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

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач випускової кафедри
_____ Н.Ф. Ржевська
«____» _____ 2021 р.

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

Тема: «ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ: МІЖНАРОДНИЙ ДОСВІД ТА ВІТЧИЗНЯНА ПРАКТИКА»

Виконавець: студентка 2 курсу, 208 М групи, Іванова Ольга Олегівна

Науковий керівник: д.і.н., проф., професор кафедри міжнародних відносин, інформації та регіональних студій Троян Сергій Станіславович

Нормоконтролер: _____ В. Ємець

КИЇВ, 2021

ЗМІСТ

ВСТУП

Актуальність теми дослідження. У процесі свого розвитку і становлення людство вступило в XXI століття. Процес глобалізації включає формування глобальної економіки, науки, інформаційного простору. Особливу роль у забезпеченні цілісності сучасного світу відіграє розвиток міжнародних комунікаційно-інформаційних мереж.

В останнє десятиліття правовим засадам забезпечення безпеки інформаційного простору від різних викликів та загроз, серед яких інформаційна війна, інформаційний тероризм та інформаційні злочини, приділяється особлива увага як на рівні законодавства, так і на рівні доктрини. Причиною є глобальні процеси інформатизації, а також прогрес у сфері розвитку інформаційних технологій.

Сучасний тероризм характеризується масштабністю терористичних акцій, високим рівнем організації та фінансування, різко збільшеною технічною і технологічною оснащеністю (такі терористичні організації, як «Хезболла», Хамас та ІДІЛ, мають складну структуру, органи управління, свої теле- і радіостанції), що зумовлює поява його нових форм. Крім того, з кожним роком зростають кількісні показники терористичної злочинності.

Запуск першого штучного супутника Землі став технологічним каталізатором формування глобальних зв'язків, і вважається символічним актом «народження» інформаційної ери. Звичайно, комп’ютерні мережі стали складнішими за супутники, а швидкість і кількість інформації, яку необхідно передати, значно зросла. Незважаючи на тенденцію до цілісності та єдності, у світі все ще існують серйозні протиріччя майже в усіх сферах людського існування (економіка, культура, суспільні відносини тощо).

Активний вплив тероризму на соціально-політичні процеси нині є постійним та суттєвим деструктивним явищем. Проблема тероризму, будучи відносно самостійною, постає як частина глобальних деструкцій, які мають відчутний вплив на соціально-політичні процеси на глобальному,

регіональному та національному рівнях. Дане питання вимагає для свого дослідження та вирішення міждисциплінарної конвергенції природного, суспільного та науково-технічного знання та чітко налагодженого міжнародного співробітництва у розробці та здійсненні комплексних цільових програм.

На фоні сучасної еволюції національних і міжнародних фінансово-економічних, соціально-культурних, політичних, технічних і технологічних процесів тероризм формується як самостійний фактор, що надає значний вплив на політичну обстановку в світі, в окремих регіонах і країнах, застосовується політичними суб'єктами та злочинними синдикатами, як дієвий метод створення цільової конфліктної ситуації для реалізації визначеної політичної поведінки, а також як виправдання політичних та економічних експансій.

На жаль, сьогодні поняття «інформаційна війна» як ніколи актуальне. Ми мимоволі ставали свідками та брали участь у різноманітних інформаційних протистояннях – чи то виборчий конкурс, чи то спроба нападу зловмисника, чи просто просування певних товарів та послуг у жорсткому конкурентному середовищі.

У класичному розумінні інформаційна війна – це форма інформаційного протистояння, це комплекс заходів впливу на суспільну свідомість з метою зміни поведінки людей та встановлення цілей, які не відповідають їхнім інтересам, і, звісно, захисту від таких впливів.

Раніше вважалося, що інформація всього лише забезпечує проінформованість людей про події й факти в навколишньому світі. Інформація сприймалася як корисний ресурс, призначений для розширення людських можливостей. У сучасних умовах інформаційна війна розглядається військовими теоретиками як якісно новий вид бойових дій, активна протидія в інформаційному просторі, а інформація при цьому - як потенційна зброя та зручна ціль. Інформаційна війна розглядає інформацію як окремий об’єкт або зброю, що не завдає фізичної шкоди але може

призвести до війни реальної. Інформаційна зброя, як правило, не спрямована на досягнення втрат у живій силі супротивника. Вона не знищує фізично й не руйнує людські, матеріально-технічні та інші ресурси, а підриває основи дії механізмів організації та управління.

Протидія тероризму належить до життєво важливих проблем сучасного суспільства. Пояснення сучасного тероризму в умовах глобалізації можливе лише в контексті багатоаспектного та полісистемного підходу, що дозволяє врахувати максимально можливу кількість факторів та умов. З огляду на особливу соціальну небезпеку наукові дослідження цього феномена мають високу значимість і актуальність.

