби з тероризмом, обміну інформацією щодо терористичних організацій та бойовиків-терористів, включаючи їх біометричні та біографічні дані. У документі також зазначається важливість співробітництва між судовими та правоохоронними органами щодо розслідування злочинів, пов'язаних з тероризмом.

У ЄС вжито низку заходів, спрямованих, у першу чергу, на підвищення ефективності взаємодії та обміну інформацією між національними спеціальними та поліцейськими службами, а також посилення прикордонного контролю. У 2016 році на основі інформації Антитерористичної групи (м. Гаага) створено єдину базу даних, до якої в режимі реального часу мають доступ понад 20 європейських спецслужб. Розроблено та заплановано реалізацію пілотного проекту щодо автоматизованого обміну даними між правоохоронними органами країн-членів ЄС щодо осіб, які мають судимість. Крім цього, активізується робота з введення в дію Європейської інформаційної системи авторизації подорожей.

У багатьох країнах запроваджено та виконуються спеціалізовані програми, спрямовані на недопущення поширення у суспільстві екстремістських поглядів,

запобігання втягування молоді до участі у терористичних організаціях, застосовуються процедури амністії окремих осіб, які брали участь в терористичній діяльності, та адаптації їх до мирного співіснування. Нещодавно було призначено нового спецпредставника ОБСЄ, який буде опікуватись координацією з обміну набутого досвіду за результатами реалізації таких програм 57 країнами, що входять до цієї організації.

Все більше країн звертає увагу на можливість радикалізації людей у місцях позбавлення волі. Так, з метою запобігання цій загрозі в КНР нині розглядається питання щодо ізолювання засуджених терористів від інших в'язнів.

Зацікавленість викликає ще один напрямок боротьби з тероризмом, який з'явився у США з огляду на особливості терористичної атаки у 2016 р. у м. Ніцца (Франція), де зловмисником використовувалась вантажівка. Передбачається, що у США до 2020 року до «Інтернету речей»[82] буде приєднано близько 250 млн. транспортних засобів, управління якими може здійснюватися через Інтернет. Це надає терористам можливість перехоплювати управління такими засобами та вчиняти терористичні атаки дистанційно, навіть не перетинаючи державний кордон. З огляду на таку потенційну загрозу в Міністерстві юстиції США розпочала функціонувати окрема група, що опікується виключно питаннями «Інтернету речей».

Сплеск масштабу нелегальної міграції до Європи у 2015 році фактично показав слабкість європейських інституцій, відповідальних за охорону зовнішніх кордонів та надання притулку біженцям: Агентства з охорони зовнішніх кордонів Євросоюзу (FRONTEX) та Бюро з питань надання притулку EASO (European Asylum Support Office), а також і прорахунки європейської політики контролю на кордонах. З огляду на це, Єврокомісія підготувала та у листопаді 2015 року оприлюднила у Брюсселі оновлену Європейську політику сусідства (Review of the European Neighbourhood Policy), якою встановлено нові рамки відносин ЄС із 16 країнами-сусідами на сході та півдні ЄС (включаючи Україну).

Вперше у такому форматі взаємодії ЄС із своїми сусідами з'явилися безпекові інструменти, серед яких – боротьба з нелегальною міграцією. У грудні

того ж року Європейська комісія оприлюднила плани щодо створення на основні FRONTEX нової прикордонної служби та берегової охорони на всіх зовнішніх кордонах ЄС, що допомагатиме сповільнити притік біженців з Близького Сходу та Африки до Європи.

На міжнародному та регіональному (європейському) рівнях відзначається тенденція до поглиблення співробітництва у сфері боротьби з тероризмом. У першу чергу, це стосується питань обміну інформацією, покращення взаємодії спецслужб та правоохоронних органів, посилення контролю за перетином державних кордонів та протидії фінансуванню терористичної діяльності.

На національному рівні держави вживають додаткових заходів, спрямованих на профілактику тероризму, вдосконалюють антитерористичне законодавство, розширюють повноваження силових структур, надаючи їм додаткові інструменти, прагнуть покращити взаємодію та обмін інформацією між уповноваженими органами, створюють нові координуючі органи по боротьбі з тероризмом, посилюють відповідальність за участь у терористичній діяльності.

Аналіз та оцінка діяльності спецслужб, правоохоронних та судових органів, їх недоліків та провалів має стати вагомим засобом у коригуванні державної політики у сфері боротьби з тероризмом. Такий аналіз має здійснюватися як на постійній основі уповноваженими координуючими і контролюючими органами (зокрема, РНБОУ, Об‘єднаним комітетом з питань розвідувальної діяльності, АТЦ при СБУ), так і у рамках Комплексного огляду сектору безпеки і оборони України.

Комплексний підхід до проблем протидії тероризму є одним з визначальних факторів успішного протистояння терористичній загрозі. Важливим напрямом антитерористичної діяльності є взаємодія і кооперація правоохоронних органів і спеціальних служб з науковими установами і дослідницькими центрами. Це сприятиме розвитку існуючих та впровадженню інноваційних методів, засобів і систем, що використовуються у протидії тероризму.

Важливе значення для України має посилення взаємодії з іншими країнами з питань протидії тероризму, налагодження обміну інформацією між

уповноваженими органами як на міжнародному, так і на національному рівнях. Проведення міжнародних антитерористичних навчань, цільових тренінгів сприятиме досягненню зазначеної мети. У цьому контексті нових можливостей для співробітництва надає створення спільної з НАТО Платформи з вивчення досвіду протидії гібридній війні в Україні, а також розвиток співробітництва з Центром передового досвіду НАТО з питань протидії тероризму (м. Анкара, Туреччина).

Таким чином, зрозуміло, що тероризм став центральним аспектом дискусії з питань безпеки. Це викликає низку питань, з одного боку, щодо можливого поєднання загроз (терористичні атаки на такі мережі, як енергетичні та використання таких постачальників енергії, як атомні електростанції, комп'ютери тощо).

По-друге, про форми антитерористичної співпраці. Різні підходи до проблеми призводять до різних підходів різних акторів, але зрозуміло, що політики, пов'язані з конкретною загрозою безпеці, є необхідним елементом стратегії безпеки в цілому.

РОЗДІЛ 3. УДОСКОНАЛЕННЯ МЕТОДІВ ПРОТИДІЇ ІНФОРМАЦІЙНОМУ ТЕРОРИЗМУ

3.1. Сучасний стан державно політики у сфері інформаційноїбезпеки в Україні

Процес глобалізації та екстенсивної комп'ютеризації суспільства справляє значний вплив на зміст і форму сучасної інформаційної війни. Це, у свою чергу, вимагає від системи національної безпеки своєчасної адаптації до нових викликів і загроз національним інтересам в інформаційній сфері [11, С. 192].

Складність сучасних загроз національній безпеці в інформаційній сфері потребує інноваційних способів створення та захисту інформаційного простору в умовах глобалізації та вільного потоку інформації.

В умовах всебічного інформування суспільства всі сфери суспільного життя все більше залежать від інформаційних факторів, а методи та інструменти ефективної реалізації державної політики інформаційної безпеки повинні постійно розвиватися. З метою захисту та реалізації національних інтересів державний контроль за процесами у національному, міжнародному та глобальному інформаційному просторі є нагальною необхідністю та неодмінною передумовою захисту країни та суспільства.