Стан вивчення проблеми складають праці українських та зарубіжних вчених, які досліджували питання інформаційного тероризму та його впливу на сучасне суспільство. Серед українських науковців можна виділити: Авдошин І.В., Баліцький В.В., Богуцький П.П., Горбулін В.П., Слюсаревський М.М., Майоров В.В., Задорожній О.В. та інші.

До зарубіжних вчених відносяться: Додонов О.Г., Жайворонок О.І., Сидненко Г.Ф., М. Дж. Девост, Б.Х. Х'ютон, Н.А. Поллард та інші.

Метою дослідження є розкриття проблеми протидії інформаційному тероризму як складника національної безпеки держави, визначення генезису поняття «інформаційний тероризм», комплексний аналіз практики застосування та особливості міжнародної боротьби з цим явищем та основні тендеції вирішення цієї проблеми.

Для досягнення поставленої мети визначені наступні **завдання дослідження:**

– дослідити історію та становлення терміну «інформаційний тероризм» ;

– проаналізувати явище інформаційного тероризму, як інструмент впливу на сучасне інформаційне поле;

– розкрити сучасний стан державної політики та основних напрямків вдосконалення системи забезпечення інформаційної безпеки України;

– проаналізувати міжнародно-правове забезпечення та інституційні механізми протидії інформаційного тероризму.

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.

Методологічну основу роботи складає сукупність загальнонаукових та спеціальних методів політичної науки. У процесі написання даного дослідження були використані різні загальнотеоретичні та спеціально-наукові методи та підходи для вивчення предмету дослідження.

Основними методами дослідження був історичний – використовувся при дослідженні та висвітленні передумов появи терміну «інформаційний тероризм»; формально метод – використовувався при аналізі законодавства зарубіжних країн, щодо боротьби з терористичними атаками; порівяльний метод використовувався для дослідження відповідальності за тероризм на міжнародному та на національному рівні.

Крім зазначених методів, також використано метод системного аналізу, логічний метод та структурно-функціональний.

Апробація результатів дослідження: результати дослідження опубліковані в електронних виданнях, подані на конференції та на стипендіальну програму «ЗАВТРА.UA»:

Публікації. Основні результати та висновки дипломної роботи знайшли відображення у трьох тезах доповідей на міжнародних науково-практичних конференціях і одній науковій статті.

– 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.

– Іванова О.О. Інформаційний тероризм та його вплив на сучасну політику світу // стипендіальна програма «Завтра.UA», м. Київ 2021

– Іванова О.О. Основні напрями вдосконалення системи забезпечення інформаційної безпеки України // Topical issues of modern science, society and education – 2021р., м. Харків, 28-30 листопада 2021р.

– Іванова О.О. Міжнародно-правове забезпечення боротьби з актами інформаційного тероризму // III Міжнародна науково-практична конференція «Modern science: innovations and prospects» - 2021 р., м. Стокгольм, 5-7 грудня 2021 р. Стокгольм, 2021.

Структура дипломної роботи. Структура дипломної роботи зумовлена предметом, метою та завданнями дослідження. Дипломна робота складається зі вступу, трьох розділів, якими охоплюються вісім підрозділів, висновків та списку використаних джерел (102 найменування). Загальний обсяг дипломної роботи 99 сторінок, у тому числі список використаних джерел – 10 сторінок.

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ АНАЛІЗУ ПОНЯТТЯ ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ

1.1. Поняття інформаційного тероризму: інформаційний простір як засіб терористичної діяльності

Тероризм, що спочатку зародився як національне явище, на сьогоднішній день становить небезпеку для всього світового співтовариства, про що свідчить різноманіття міжнародних документів, що так чи інакше містять у собі питання, пов'язані з визначенням його сутності, заходів протидії та із притягненням до відповідальності осіб, які вчинили терор.

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

Кібертероризм є серйозною загрозою для людства, порівнянною з ядерною, бактеріологічною та хімічною зброєю; причому ступінь цієї загрози через свою новизну не до кінця ще усвідомлений і вивчений. Досвід світової спільноти в цій галузі з усією очевидністю свідчить про безперечну вразливість будь-якої держави, тим більше що кібертероризм не має державних кордонів, кібертерорист здатний однаково загрожувати інформаційним системам, розташованим практично в будь-якій точці земної кулі [6, с. 146].

Наразі всі терористичні та екстремістські організації, що активно діють, мають свої інтернет-сайти у світовій мережі. Як правило, вони містять детальний огляд соціальних і політичних мотивів, що послужили підставою для створення терористичних та екстремістських організацій, інформацію про політичні та ідеологічні цілі, які вони переслідують, відомості про

найбільш відомі акції, біографію засновників та «героїв», жорстку критику «ворогів» , а також огляд поточних новин. Сучасні терористичні та релігійно-екстремістські організації все частіше використовують глобальний інформаційний простір як «прес-центри» для звернень лідерів бойовиків, терористів, повстанців, релігійних радикалів [3, с. 110].

Створювані сайти антигромадського спрямування проектуються на досить високому професійному рівні з використанням великої кількості наочної інформації: фото-, аудіо- та відеофайли, які покликані полегшити сприйняття інформації, залучити якнайбільше прихильників та джерел фінансування. На зазначених сайтах часто розміщуються відомості про тактику та засоби проведення терористичних актів, про типи вибухових та отруйних речовин, основи вибухотехніки, виготовлення саморобних вибухових пристроїв, методи конспірації [16]. Терористичні та екстремістські організації прагнуть використати комунікаційні можливості Всесвітньої павутини для залякування суспільства, поширення антигромадської інформації, пропаганди своїх злочинних ідей.

Протягом багатьох років на міжнародному рівні запроваджувались спроби пояснити, що є тероризм, які найчастіше зводилися до переліку конкретних суспільно небезпечних діянь, що загрожують життю, тілесної недоторканності, здоров'ю людини і т. д. Адекватна неможливість формулювання єдиного поняття тероризму на міжнародному рівні обумовлена різними внутрішньодержавними підходами явища, а також його мінливим та багатоаспектним характером [17].

Визначення тероризму зазвичай складне та суперечливе, і через притаманну тероризму жорстокість і насильство цей термін у його популярному вживанні набув сильного стигматизації. Вперше він був озвучений у 1790-х роках для позначення терору, який використовували революціонери під час Французької революції проти своїх супротивників. Якобінська партія Максимілієна Робесп'єра здійснила «Правління терору», що передбачало масові страти на гільйотині. Хоча тероризм у цьому

вживанні має на увазі акт насильства з боку держави проти своїх внутрішніх ворогів, починаючи з 20-го століття цей термін найчастіше застосовувався до насильства, спрямованого, прямо чи опосередковано, проти урядів з метою вплинути на політику або повалити існуючу режим [25].

Інформаційний тероризм – явище, яке створює прямий вплив на психіку і пізнання людей у цілях формування потрібних думок та суджень, певним чином направляючих поведінку людей [101].

На практиці під інформаційним тероризмом зазвичай розуміють насильницький пропагандистський вплив на психіку, яке не надає можливості людям для критичної оцінки одержуваної інформації.

Інформаційний тероризм це, перш за все, форма негативного впливу на особистість, суспільство і державу всіма видами інформації. Його ціллю є ослаблення і послаблення конституційного устрою держави. Він ведеться усіма доступними цілями та засобами від агентів іноземних спецслужб до державних та зарубіжних засобів масової інформації [87].

У деяких країнах немає законодавчо закріпленого поняття тероризму, як, втім, немає поняття інформаційного тероризму. Однак немає сумнівів у тому, що розробка такого поняття насамперед – на національному рівні конкретизувала б, які злочинні діяння відносяться до тероризму.

Дослідники М. Дж. Девост, Б. Х. Х'ютон, Н. А. Поллард визначають інформаційний тероризм як свідоме зловживання цифровими інформаційними системами, мережами чи компонентами цих систем чи мереж з метою, які сприяють здійсненню терористичних операцій чи актів [82]. Дороті Деннінг (Dorothy Denning), професор комп'ютерних наук Джорджтаунського університету та один з найавторитетніших експертів у галузі комп'ютерної злочинності та кібербезпеки, у своїй книзі «Активність, хактивізм і кібертероризм: Інтернет як засіб впливу на зовнішню політику» говорить про кібертероризм як про « атаці чи загрозі атаки на комп'ютери, мережі чи інформацію, що у них, досконалої з єдиною метою змусити органи влади до сприяння у досягненні політичних чи соціальних цілей» [81, с. 192].

На думку Е.А. Роговского, слідуючи цим визначенням, можна назвати два виду кібертероризму:

– безпосереднє вчинення терористичних процесів з допомогою комп'ютерів і комп'ютерних мереж;

– використання кіберпростору терористичними групами в організаційно-комунікаційних цілях і з метою шантажу, але не для безпосереднього вчинення терактів [5, с. 113].