Це також можна пояснити тим, що міжнародні та світові політичні суб'єкти часто використовують для таких цілей інформаційні можливості та суперечать чи загрожують національним інтересам України (у тому числі таким об'єктам національної безпеки, як людина і громадянин, суспільство та держава).

У російсько-українському конфлікті пріоритетом стали захист національного інформаційного простору від негативних інформаційно-психологічних наслідків, дій і воєн, інформаційна безпека та інформаційний суверенітет, що було чинником збереження та реалізації національної ідентичності України.

Сучасна політика інформаційної безпеки в суспільних інтересах визначається приматом національних інтересів, системою загроз і небезпек і реалізується в інформаційній сфері відповідно до законодавства шляхом реалізації відповідних теорій, стратегій, концепцій і програм.

Інформаційна безпека є невід'ємною частиною національної безпеки та пріоритетом для країни. Інформаційна безпека забезпечує громадян вичерпною інформацією та вільним доступом до різноманітних джерел інформації, регулює поширення дезінформації, сприяє соціальній цілісності, захищає інформаційний суверенітет, веде боротьбу з негативною інформаційною та психологічною пропагандою, забезпечує національний інформаційний простір, попереджає маніпуляції, інформаційні війни та бойові дії [40].

Вирішення комплексної проблеми інформаційної безпеки сприятиме захисту інтересів суспільства та країни, а також права громадян на вичерпну, об’єктивну та якісну інформацію. Потребує перегляду і розвитку модель взаємовідносин правоохоронних органів і спеціальних служб України з населенням з питань запобігання і протидії тероризму. Активне залучення громадян і суспільства в цілому до боротьби з цим небезпечним явищем дозволить підвищити ефективність такої діяльності і рівень довіри населення до відповідних уповноважених органів.

Сутністю інформаційної безпеки є захищений стан інформаційного простору України, в якому не домінують спеціальні інформаційні операції, акти зовнішніх інформаційних атак, інформаційний тероризм, привласнення інформації спеціальними технічними засобами, кіберзлочинність та інші руйнівні інформаційні наслідки що можуть завдати серйозної шкоди національним інтересам [43, с. 14].

Тому пріоритетними напрямами сучасної державної політики щодо забезпечення інформаційної безпеки України є:

1) забезпечення інформаційного суверенітету України, створення стандартизованих правових та економічних умов для розвитку інформаційної інфраструктури та ресурсів, впровадження нових технологій у цій сфері,

створення єдиного закону, економічні передумови для впровадження інформаційної інфраструктури та ресурсів, необхідних для впровадження нових технологій у цій сфері, з метою наповнення національного та світового інформаційного простору достовірною інформацією про Україну;

2) активна участь ЗМІ у запобіганні та протидії корупції, зловживанню службовим становищем та іншим явищам, що загрожують національній безпеці України;

3) забезпечення суворого дотримання конституційних прав на свободу вираження поглядів, доступ до інформації, захист персональних даних, недопущення незаконного втручання органів державної влади, органів місцевого самоврядування, їх представників у ЗМІ та журналістів, заборона цензури, дискримінації у професійній сфері, політичних утисків, та критики претензій;

4) вживання комплексних заходів щодо захисту національного інформаційного простору та монополізації інформаційної сфери України.

Враховуючи процес інтеграції України в міжнародну систему інформаційної безпеки, стоїть завдання розробити національну політику інформаційної безпеки як регіональний кластер просторової безпеки комплексної системи міжнародної безпеки, безумовно, з урахуванням відповідних національних інтересів (інформаційне запобігання).

Забезпечення інформаційної безпеки України є спільною турботою української держави та народу, що є одним із напрямків сучасних глобальних та регіональних інформаційних конфліктів крізь призму громадського порядку в Україні. Захист національного інформаційного простору від зловмисників та забезпечення інформаційної безпеки будуть пріоритетними.

Законодавство України має надавати належну інформацію про рішення органів влади, громадян та об’єднань громадян та інших юридичних осіб в Україні, які гарантують свободу інформації та доступ до інформації.

У Доктрині інформаційної безпеки України визначено, що до національних інтересів України в інформаційній сфері віднесено такі життєво-важливі інтереси особи, як:

- забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації;
- забезпечення конституційних прав людини на захист приватного життя;
- захищеність від руйнівних інформаційно-психологічних впливів.

Проте, цей документ являє собою сукупність теоретичних понять про цілі, принципи та правові складові інформаційної безпеки.

Відтак, з нього не зрозуміло чітких завдань та відповідальних суб'єктів за інформаційну безпеку, оскільки він є лише основою для розроблення проектів, концепцій, стратегій, цільових програм і планів дій із забезпечення інформаційної безпеки України. Протягом останніх років значно зросла необхідність в комплексному та ефективному підході до процесу забезпечення безпеки національного інформаційного простору, і це проглядається у нормативних документах зарубіжних країн.

Для захисту українського національного інформаційного простору має відбуватися повний розвиток інформаційної структури, підтримка використання науково-технічних досягнень українського народу та особливостей інтелектуального та культурного життя України, розвиток національних інформаційних ресурсів, створення та впровадження безпечних інформаційних технологій.

Передумовами укріплення національної інформаційної безпеки є національна власність на стратегічні об'єкти, охорона державної таємниці та обмежений доступ до певних об'єктів, що перебувають у власності чи користуванні держави; Створення загальної системи захисту інформації, зокрема захисту державної таємниці та іншої інформації з обмеженим доступом; захист національного інформаційного простору України від спотворення або поширення забороненої законодавством України інформаційної продукції; Прийняття законів, що визначають систему доступу іноземних держав або їх представників до національних інформаційних ресурсів України та порядок використання цих ресурсів відповідно до договорів, укладених з іноземними державами [54].

Слід підкреслити, що сучасні виклики щодо інформаційної безпеки в Україні пов’язані як з внутрішніми, так і з зовнішніми чинниками: внутрішніми – переважно в Україні, відсталістю інформаційних технологій світового лідера, низькою поінформованістю, роздробленістю державної влади, інформаційним законодавством. Тенденції створення та застосування інформаційних технологій, спроби зарубіжних акторів впливати на світовий та вітчизняний інформаційний простір.

Знижена увага до проблем інформаційної безпеки України також є умовою для спроб сепаратизму, насильства, антиукраїнських впливів, які пропагують ідеали національної ворожнечі, руйнування національної ідентичності України та порушення конституційного ладу України. Україна довго не могла вийти з замороженого конфлікту у Східній війні, оскільки Російська Федерація розширювала сферу пропагандистського впливу активно використовуючи психологічні операції.

Російська пропаганда своїми інформаційно-психологічними кампаніями, акціями та медійними заходами впливає не лише на суспільну свідомість громадян України, а й на світову спільноту. Наразі, після початку Повномасштабної війни з РФ, поновлюється домінування української (і світової) інформації та медіаконтенту.

Ще у 2015 році речник Асоціації «Інформаційний спротив» В. Гусаров заявив, що Росія проводить інформаційно-психологічні атаки з метою ескалації конфлікту на сході України та тисне на українське керівництво з метою посилення «московського» опору.

В. Гусаров виділяє напрямки інформаційно-психологічних атак на Україну:

- нав'язування думок про неспроможність влади управляти та раціоналізувати державу;
- негативні судження та хаотичні дії проти військово-політичного керівництва України призводять до невиправданих втрат;
- поширення недовіри до української армії на сході України та їх недовіри до керівництва спецпідрозділів;

- Хибна інформація про те, що Україна не буде позбавлена російського газу, і сторони повинні повернутися, щоб переглянути свої газові контракти. Експерт зазначає, що сьогодні цільовою аудиторією Кремля є російське населення, російськомовна діаспора, яка проживає за кордоном, населення України, включаючи окупований Донбас, громадяни Заходу, країни БРІКС і Митного союзу, а також політичні сусіди Росії. Україна стала суб'єктом інформаційно-психологічних впливів, дій і воєн, на кону інформаційна безпека.

Слід уточнити, що український інформаційний простір не зазнав впливу зовнішньої негативної пропаганди та маніпуляцій, а став предметом поширення інформації. У світовому медіапросторі немає українського національного інформаційного продукту, який поширюється об’єктивно, справедливо та ефективно - актуальна інформація про події в Україні. В результаті міжнародне співтовариство не володіє інформацією або отримує інформацію з інших джерел, яка іноді вводить в оману, транслює викривлену та неповну картину.

На жаль, національний інформаційний простір України стоїть перед серйозними викликами з боку держави, політичного та економічного розвитку, євроінтеграції та євроатлантичних структур.

На цьому етапі Україні необхідно зосередитися на двох основних напрямках: модернізації внутрішніх справ України, безпеці, структурній цілісності та конкурентоспроможності, забезпеченні інформаційної присутності країни у світі та сприянні її позитивному іміджу.

Інформаційна безпека має базуватися на моделі стратегічного мислення: принципах демократії, прав людини та безпечного Інтернету. Необхідно вжити заходів для захисту, підтримки цілей та забезпечення безпеки. При цьому інформаційна безпека є невід’ємною складовою розвитку інформаційного суспільства. Розвиток інформаційного суспільства має бути досягнутий не лише через вдосконалення технічних можливостей для обміну інформацією, а й через глибоке розуміння різних учасників інформаційного суспільства. Тому актуальні теми інформаційної безпеки включають такі теми, як інформаційна етика,

конфіденційність в інформаційному суспільстві та запобігання наслідкам маніпулювання інформацією.

Зараз майже всі сфери суспільного життя знаходяться під безпосереднім впливом суб'єктів інформаційної політики всіх рівнів. Ефективний вплив потоку інформації на життєво важливі інтереси особи, суспільства та країни залежить від ефективного управління інформаційним полем держави, стану та динаміки практично всіх якісних показників державного управління.

Сьогодні у Верховній Раді діють чотири комітети, які займаються питаннями свободи слова, регулювання ЗМІ, інформаційної політики та інших сфер, пов'язаних із ЗМІ. До них належать Комітет з гуманітарних питань та інформаційної політики; Комітет зі свободи вираження поглядів; Комітет цифрової трансформації; Комісія з прав людини, окупації та переселення в Донецькій, Луганській та Севастопольській області Автономної Республіки Крим [48].

Міністерство культури та інформаційної політики України є головним органом центральної системи органів виконавчої влади у сфері національного мовлення та інформаційного суверенітету України (керує всім комплексом Державного інформаційного агентства України «Укрінформ»), інформаційної безпеки та поширення публічної інформації в Україні та за кордоном.

Іншим органом виконавчої влади є Міністерство цифрової трансформації України, до складу якого входять Національне агентство з питань електронного урядування та Міністерство освіти. Агентство співпрацює з іншими державними установами, муніципалітетами та міжнародними партнерами, щоб забезпечити сумісність – принцип, згідно з яким різні джерела інформації можуть взаємодіяти через спільні угоди.

Результати роботи Міністерства цифрової трансформації можна вважати ефективною базовою платформою для розгортання телекомунікаційних компонентів для забезпечення ефективного розвитку інформаційної безпеки в Україні. Звичайно, РНБО як компетентний державний орган має координуючу роль.

Іншими словами, якщо глобалізація встановлює правила на світовій арені через соціальну цифровізацію, чому б не використати інформаційну безпеку українського суспільства, створюючи сучасний національний простір і не побудувати технічні складові українського суспільства?

Таким чином, діяльність із інформаційної безпеки видається інтегрованою в сучасну цифрову трансформацію через свої завдання.

Крім того, Національне агентство з питань комунікації та захисту інформації має бути обрано окремо від працівників ЗМІ.

Національний програмний комітет телебачення і радіомовлення також відіграє роль у системі органів виконавчої влади. Держкомтелерадіо є головним органом центральної виконавчої влади, що формує та реалізує державну політику у сфері телебачення і радіомовлення, інформації та видань.

До органів зі спеціальним статусом у сфері ЗМІ належить Національна рада з питань телебачення і радіомовлення [51], регулюючи закони з мовних питань, питань пов'язаних із захистом суспільної моралі, тощо. Як регулятор, цей орган може застосовувати санкції за порушення в межах своєї компетенції.

Іншою установою є Рада національної безпеки і оборони України [61], яку очолює Президент України. Відповідно до Конституції України та Закону про Раду національної безпеки і оборони України до складу Координаційного органу входять керівники профільних міністерств та інші посадові особи. До компетенції Управління входить можливість діяльності у сфері інформації, у тому числі потенційних та реальних загроз національним інтересам (за даними Комітету з питань національної безпеки і оборони).

До інституцій зі спеціальним статусом належать дві установи під головуванням Президента України – Комітет з питань свободи слова та захисту журналістів [60] та Державний комітет зв'язку та інформатизації [57].

Тому певна система влади визначає та аналізує загрози інформаційній безпеці в Україні, розробляє та впроваджує заходи, необхідні для реагування на них в країні. Проте в сучасних умовах ефективно протистояти інформаційним загрозам може лише добре організована система громадської безпеки, яка має

здійснюватися за повної взаємодії всіх органів влади, громадських організацій та громадян [17]. Системні визначення та поняття, що з'являються в законодавстві, та твердження, що базуються на них, свідчать про те, що інформаційна безпека є одним із пріоритетів сучасної внутрішньої політики в Україні.

Підсумовуючи аналіз ситуації з інформаційною безпекою в Україні, слід зазначити, що національний інформаційний простір України становить серйозну загрозу для діяльності, політичного та економічного розвитку країни, європейської інтеграції та інтеграції в євроатлантичні структури. Для ефективної політики публічної інформаційної безпеки держава має активно брати участь у регулюванні інформаційних продуктів, що розповсюджуються за допомогою телекомунікацій, а пріоритетом громадського порядку у забезпеченні внутрішньої інформаційної безпеки має бути відповідна розробка інформаційного законодавства. Участь громадськості та ЗМІ покращать якість інформації, але немає механізму безпеки для запобігання, стримування та боротьби зі злочинністю.

3.2. Основні напрями вдосконалення системи забезпечення інформаційної безпеки в контексті протидії інформаційному тероризму

Слід зазначити, що зі стрімким поширенням макроекономічної глобалізації потенційний вплив інформації на окремих людей, суспільство та країни зростає. Безперервне широкомасштабне поширення інформації допомагає її розповсюдженню на великі території за дуже короткий час. Хоча це і вважається головним досягненням людства, воно має свої негативні сторони, оскільки глобалізація інформатизації посилила потенціал інформаційних загроз. Інформаційна ера розширила сферу інформаційно-комунікаційної війни, об’єднавши інформаційний тероризм як засіб інформаційної війни, основу фізичного тероризму з інформаційними системами та навмисне неправомірне використання кіберпростору, мереж або компонентів для сприяння терористичним операціям [4].