Перший вид відповідає об'єднанню понять «кіберпростір» і «тероризм» і є навмисну атаку на комп'ютери, комп'ютерні програми, комп'ютерні мережі чи оброблювану ними інформацію, що створює небезпеку загибелі людей, заподіяння значної майнової шкоди чи інших суспільно небезпечних наслідків. Наприклад, перехоплення управління військовим чи інфраструктурним об'єктом з метою порушення громадської безпеки, залякування населення чи впливу прийняття рішень органами влади шляхом загрози здійснення аварії (катастрофи) [20, с. 36].

До першого виду кібертероризму примикають усі здійснювані з допомогою Інтернету, звані, «інформаційні» правопорушення проти Конституції (антиконституційні заклики, загрози конституційним права і свободи людини і громадянина, поширення страхітливих чуток, загрози інформаційному забезпеченню державної політики та інших.).

Другий вид кібертероризму - використання інформаційного простору терористичними групами в організаційно-комунікаційних цілях (але не для безпосереднього вчинення терактів), проведення теоретичного, військового, теологічного навчання та пропаганди, а також рекрутування нових членів та забезпечення зв'язку між окремими осередками. Нині у науковій літературі немає загальновизнане визначення поняття «інформаційний тероризм» («кібертероризм») [30].

Тероризм є складним, багатоаспектним та мінливим явищем. Вивченням феномена тероризму займаються вчені різних галузей знань (соціологи, політологи, кримінологи, психологи та ін.).

Звісно ж, що всебічне дослідження цього негативного явища, його наслідків, і навіть попередження можливе лише після розробки відповідального вимогам у суспільному розвиткові понятійного апарату [8, с. 231].

Також важливо звернути увагу на розуміння поняття інформаційного простору. Інформаці́йний про́стір — сукупність результатів семантичної діяльності людства. Багаторівнева структура, що акумулює результати діяльності суспільства, за допомогою конкретних компонентів системи інформації та зв'язку [24].

М. М. Слюсаревський у власній «реляційної теорії інформаційного простору» розглядає інформаційний простір як стан (а також результат) постійної взаємодії виробництва та споживання інформації, тобто інформаційний простір розглядається, як простір для обробки інформації. При цьому, коли хтось сприймає інформацію, то існування інформації вважається можливим, тобто обов'язковою умовою для обробки інформації є наявність системи зв'язку «джерело інформації - приймач інформації».

Вважається, що параметри інформаційного простору зумовлені часовими та психологічними особливостями інформаційного процесу та соціально-психологічними характеристиками споживачів інформації. Тому цю категорію рекомендується характеризувати не за обсягом виробництва інформації чи площиною поширення інформації, а за її споживанням та інтенсивністю. Тому категорія інформаційного простору наповнена власними теоріями — змістом комунікації та соціальної психології, відривається від географії та інших рівнів і починає виконувати самостійну функцію.

Центром інформаційного простору є суб'єкт, який у процесі своєї діяльності створює, накопичує, зберігає та передає інформацію. Такими суб'єктами можуть бути окремі особи або соціальні групи, організації, підприємства і навіть державні установи, тобто користувачі будь-яких інформаційних технологій [72, с. 340].

До характерних рис терористичних актів в інформаційній сфері відносять:

– прихований характер підготовки та реалізації таких діянь – відсутність проявів та слідів проникнення;

– масштабність атак – завдання удару по великій кількість об'єктів;

– синхронність атак - вони можуть бути здійснені одночасно за багатьма об'єктами;

– віддаленість - джерело атаки може перебувати за межами країни, в якій відбувається напад;

– інтернаціональність – шкода може поширюватися на декілька та більше держав [33, с. 41].

Тероризм – не статичне явище; він завжди корелює зі змінами, що відбуваються у суспільстві (у галузі озброєння, технічного та інформаційного обладнання тощо). У зв'язку з цим тероризм існує у співвідношенні з процесами, що відбуваються у різних сферах життя суспільства та держави.

Таким чином, інформаційний тероризм (кібертероризм) – це навмисні атаки на інформаційні системи, інформаційно-телекомунікаційні мережі або компоненти цих систем чи мереж, на комп'ютерні мережі, апаратно-програмні комплекси державних, оборонних установ, важливих, особливо важливих та інших об'єктів, у тому числі фізичних осіб, з метою дезорганізації їх роботи та саботажу, вчинення з використанням інформаційних засобів дій, що лякають населення, з метою дестабілізації діяльності органів влади або міжнародних організацій або впливу на прийняття ними рішень, а також загроза вчинення зазначених дій з тією ж метою, якщо ці дії створюють небезпеку загибелі людини, заподіяння значної майнової шкоди чи настання інших тяжких наслідків [89, с. 57].