Існують докази того, що з посиленням пропаганди та сепаратистських рухів інформаційний тероризм набув нової форми загрози, яка в кінцевому підсумку може призвести до втрати національного суверенітету, незалежності та територіальної цілісності.

На думку експертів НАТО, «гібридна операція» є цілеспрямованою, скоординованою за місцем і часом і має на меті досягнення необхідного впливу на країну без прямого і явного застосування сили [28].

В українському науковому середовищі немає базисної узагальнюючої роботи, яка б значно покращила вирішення практичних завдань у сфері інформаційної політики при розробці та реалізації державної політики.

У боротьбі з інформаційним тероризмом взаємодія між владою, ЗМІ та суспільством не є конструктивною, що проявляється в хаотичних, неузгоджених і неактуальних діях.

Тому слід зазначити, що складно сформулювати єдині превентивні, та специфічні кримінально-правові, адміністративно-організаційні, економічні, та технічні заходи щодо боротьби з інформаційним тероризмом.

Комплексний механізм боротьби з інформаційним тероризмом має включати інституційні, правові та методичні ресурси. Тобто, враховуючи цей механізм, нам необхідно чітко визначити сферу діяльності так званої структури-учасниці (або організації, яка займається протидією інформаційному тероризму) та забезпечити чітко визначену нормативну базу її діяльності (включаючи нормативну координацію) ресурсів (людські ресурси, фінансові ресурси, матеріали тощо) і чітко визначати процес його діяльності (активація механізму, взаємодія один з іншими елементами тощо).

Законодавство щодо інформаційної безпеки розподіляється між уповноваженими організаціями для забезпечення виконання завдань у цій сфері в межах їх повноважень. Незважаючи на реакцію українських законодавців на сучасні інформаційні виклики, прикро, що законодавча база не отримала змістовного базису для активних заходів боротьби з інформаційним тероризмом.

Враховуючи координуючу роль головного органу МВС України в боротьбі з інформаційним тероризмом, нове законодавство неминуче призведе до вироблення цілісного, комплексного підходу до всіх складових внутрішнього антитерористичного механізму.

Тому розвиток існуючої структури української антитерористичної системи в боротьбі з інформаційним тероризмом є окремим важливим напрямом. Без шкоди для створеної та існуючої структури Національного антитерористичного механізму, його реформування відіграватиме ключову роль у складному механізмі протидії інформаційному тероризму в Україні, тобто серед суб'єктів боротьби з інформаційним тероризмом.

Цей метод також дає змогу національному механізму боротьби з тероризмом досягти належного та ефективного поточного рівня управління – як частина національного антитерористичного механізму, він відповідає за координацію повсякденних операцій та обробку контртерористичної інформації. Здатність діяти, розвивати та захищати національних лідерів високого рівня є доцільною для боротьби з інформаційним тероризмом. Крім того, антитерористичні операції з розвідкою можуть проводитися і як окрема операція, так і в складі більш складної та широкомасштабної антитерористичної операції [36].

Тому структура штабу Контртерористичного центру Служби безпеки України потребує модернізації, щоб більш якісно виконувати свою роль у боротьбі з інформаційним тероризмом. Як виконавчий орган, штаб здійснює поточну організаційну роботу, виконує завдання технічного управління і відповідно визначає завдання апарату. Також варто відзначити роль Штабу в організації науково-методичної роботи з розробки форм і методів боротьби з тероризмом. Тому запровадження сучасного, ефективного та необхідного сучасного національного антитерористичного механізму потребуватиме оптимізації структури управління.

Ці підрозділи, співпрацюючи з головним органом протидії інформаційному тероризму, іншими державними органами, засобами масової інформації,

громадськими та приватними особами, створюють та забезпечують організаційно-правову базу для забезпечення та функціонування громадського порядку.

Необхідно розвивати роль і позицію організацій, що займаються боротьбою з інформаційним тероризмом, у всій національній системі: по-перше – це потреба в специфічній правовій базі; по-друге — спільна організація та здійснення практичних заходів щодо боротьби з інформаційним тероризмом.

Наступною бажаною ціллю Центру запобігання інформаційному тероризму Служби безпеки України має бути узагальнення, реорганізація та вдосконалення вітчизняного законодавства щодо боротьби з інформаційним тероризмом.

Необхідно визнати той факт, що на сьогоднішній день в Україні не існує дієвого та практичного законодавства щодо боротьби з інформаційним тероризмом. Через призму психології інформаційного тероризму та складових інформаційних технологій аналіз перших кількох етапів чинного законодавства виявляє досить насичену, але неструктуровану «картину процесу реагування на інформаційні загрози». Новостворений Центр має закріпити на законодавчому рівні поняття інформаційного тероризму, модернізувати діюче законодавство та забезпечити правову базу Національного механізму боротьби з інформаційним тероризмом.

До цієї роботи мають бути залучені фахівці з боротьби з тероризмом та експерти з науковим потенціалом. Крім того, дослідження, проведені вітчизняними та зарубіжними школами, показують великий дослідницький потенціал у сфері інформаційної безпеки. Одним словом, механізм розробки та реалізації національної політики щодо боротьби з інформаційним тероризмом українськими вченими не враховано повністю та не охоплено розвитком інформаційної безпеки в Україні та боротьбою з тероризмом загалом.

Тому в науковому середовищі практично відсутня узагальнююча робота, яка б суттєво посилила вирішення практичних завдань у розробці та реалізації національної політики у боротьбі з інформаційним тероризмом.

Для пояснення змісту модернізації управління національним механізмом боротьби з інформаційним тероризмом, перш за все, необхідно зрозуміти його

природу та завдання. Підсумовуючи, зрозуміло, що національний лідер (Президент України) має бути якнайшвидше інформований про загрози національній безпеці, у тому числі тероризм, для швидкого прийняття керівних рішень. Тому для реалізації місії мають бути досягнуті такі аспекти: ефективність інформаційного потоку; цілісність обробки інформації; своєчасне реагування на зміни та отримання додаткової інформації; інформація оцінюється максимально комплексно; ефективні управлінські рішення приймаються на сучасному рівні та доводяться до підлеглих; контроль за чітким виконанням управлінських рішень; вживати заходів щодо координації підпорядкованих сил [83].

Цифрова трансформація покращить здатність антитерористичних суб'єктів зосереджуватись та вживати необхідних заходів (наприклад, шляхом усунення неправдивої та спотвореної інформації чи реагування шляхом надання точної та об'єктивної інформації громадськості). Тому ефективна платформа для автоматизації аналізу телекомунікаційної інформації може бути використана як технічний компонент системи управління антитерористичною інформацією.

Це відповідає Указу Президента України № 379/99 про Антитерористичний центр та його координаційні групи при регіональних органах Служби безпеки України, який уповноважує АТЦ створювати та експлуатувати загальну автоматизовану інформаційну систему [84].

Звісно, необхідно розробити технічну складову, яка включатиме систему управління інформацією, тобто платформу для інформаційного аналізу організацій, що займаються боротьбою з інформаційним тероризмом та автоматизацією телекомунікацій. Платформа передбачена у вигляді так званого технічного інструменту адміністративного підрозділу Національного інформаційно-контртерористичного механізму, від якого певною мірою залежить ефективність управлінських рішень національного керівництва у боротьбі з тероризмом в Україні.

Крім того, оскільки зрозуміла логіка побудови складової технології управління, зрозуміло, що вона буде інтегрована в систему ситуаційних центрів, які керуються Головним ситуаційним центром України [65, с. 72]. Паралельно

механізм координації та управління боротьбою з інформаційним тероризмом буде реалізований у більш глобалізованій системі, тобто головному центрі України, як комплекс програмно-технічних засобів для збору та обробки інформації.

З організаційної точки зору створення штабу АТЦ як окремого підрозділу у співпраці з головним органом боротьби з інформаційним тероризмом та іншими національними установами створює ІТ-платформу для вищезгаданого національного антитерористичного механізму. Представники груп та громадян забезпечують ефективне функціонування організаційно-правової бази національного механізму боротьби з інформаційним тероризмом, а координацію діяльності головного органу з боротьби з інформаційним тероризмом здійснює його загальна система. Крім того, можливим стане вироблення скоординованих інформаційно-аналітичних матеріалів, передбачення терористичних криз та ухвалення рішень для швидкого прийняття керівництвом.

Крім того, в контексті розбудови демократичного суспільства в Україні та процесу європейської інтеграції цей метод посилює реалізацію адміністративної політики та піднімає на більш ефективний рівень ще одну функцію АТЦ: належну комунікацію із ЗМІ та громадськістю, участь і співпраця у профілактичних заходах, боротьба з тероризмом та підготовка населення у разі загрози чи терористичного нападу, а також співпраця у запобіганні тероризму.

У контексті реформування антитерористичної системи України буде враховано інформаційно-технологічну складову України (як ресурсну складову інформаційного антитерористичного механізму). Акцент слід також зробити на розвитку аналітичної складової прийняття управлінських рішень з метою висвітлення процесу боротьби з інформаційним тероризмом. Додатковою особливістю стане введення відповідного нового підрозділу.

Міжвідомчий координаційний комітет при АТЦ здійснює такі види діяльності: організація правової оцінки діяльності, своєчасне виявлення рівня терористичної загрози та вироблення рекомендацій у країні (або в окремих регіонах); надання вищому керівництву країни необхідних рішень щодо боротьби з інформаційним тероризмом; здійснення низки запобіжних заходів щодо

підготовки сил і засобів осіб, які беруть участь у боротьбі з інформаційним тероризмом; рішення про підготовку до проведення антитерористичної інформаційної операції (в одній із трьох ситуацій, зазначених вище). У разі потреби підрозділ рекомендує запровадити відповідний рівень підготовки організацій, які безпосередньо займаються боротьбою з тероризмом.

Міжнародно-правове дослідження показало, що навіть на цьому рівні не існує комплексного документа щодо боротьби з інформаційним тероризмом, який би конкретно торкався запобігання та використання телекомунікаційних технологій терористами.

Існує потреба у створенні та запровадженні єдиної правової бази на міжнародному рівні (так зване типове законодавство), яке відігравало б керівну та важливу роль у поєднанні до існуючого законодавства без створення правових зобов'язань. Після терористичних атак європейські країни працюють над модернізацією свого антитерористичного законодавства, включаючи норми щодо механізмів боротьби з тероризмом (збір даних, відеоспостереження, прослуховування телефонних розмов, запис та передача даних про неповнолітніх тощо).

Підсумовуючи, інформаційну безпеку в Україні маємо розглядати як систему з чотирьох складових компонентів: правового, технічного, комунікаційного та освітнього.

Перш за все, правовий компонент повинен встановити норми та гарантувати юридичні механізми системи інформаційної безпеки в державі, забезпечувати відповідний механізм реагування та покарання будь-яких посягань на інформаційну безпеку.

Другий компонент – технічний, має забезпечити інженерно-технічними заходами конфіденційність, цілісність та доступність інформації;

Третій – комунікаційний компонент відповідальний за забезпечення системи моніторингу та формування контенту у соціальних мережах;

І останній, четвертий – освітній компонент охоплює інтегроване систематичне навчання інформаційній безпеці у закладах освіти, а також

підвищення кваліфікації для працівників органів державної влади та місцевого самоврядування, які працюють з інформацією.

Для посилення інформаційної безпеки України передбачаємо відповідні покрокові дії:

1) Виявлення специфічних сегментів, що вимагають реформування у сфері інформаційної безпеки. Наприклад, провести комплексні аудити (правовий, технічний, комунікаційний та освітній) у сфері інформаційної безпеки у державних органах із залученням зацікавлених суб'єктів.

2) Базуючись на виявлених вразливостях із фахівцями у сфері інформаційної безпеки сформувати національну стратегію інформаційної безпеки та реалістичний план її виконання.

3) Започаткування власне реалізації реформи.

ВИСНОВКИ

Передумовою виникнення інформаційного тероризму був міжнародний розвиток інформаційного суспільства, прості методи та технології реалізації, ефективність, секретність та безкарність такого роду злочинів. Інформаційний тероризм поділяється на інформаційно-психологічний тероризм та інформаційно-технологічний тероризм.

Серед проявів такого роду тероризму найпоширеніші: контролювання засобів масової інформації і поширення ними неправдивої інформації, чуток, демонстрація сили терористичних організацій, пошкодження окремих елементів і всього інформаційного середовища противника: знищення елементних баз, активне придушення ліній зв'язку, штучне розрядження вузлів зв'язку тощо.

Проаналізовано комплексний виклад проблем державної безпеки у протидії терористичним загрозам в інформаційній сфері в рамках державної політики на основі системного аналізу теоретико-методологічних підходів вітчизняної політології, політичної соціології та конфліктології.

Інформаційний тероризм, що є предметом цього дослідження, займає особливе місце серед форм тероризму за двома критеріями - простором реалізації (інакше середовище) та засобами (інструментами), які використовуються терористами та терористичними організаціями (спільнотами).

Вважаємо необхідним проведення активної роботи над адаптацією досвіду європейських спецслужб у боротьбі з інформаційним тероризмом до внутрішніх проблем України у цій сфері, зокрема до пропаганди російських спецслужб та формування хибної громадської думки щодо ситуації на Сході України. Питання взаємодії з громадськими організаціями, які виступають важливими лідерами та елементом зв'язку між державою та її громадянами у боротьбі з тероризмом, у тому числі інформаційним, потребує більшої уваги. На нашу думку, така форма взаємодії державних організацій з профільними спецслужбами є дуже важливою сьогодні для України у питанні вироблення державної політики боротьби з інформаційним тероризмом, особливо щодо проявів конфлікту з РФ.

Організаційно-правовий механізм боротьби з інформаційним тероризмом має бути конструктивно розроблений для компетентної державної установи – Контртерористичного центру СБУ.