У цьому визначенні враховано обидва види здійснення кібертероризму: по-перше, безпосереднє вчинення терористичних дій за допомогою інформаційних засобів і, по-друге, використання кіберпростору терористичними групами для безпосереднього здійснення атак на

інформаційні системи, інформаційно-телекомунікаційні мережі або компоненти цих систем чи мереж терористичних цілях.

Сьогодні форми та методи захисту від інформаційного тероризму, що спираються на нові мережеві технології, значно збільшили масштаб, ефективність та результативність цього виду діяльності.

По-перше, рекрутування може здійснюватися дистанційно. З урахуванням практично повсюдної доступності відповідних матеріалів в Інтернеті, традиційний контакт "віч-на-віч" стає не потрібен. При цьому завдання рекрутування полегшуються за рахунок того, що ширші аудиторії можуть дізнатися про існування та цілі тієї чи іншої організації.

По-друге, сучасні форми дистанційного рекрутування ефективніші завдяки тому, що один рекрутер має можливість “розробляти” одночасно велику кількість людей, котрі живуть у межах його регіону, країни, але й у віддалених кінцях світу. Сучасні мережеві технології, такі як Інтернет та відеоігри, підвищують можливості терористичних груп поширювати та пропагувати свої ідеї, у тому числі враховуючи проблеми адаптації форми та змісту послання до особливостей конкретних цільових аудиторій [98].

1.2. Види інформаційного тероризму та інструменти інформаційного впливу

Інформаційний тероризм – це абсолютно нова терористична діяльність, метою якої є використання сучасних інформаційних технологій для пошкодження або знищення урядової інфраструктури (критичної інфраструктури, яка може бути вразливою до антитерористичних атак тощо). Його характеристика — маніпулювання свідомістю людей шляхом активного використання психологічного впливу [91].

Внаслідок широкого застосування нових інформаційних технологій зазнали зміни як засоби збройної боротьби, так і стратегія, і тактика ведення сучасних воєн, з'явилися нові концепції ведення бойових дій «інформаційний

вік», враховують нові чинники вразливості сторін. Ці нові концепції безпосередньо пов'язуються з тим, що стрімка еволюція кіберпростору може відкрити додаткові можливості якісного вдосконалення озброєння та військової техніки, але й зумовити нові проблеми та вразливі сторони протиборчих сторін: у сучасних умовах більш вразлива та з воюючих сторін, яка має менше інформації про поле бою, повільніше обробляє інформацію та приймає рішення з меншою оперативністю.

Очевидно, що терористи, які використовують новітні технічні досягнення, значно розширили свої деструктивні можливості, дозволивши привернути увагу громадськості, постійно тримаючи людей в страху, впливаючи на їхній психологічний стан. Сьогодні майже всі цифрові засоби обробки та зберігання інформації уразливі до терористичних атак.

Неухильно зростає залежність процесів, які у областях різних функціонування інформаційно-телекомунікаційних систем. Ефективність функціонування більшості сучасних засобів збройної боротьби визначається, в першу чергу, можливостями забезпечують військову діяльність, від якості діяльність автоматизованих систем управління та зв'язку. З'являється широкий спектр методів та засобів впливу на подібні системи шляхом виведення з ладу окремих структурних елементів, ключових операторів або маніпуляції інформацією в них на користь зацікавлених сторін [12, с. 165].

При цьому сам конфлікт у стадію відкритого збройного зіткнення може і не перейти, а протиборства», результатом якого стане усвідомлення однієї з сторін, що вона не може більше розраховувати на ефективне застосування своїх засобів збройної боротьби. У будь-якому випадку сторона, яка краще володіє стратегією та тактикою ведення військових дій в інформаційному просторі (інформаційною завершиться вже після етапу “інформаційного протиборства”, результатом якого стане усвідомлення однієї з протиборчих сторін, що вона не може більше розраховувати на ефективне застосування своїх засобів збройної боротьби. У будь-якому випадку сторона, яка краще

володіє стратегією та тактикою ведення воєнних дій в інформаційному просторі (інформаційної війни), матиме в сучасних умовах істотні переваги.

В якості інформаційної зброї може виступати зовсім різні інструменти: високоточна зброя для ураження органів управління або радіоелектронної боротьби, джерела потужного електромагнітного імпульсу, програмні віруси та ін. Критерієм віднесення до розряду «інформаційної зброї» може розглядатися тільки ефективність того чи іншого озброєння при вирішення завдань інформаційної війни. окремих радіоелектронних засобів, засоби Наступальна операція з використанням інформаційної зброї (інформаційна наступальна операція) може проводитися як самостійно, так і в комплексі з традиційними наступальними діями, або передуючи їм або підтримуючи їх проведення. У будь-якому разі інформаційна наступальна операція покликана забезпечити «інформаційну перевагу» в ході конфлікту за рахунок впливу на засоби збору інформації, її переробки та зберігання, а також на особовий склад, який обслуговує техніку та приймає рішення [27, с. 110].