Просуваючись вперед у реформуванні системи інформаційної безпеки України, необхідний сталий розвиток Національного механізму інформаційного тероризму, як невід'ємної частини апарату державної безпеки, що координуватиме повсякденні оперативні завдання та виклики інформаційного тероризму. Потребує перегляду і розвитку модель взаємовідносин правоохоронних органів і спеціальних служб України з населенням з питань запобігання і протидії тероризму. Активне залучення громадян і суспільства в цілому до боротьби з цим небезпечним явищем дозволить підвищити ефективність такої діяльності і рівень довіри населення до відповідних уповноважених органів.

На міжнародному рівні, у стані активного збройного конфлікту, як держава, що бореться зі «змішаним» інформаційним протистоянням, необхідно розпочати єдиний законодавчий процес у боротьбі з інформаційним тероризмом.

Дослідження розкриває конкретику реалізації інформаційної антитерористичної політики в контексті сучасних глобальних викликів і загроз, показавши, що головною метою системи антитерористичної протидії України є забезпечення безпеки людей, суспільства та країни від тероризму. Сучасна модель глобалізації дає змогу поширювати міжнародний тероризм та міжнародну злочинність. У світовій геополітичній системі, що сформувалася в процесі глобалізації, міжнародний тероризм відіграє ключову роль з початку XXI століття і являє собою глобальну руйнівну силу, яка загрожує самим основам людської цивілізації.

СПИСОК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. Київ, 2019. URL: http://academy.ssu.gov.ua/uploads/p_57_53218641.pdf (дата звернення: 12.04.2022)
2. Армія FM Військове радіо: веб сайт. URL: http://mediasat.info/2016/03/16/armiya-fm-vijskove-radio (дата звернення: 07.04.2022)
3. Баланда А.Л. Соціальні детермінанти національної безпеки України: Монографія. Київ, 2008. 414 с.
4. Банк Р.О. Інформаційний тероризм як загроза національній безпеці України: теоретико-правовий аспект, 2016. 110-116 с.
5. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: термінологічний навчальний довідник. Київ, 2004. 68 с.
6. Бойченко О. В. Кібертероризм у складі сучасних проблем національної безпеки. Київ, 2010. 57–62 с.
7. Бойченко О. В. Медіа-тероризм: особливості сучасних ознак інформаційній безпеці: Друга міжнародна наук.-практ. конф..). НАУ, 2009. 230–232 с.
8. Бочарніков І. В. Інформаційна протидія тероризму в сучасних умовах / Електронний науковий журнал Проблеми безпеки, 2013 № 3 (21).
9. Варенья Н. М. Щодо методів виявлення небезпек та загроз терористичного характеру. Верховенство права у процесі державотворення та захисту прав людини в Україні: тези міжнародної наук.-практ. конф. Одеса, 2016. 104-108 с.
10. Герасименко К.С. Сучасні ознаки загроз «інформаційного тероризму». Київ, 2009. 162–166 с.
11. Глазов О. В. Міжнародний інформаційний тероризм в контексті загроз національній безпеці України / О. В. Глазов URL: http://lib.chdu.edu.ua/ pdf/naukpraci/politics/2012/197-185-15.pdf. (дата звернення: 18.04.2022)

12. Горбань Ю.О. Інформаційна війна проти України та засоби її ведення. URL:http://www.visnyk.academy.gov.ua/wpcontent/uploads/2015/04/20.pdf (дата звернення: 20.04.2022)

13. Гусаров В. Кремль розпочав нову інформаційну операцію проти України. URL: http://www.osvita.mediasapiens.ua/material/34281.

14. Діордіці І. В. Кібертероризм як елемент дестабілізації системи стратегічних комунікацій / І. В. Діордіці. – 2016. – URL: https://goalint.org/kiberterorizm-yak-elementi-destabilizacii-sistemi-strategichnixkomunikacij/ (дата звернення: 21.04.2022)

15. Дмитренко М.А. Спеціальні заходи впливу як механізм протистояння зовнішньополітичним впливам в інформаційних війнах. Збірник наукових праць Інституту Служби зовнішньої розвідки України. 2016. №12. С. 21-37.

16. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25.02.2017 р. № 47/2017 URL: http://president.gov.ua (дата звернення: 11.04.2022)

17. Дослідження медіа-ситуації в південних і східних областях України 2017. - Інститут масової інформації. URL: https://imi.org.ua/monitorings/doslidzhennya-media-sytuatsiji-v-pivdennyh-ishidnyh-oblastyahukrajiny2017. (дата звернення: 12.04.2022)

18. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія / Д. В. Дубов. – К. НІСД, 2014. – С. 36. 91

19. Жайворонок О. І. Організаційно-правові засади формування та реалізації публічної політики протидії інформаційному тероризму в Україні : дис. докт. філос. наук : 281 / Жайворонок О. І. – Київ, 2021. – 251 с.

20. Задорожній О. В. Анексія Криму – міжнародний злочин : моногр. / О. В. Задорожній. – Київ : К.І.С., 2015. – 576 с.

21. Іванова О.О. Information terrorism: general information and ways of prevention // Міжнародна науково-практична конференція здобувачів вищої освіти і молодих учених «Політ. Сучасні проблеми науки» – 2021 р., м. Київ, 5–9 квітня

2021 р. Київ, 2021. С. 44–46. URL: http://fmv.nau.edu.ua/політ2021/ (дата звернення: 14.04.2022).

22. Інформаційний простір – 2019. – URL: https://uk.wikipedia.org/wiki/Інформаційний_простір (дата звернення: 21.04.2022)

23. Інформаційно-аналітичне забезпечення як вид інформаційного забезпечення в системі державного управління / Ю.О. Саричев // Вісник НАДУ при Президентові України [за заг. ред. Ю.В. Ковбасюка]. – 2017. – № 3 (86)

24. Кібербезпека в інформаційному суспільстві: Інформаційноаналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Науководослідний інститут інформатики і права НАПрН України; Національна бібліотека України ім. В.І.Вернадського. – К.: Видавничий дім «АртЕк», 2018. №1-12.

25. Клименко С. Теорія и практика ведення «гібридних воєн» (за поглядами НАТО). Зарубіжний воєнний огляд. / Вип. 5, 2015. С. 109-110.

26. Козюра В.Д. Як протистояти реальним кіберзагрозам об'єктам критичної інфраструктури України / В.Д.Козюра. URL: http://dspace.oduvs.edu.ua/bitstream/123456789/501/1/ilovepdf_com-79-80%5B1%5D.pdf (дата звернення: 28.04.2022)

27. Комп'ютерна злочинність і інформаційна безпека / А.П.Леонов; під заг. ред. А. П. Леонова. – Мінськ: АРІЛ, 2000. – 552 с. 92

28. Комп'ютерний тероризм : практика запобігання, протидії, розслідування : навч. посіб. / П. Д. Біленчук, В. В. Кравчук, О. В. Кравчук, В. М. Кулик ; М-во освіти і науки України, Хмельниц. держ. центр наук.-техн. і екон. інформації, Київ. нац. ун-т внутр. справ. − Хмельницький, 2008. − 258 с. : іл. − Бібліогр: с. 243−252 (164 назви). − ISBN 978-966-7872-54-0.

29. Конституція України // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141

30. Конституція України від 28.06.1996 № 254к/96-ВР // Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141.

31. Корченко О. Г., Бурячок В. Л., С. О. Гнатюк. Кібернетична безпека держави: характерні ознаки та проблемні аспекти. Безпека інформації. 2013. Т. 19. № 1. С. 40–45

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

33. Коршунов В.О. Політичний тероризм: інформаційні методи боротьби: автореф. дис. канд. політ. наук: спец. 23.00.02. Дніпропетровськ, 2008. 18 с.

34. Костіхін А. А. Інтернет як інструмент терористичних та екстремістських організацій у психологічній війні URL: http://www.iimes.ru/?p=4737 (дата звернення: 16.04.2022)

35. Кубишкін О. В. Міжнародно-правові проблеми забезпечення інформаційної безпеки держави URL: http://pravolib.pp.ua/mejdunarodnopravovyie-problemyi obespecheniya.html/ (дата звернення: 01.05.2022)

36. Кунєв Ю.Д. Правове забезпечення інформаційної безпеки як предмет правового дослідження. Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право». Київ: НАУ, 2021. № 1 (58). С. 95-102. URL: https://doi.org/10.18372/2307- 9061.58.15314 93 (дата звернення: 02.05.2022)

37. Логвінець В. Епоха інформаційно-психологічних операцій: Лівія. URL: http://psyfactor.org/psyops/psyops5.htm (дата звернення: 03.05.2022)

38. Лужецький В.А. Інформаційна безпека: навч. посіб. / В.А.Лужецький, О.П.Войнович, А.В.Дудатьєв. – Вінниця : УНІВЕРСУМВінниця, 2009. – 240 с.

39. Майоров В.В. Розмежування терористської та екстремістської діяльності. URL: http://goal-int.org/rozmezhuvannya-teroristskoi-taekstremistskoi-diyalnosti (дата звернення: 01.05.2022)

40. Макаров В. М. Консциентальна війна: міф чи реальність? Наука і військова безпека. 2003, №2. С. 18-22.

41. Малик Я. Інформаційна безпека України: стан та перспективи розвитку. Ефективність державного управління. Збірник наукових праць. 2015. Вип. 44. С. 13-20.

42. Марущак А. І. Проблеми розслідування кіберзлочинів в Україні. Економіка. Фінанси. Право. 2018. № 1. С. 23-27.

43. Матула М. М. Феномен інформаційного тероризму як загрози національній та міжнародній безпеці / М. М. Матула // Науковий блог НАУ „Острозька Академія URL: http://naub.oa.edu.ua/2014/fenomen-informatsijnohoteroryzmu-yakzahrozy-natsionalnij-ta-mizhnarodnij-bezpetsi/ (дата звернення: 05.05.2022)

44. Методи інформаційного захисту простору. Інформаційна безпека України. URL: http://www.uatextreferat.com/referat-7471.html. (дата звернення: 02.04.2022)

45. Методика формування переговорного досьє в системі Служби безпеки України: практ. посіб. [для курсантів, слухачів НА СБ України] / І.В. Авдошин. – К. : Нац. акад.. СБУ, 2015. – 242 с

46. Методики аналізу, розробки та прийняття рішень в публічному управлінні щодо протидії інформаційному тероризму : публічне управління та публічна служба в Україні: стан проблем та перспективи розвитку /матеріали науково-практичної конференції за міжнародною участю (07-08 вересня 2018 р., м. Київ)] ; за заг. ред. В.С. Куйбіди, М.М. Білинської, В.Л. Федоренка. Київ : Видавництво Ліра-К, 2018. С. 170-176 94

47. Моїсеєв А. І. Проблема міжнародного інформаційного обміну у боротьбі з тероризмом / А. І. Моїсеєв. // Актуальні проблеми російського права. - 2014. - №11. - С. 62-66.

48. Пилипчук В.Г., Брижко В.М., Баранов О.А. та ін. Становлення і розвиток правових основ та системи захисту персональних даних в Україні : монографія / В.Г. Пилипчук, В.М. Брижко, О.А. Баранов, К.С. Мельник; за заг. ред. Брижка В.М., Пилипчука В.Г. – К. : ТОВ «Видавничий дім «АртЕк», 2017. – 226 с.

49. Про Доктрину інформаційної безпеки України Указ Президента України від 29 грудня 2016 року від 25.02.2017 № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 19.04.2022)

50. Про боротьбу з тероризмом: Закон України від 24.11.2021 р. № 25/ Верховна Рада України URL: https://zakon.rada.gov.ua/laws/show/638 (дата звернення: 03.05.2022)

51. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 № 3475-IV / Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/3475 (дата звернення: 28.03.2022)

52. Про затвердження Положення про Державний комітет телебачення і радіомовлення України: постанова Кабінету Міністрів України від 13 серпня 2014 р. № 341. URL: https://zakon.rada.gov.ua/laws/show/341

53. Про Концепцію боротьби з тероризмом в Україні: Указ Президента України від 05.03.2019 р. № 53/2019. URL: https://zakon.rada.gov.ua/laws/show/53/2019#Text (дата звернення: 25.03.2022)

54. Про Концепцію Національної програми інформатизації: Закон України від 04.02.1998 р. № 75/98-ВР / Відомості Верховної Ради України. 1998. № 27-28. Ст. 182.

55. Про Національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації: Указ Президента України від 23.11.2011 № 95 1067/2011/ Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/1067/2011#Text (дата звернення: 29.03.2022)

56. Про особливий порядок місцевого самоврядування в окремих районах Донецької та Луганської областей: Закон України від 16.09.2014 № 1680-VII / Відомості Верховної Ради (ВВР), 2014, № 45, ст. 2043.

57. Про Раду національної безпеки і оборони України від 05.03.1998 № 183/98-ВР/ Верховна Рада України. Законодавство України. URL:https://zakon.rada.gov.Ua/laws/show/183/98D0%B2%D1%80#Text (дата звернення: 21.03.2022)

58. Про Національну раду України з питань телебачення і радіомовлення від 23.09.1997 № 538/97-ВР // Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/538/97- %D0%B2%D1%80#Text. (дата звернення: 01.04.2022)

59. Про рішення Ради національної безпеки і оборони України від 25.01.2015 «Про створення та забезпечення діяльності Головного ситуаційного центру України» : Указ Президента України від 28.02.2015 № 115/2015. URL: http://www.president.gov.ua/documents/1152015-18567. (дата звернення: 10.04.2022)

60. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII / Відомості Верховної Ради (ВВР), 2017, № 45, ст.403, URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 11.04.2022)

61. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: указ Президента України від 26.05.2015 № 287/2015. // База даних Законодавство України / ВР України. URL: http://zakon5.rada.gov.ua/laws/show/287/2015 (дата звернення: 01.05.2022)

62. Про рішення Ради національної безпеки і оборони України: Указ Про Службу безпеки України: Закон України від 25.03.1992 № 2229-XII/ Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text (дата звернення: 30.04.2022)

63. Проблеми забезпечення національної безпеки України на сучасному етапі державотворення: матеріали круглого столу (Київ, 21 жовт. 96 2010 р.); НАДУ при Президентові України ; за заг. ред. Г. П. Ситника. – К. : НАДУ, 2011. – 72 с

64. Протидія російській інформаційній агресії: спільні зусилля задля захисту демократії. Матеріали круглого столу/ URL: http://osvita.mediasapiens.ua/monitoring/advocacy_and_influence/vlasniy_narativ_zamist_kontrpropagandi/ (дата звернення: 18.04.2022).