Нині немає усталеної класифікації інформаційної зброї, як і і чіткого визначення цього поняття. Виходячи із загальних міркувань до інформаційного відносять зброю, що найбільш ефективно вирішує завдання інформаційної війни. При цьому слід додати, що інформаційна зброя має сприяти досягненню військової переваги нетрадиційним чином, виключаючи масовану фізичну поразку та орієнтуючись на високоточні та максимально потайливі нелетальні способи впливу.

За своїм цільовим призначенням інформаційна зброя ділиться на оборонну та наступальну. Оборонна інформаційна зброя вирішує завдання оборонної інформаційної війни та комп'ютерної активної протидії Наступальне собою являє безпеку системи багаторівневої різні системи інформаційну інформаційну зброю призначено для впливу на противника шляхом ураження його найбільш критичних структур:

– засоби впливу на компоненти радіоелектронного обладнання та їх енергоживлення для тимчасового або незворотного виведення з ладу окремих компонентів радіоелектронних систем;

– засоби впливу модулів управління, що забезпечують виведення їх з ладу або зміну алгоритму їх функціонування за допомогою використання на програмний ресурс електронних спеціальних програмних засобів;

– засоби впливу на процес передачі інформації, які призначені для припинення або дезорганізації функціонування підсистем обміну інформацією за поширення сигналів та алгоритми функціонування;

– засоби пропаганди та дезінформації для внесення змін до інформації систем управління, створення віртуальної картини обстановки, яка відрізняється від дійсності, зміна системи цінностей людини, завдання шкоди духовно-моральному життю населення противника;

– засоби призначені для впливу на психіку та підсвідомість людини з метою зниження та придушення її волі, тимчасового виведення з ладу, зомбування [26].

Не можна стверджувати, що ця класифікація охоплює всі види інформаційної зброї, поява яких можлива у майбутньому. Проте всі відомі практичні розробки, що проводяться нині, повністю охоплюються.

Інформаційну зброю кожного виду можна класифікувати за низкою ознак: одно- та багатоцільова чи універсальна; ближнього та далекого радіусу дії; індивідуального, групового або масового ураження; за типом носія; за ефектом ураження.

На основі опрацювання, аналізу та розуміння різних поглядів на одне з найнебезпечніших і важко передбачуваних явищ сучасності – інформаційний тероризм та вплив глобалізаційної трансформації на національне державотворення, можна визначити поняття та виділити його основні види, а саме:

«Інформаційний тероризм» — це вид тероризму, який зосереджується на використанні різних форм і методів для тимчасового або безповоротного

виведення з експлуатації інформаційної інфраструктури країни або її елементів, а також використання цієї інфраструктури для цілеспрямованого створення умов, що має катастрофічні наслідки для всіх сторін суспільства і країни, включаючи використання різних методів і засобів для інформаційного впливу на всі сторони людського суспільства (фізичну, інформаційну, когнітивну, соціальну) [23, с. 44].

Можна виділити основні компоненти:

– інформаційно-психологічний тероризм – контроль над засобами масової інформації для поширення дезінформації, чуток, терористичних організацій; шляхом насильства або погроз насильством, підкупу, введення наркотичних засобів і психотропних речовин, використання методів нейролінгвістичного програмування, гіпнозу, засобів створення ілюзій, мультимедійних засобів введення інформації в підсвідомість тощо.;

– інформаційно-технологічний тероризм - знищення окремих фізичних елементів національного інформаційного середовища, створення перешкод, використання спеціальних процедур для стимулювання руйнування системи управління, або, навпаки, зовнішній тероризм, що контролює та знищує технічні засоби (у тому числі літаки), біологічні та хімічні засоби руйнування елементної бази та ін. , знищення або активне придушення ліній зв'язку, неправильна адресація, штучне перевантаження вузлів комутації тощо;

– когнітивний тероризм – легітимізація насильницьких способів досягання протиправних терористичних цілей шляхом впливу на емоції та поведінкові елементи людського суспільства, суспільної свідомості, формування радикальних соціальних стереотипів, соціальних уявлень та концепцій, підсвідомості, емоційної стимуляції ставлення до легалізації насильства. Зачіпає нестійкі, переважно емоційні погляди, особливо молоді, яка через екстремістські та радикальні дії розуміє навколишній світ і себе. Приводить до таких когнітивних концепцій, як радикалізм, екстремізм, фанатизм, шовінізм і фундаменталізм;