65. Протидія російській інформаційній агресії: спільні зусилля задля захисту демократії. Матеріали круглого столу/ URL: http://osvita.mediasapiens.ua/monitoring/advocacy_and_influence/ vlasniy_narativ_zamist_kontrpropagandi/ (дата звернення: 29.04.2022)

66. Ржевська Н. Ф. Інформаційна протидія та безпека: нові об'єкти інформаційної безпеки // Актуальні проблеми міжнародних відносин: зб. наук. праць, Київ: ІМВ КНУ імені Тараса Шевченка, 2008. 61–63 с.

67. Рева Т.С. Сучасний політичний екстремізм (на прикладі Іспанії, Італії та Німеччини) : дис. канд. політ. наук: 23.00.02 / Т.С. Рева . – Київ : Київський національний університет імені Тараса Шевченка., 2012 . – 211 с.

68. Резнікова О. О. Актуальні питання протидії тероризму у світі та в Україні / О. О. Резнікова, А. О. Місюра, К. Є. Войтовський. – Київ: НІСД, 2017. – 60 с.

69. Роговець В. Інформаційні війни в сучасному світі: причини, механізми, наслідки / В.Роговець // Персонал. – 2000. – № 5.

70. Роль та місце інформаційного забезпечення в системі державного управління / П.М. Сніцаренко, Ю.А. Саричев // Державне управління: теорія та практика (електронне наукове фахове видання НАДУ). – 2016. – № 1. – С.46-56.

71. Слюсаревський М. Інформаційний простір : критика існуючих визначень і спроба побудови теорії. Вісн. ХДУ. Серія «Психологія, політологія» : Особистість і трансформаційні процеси в суспільстві. 97 Психолого-педагогічні проблеми сучасної освіти. Харків. 1999. Ч. 4-5. С. 337- 342.

72. Сологуб Р. - Як захистити критичну інфраструктуру країни у кіберпросторі / Р. Сологуб / URL: https://biz.nv.ua/ukr/experts/jakzakhistitinajtsinnishu-informatsiju-u-kiberprostori-2510093.html (дата звернення: 04.05.2022)

73. Соцопитування: Населення Донбасу не хоче жити у ЛНР/ДНР. URL: http://news.vash.ua/news/suspilstvo/sotsopytuvannya-naselennya-donbasune- khoche-zhyty-u-lnrdnr.

74. Старостіна, Є. В. Захист від комп'ютерних злочинів та кібертероризму. Питання та відповіді / Є. В. Старостіна, Д. Б. Фролов. М.: Ексмо, 2005.

75. Статут Організації Об’єднаних Націй і статут Міжнародного суду: від 26.06.1945. URL: https://zakon.rada.gov.ua/laws/show/995_010#Text. (дата звернення: 12.05.2022)

76. Стратегія кібербезпеки України, затверджена Указом Президента України від 15.03.2016 № 96 // Офіц. вісн. України. – 2016. – № 23

77. Стратегія національної безпеки України, затверджена Указом Президента України від 26.05.2015 № 287/2015.

78. Телешун С. О. Публічна політика та управління / С. О. Телешун, О. Р. Титаренко, С. В. Ситник., 2010. – 36 с.

79. Теоретичний підхід до інформаційного забезпечення в системі державного управління у воєнній сфері / Ю.О. Саричев // Вісник НАДУ при Президентові України [за заг. ред. Ю.В. Ковбасюка]. – 2016. – № 4 (83). – С.153-160.

80. Тероризм: визначення та сутність: монографія / [А. В. Коростиленко, Б. Д. Леонов, І. Н Рижов та ін.]; під. заг. ред.. В. В. Крутова, І. І. Мусієнко, В. А. Глушкова. - К.: Центр уч.-наук. та наук.-практ. видань НА РБ України, 2014. – 192 с.

81. Томас Т.Л. Стримування асиметричних терористичних загроз, що стоять перед суспільством в інформаційну епоху// Світова спільнота проти глобалізації злочинності та тероризму: матеріали міжнар. конф. М., 2007 р. 98

82. Указ Президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». URL: https://www.president.gov.ua/documents/472017-21374. (дата звернення: 08.04.2022)

83. Фурсов А.І Психоісторична війна. URL: https://firtka.if.ua/blog/view/a-i-fursov-psihoistoricna-vijna45613. (дата звернення: 02.04.2022)

84. Шеломенцев В.П. Кримінологічна безпека у кіберпросторі: система понять. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2010. № 23. С. 342-348.

85. Шхагапсоев З.Л., Тарчоков Б.А. Современные контуры системы противодействия различным проявлениям терроризма : учеб. пособие. Нальчик, 2012 р. 136 с.

86. Щекотихін В. М. Інформаційна війна. Інформаційне протиборство: теорія і практика: монографія / В. М. Щекотихін, А. В. Корольов, В. В. Корольова та ін - М.: Академія ФСО Росії, ЦАТУ, 2010. - 999 с.

87. Ярема О.Г. Предмет правового забезпечення інформаційної безпеки в інформаційному праві / О.Г. Ярема, С.С. Єсімов // Науковий вісник Львівського державного університету внутрішніх справ. – 2016. – № 2. – С. 244-252.

88. Яцик Т.П. Особливості інформаційного тероризму як одного із способів інформаційноївійни // Науковий вісник Національного університету ДПС України (економіка, право). – 2014. – № 2 (65) – С. 55-60.

89. Bennett C.J., Raab C.D. Taking the Measure of Privacy: Can Data Protection be Evaluated? // International Review of Administrative Sciences. – 1996. – № 4 (62). – P. 31-32.

90. Defining cyber terrorism URL: https://www.ipolicy.org/2009/07/defining-cyber-terrorism.html (дата звернення: 30.04.2022).

91. Francen E. Gender Inequality in Information Security. URL: https://www.infosecurity-magazine.com/opinions/gender-inequality-security/. 99

92. Hoffman B. Inside Terrorism. N.Y.: Columbia University Press, 2006. P. 202.

93. Human Rights Watch: Росія масово порушує права людини в Криму. URL: http://krymsos.com/news/human-rights-watch-rosiya-masovoporushuye-prava-lyudini-v-krimu (дата звернення: 07.05.2022)

94. Jerrold M. From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism / M. Jerrold // NATO Library

at:TERRORISM_AND_POLITICAL_VIOLENCE, vol. 12, no. 2, Summer 2000, P. 97-122.

95. Jerrold M. From Car Bombsto Logic Bombs : The Growing Threat from Information Terrorism / M. Jerrold // NATO Libraryat : Terrorism and political violence, vol. 12, no. 2, Summer 2000. – P. 97-122.

96. Marianne W Jørgensen, Louise J Phillips Discourse Analysis as Theory and Method SAGE, 2002-229 ISBN 0761971122, 9780761971122

97. National Commission on Terrorist Attacks upon the United States. The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States. New York, 2004.

98. Proposed policy recommendations for the high level conference. – RAN.2012.December. – URL: http//ec.europa.eu/dgs/home-affairs (дата звернення: 02.05.2022)

99. Поведа О. Геополітичні виміри подальшого розширення ЄС // Сучасні міжнародні відносини: актуальні проблеми теорії і практики. Матеріали міжнародної науково-практичної конференції. Том ІІ. Київ, 2020. – С. 77-85

100. Магда Є. Гібридна війна. Київ, 2015.