– мережевий тероризм (кібертероризм) – масивні узгоджені дії великих соціальних мереж (автономні приватні чи неурядові організації) через деструктивний терористичний вплив, усвідомлення та управління суспільством (фізичними особами, народними об'єднаннями) (релігійні секти, громадські організації, рухи, некомерційні організації);

– соціально-комунікаційний тероризм - руйнування суспільного фундаменту через спеціально розроблені програми, які вчать людину легковажно сприймати будь-яку інформацію і вірити в неї (всебічне поширення та маніпулювання громадською думкою, свідомістю, подання з використанням фізіологічних і психологічних законів її сприйняття). Використовується певний текст, певний ритм і мовна модуляція. Маніпулювання свідомістю здійснюється шляхом занурення людей у контрольоване інформаційне поле, що створює фіктивну картину світу. Фундаментом формування віртуального інформаційного поля є обман [29].

Слід зазначити, що для України, де соціальна інформатизація ще на стадії зародження, а інформаційні ресурси знаходяться в руках приватних підприємств, основна загроза інформаційного тероризму надходить ззовні, а не зсередини. В основному вони створені іноземними та міжнародними терористами та іншими злочинними групами та організаціями, яким бракує координації та зосередженості на державному управлінні в боротьбі з цим небезпечним явищем.

Нездатність органів державного управління створити ефективні механізми боротьби з інформаційними загрозами створила передумову для зростання чисельності інформаційного тероризму. Особливо це помітно в контексті збройного конфлікту на сході України. Тому вдосконалення механізму боротьби з інформаційним тероризмом дасть змогу інформаційному законодавству України перейти на новий якісний рівень та пришвидшити вироблення ефективних заходів протидії цьому негативному явищу [69, с. 60].

Можна сказати, що боротьба з тероризмом – це діяльність з попередження, виявлення, припинення та мінімізації наслідків терористичної діяльності.

В. Ліпкан запропонував обґрунтоване визначення цього терміну, а саме: «Боротьба з тероризмом:

– система організаційно-правових, режимних, оперативно-розшукових, інженерно-технічних, бойових та інших заходів, що здійснюються спеціально уповноваженими органами державної влади з метою запобігання, виявлення та припинення терористичних актів та терористичних злочинів, а також нейтралізації посттерористичних ситуацій, розкриття злочинів цієї категорії, виявлення винних і їх покарання;

– комплекс економічних, політичних, правових, психологічних, організаційних і технічних заходів, спрямованих на запобігання (пом'якшення) факторів, що сприяють тероризму, запобігання, припинення, реєстрацію, розкриття (розшук терористів) та розслідування тероризму, кримінальне судочинство, виправлення винних у тероризму і контроль за їх поведінкою для відбуття ними покарання, а також компенсацією негативних наслідків;

– діяльність щодо запобігання, виявлення та припинення терористичних актів;

– діяльність, спрямована на ліквідацію тероризму як деструктивного, руйнівного та соціально небезпечного явищ, у тому числі підготовка та реалізація політичних, правових, соціально-економічних, інформаційних, освітніх, організаційних, оперативно - розшукових, розвідувальних і контррозвідувальних, спеціально призначена для запобігання, виявлення, припинення терористичної діяльності, мінімізації її наслідків, визначення та усунення причин і умов, що призводять до терористичної діяльності та які їй сприяють» [9].

Тоді боротьба з інформаційним тероризмом означає моніторинг, розслідування, припинення, мінімізацію його наслідків, попередження та

запобігання цього негативного явища з метою забезпечення безпеки життєво важливих інтересів особи та суспільства в інформаційній сфері особи, суспільства і держави.

Національні механізми боротьби з інформаційним тероризмом – в умовах публічної політики існуючі та спеціально створені державні установи, формальні та неформальні державні та громадські організації, соціальні групи, громадські об’єднання, окремі особи, а також правові, економічні, політичні, інформаційні та інші комунікації: в тому числі взаємозв’язки, засоби та технології призначені для запобігання, виявлення, боротьби та ліквідації наслідків інформаційного тероризму.

Управління національним механізмом боротьби з інформаційним тероризмом є невід'ємною частиною національного механізму боротьби з інформаційним тероризмом, завданням якого є координація повсякденної діяльності та управління основним органом боротьби з інформаційним тероризмом при появі ознак інформаційного тероризму, а також вироблення і надання вищому керівництву держави необхідних варіантів протидії цьому негативному явищу [38, с. 100].

У зв’язку з цим, виділимо основні ознаки інформаційного тероризму:

– особливий вид психологічної та/або кіберзлочинності;

– набули поширення через засоби масової інформації, комп'ютери та інші мережі, інформаційно-комунікаційні системи тощо;

– завдяки використанню інформаційного тероризму він має психічний вплив на широку громадськість та об'єкти ключової інформаційної інфраструктури;

– може трансформуватися, до Закону України «Про боротьбу з тероризмом» в технологічний тероризм (з використанням ядерної, хімічної, бактеріальної (біологічної) та іншої зброї масового ураження або її компонентів, інших шкідливих для здоров’я людей речовин, електромагнітних засобів, комп’ютерних систем та комунікаційних мереж, включаючи захоплення, виведення з ладу і руйнування потенційно

небезпечних об’єктів, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації));

– залякування для досягнення бажаного ефекту;

– мета – привернути увагу значної кількості людей шляхом широкого розголосу та демонстраційних дій [100].

1.3. Інформаційний тероризм як загроза національної безпеки

Вплив загрози тероризму може порушити нормальну роботу країни та суспільства. Для своєчасного вжиття превентивних заходів необхідно оцінити стійкість держави та суспільства (як елемента національної стійкості) до відповідних загроз [1, с. 71].

Проте розвиток інформаційного поля супроводжується появою нових загроз інтересам особистості, суспільства, країни та її національній безпеці. Сьогодні за допомогою ЗМІ можна впливати на інформованість громадян у конкретних країнах, регіонах та світі.

Так, в Україні іноді навіть ЗМІ відкрито виступають проти чинної влади, що зазвичай для демократичних держав. Тільки тоді, коли ЗМІ економічно самодостатні, вони можуть чесно й конструктивно протистояти владі, бо лише за таких умов їх можна вважати незалежними.

На жаль, українські ЗМІ опираються не на споживачів інформації, а на певні фінансово-промислові групи, які часто зловживають свободою слова, використовують її для розгортання інформаційної війни проти конкурентів, «споживають компромісну інформацію» тощо.

Все це фактори, які призводять до інформаційного тероризму проти населення країни. Крім того, системна зовнішня політика Російської Федерації загострила цю ситуацію. Можна сказати, що його метою є модифікація реальної системи безпеки в Європі.

Наразі актуальними є такі сфери, де кіберінструменти використовуються в терористичних цілях:

– пропагувати тероризм та екстремістські ідеології через соціально-орієнтовані Інтернет-мережі, спеціалізовані мережеві ресурси, месенджери та заражені веб-сайти;

– створити умови для терористичної діяльності шляхом організації прихованих каналів зв'язку, постачання та фінансування на основі популярних і прихованих онлайн-сервісів, платіжних систем, торгових майданчиків тощо;

– використання кіберпростору для спричинення руйнівного впливу на інформаційні та телекомунікаційні системи критичних інфраструктур для ініціювання техногенних надзвичайних ситуацій (кібертерористичні операції);

– використовувати інформацію та кіберпростір для поширення завідомо неправдивої анонімної інформації з терористичними загрозами, розпалювання ворожнечі між етнічними групами та релігіями, підриву стабільності соціальної та політичної ситуації в країні чи окремому регіоні.

Сьогодні Російська Федерація розгортає інформаційну війну проти України, яка як країна, яка прагне інтегруватися в європейські (і цивілізовані світові) спільноти, має на меті нав’язувати певні ідеологічні стереотипи та громадську думку через ЗМІ, особливо через електронні видання [46]. Такі війни дуже поширені в глобальному інформаційному полі. Наприклад, Національний інститут стратегічних досліджень США та деякі західні експерти проаналізували його і вважали психологічну війну частиною інформаційної війни. На їхню думку, головним завданням психологічної війни є маніпулювання масами [66].

Метою цієї маніпуляції є: впровадити у свідомість громадськості та окремих людей ворожі думки та думки; дезорієнтація та дезінформація мас; послабити певні переконання та тероризувати народ образом ворога; використати власну владу для залякування ворога [14].

Експерти оперативної групи East Strat Com Task Force щороку реєструють тисячі випадків дезінформації та неправдивої інформації з російських і проросійських ЗМІ, які поширюються 18 мовами в Європі та світі [99].

Іншими словами, в ідеалі існує емоційний вплив на маси, щоб підірвати здатність країни протистояти загрозам (включаючи інформацію). По суті, це так званий елемент змішаної війни.У цей період Російська Федерація:

– наклеп на українське керівництво та репутацію України як проєвропейської країни;

– продовжувати консолідувати економічне та військове управління тимчасово окупованими територіями Донбасу з метою збереження загрози застосування сили проти України та окупації нових територій;

– розпалювати ворожнечу українського суспільства на основі раси, мови, релігії та регіону, щоб спровокувати громадянські заворушення, насильницькі заворушення та дискредитувати органи влади;

– посилення економічного тиску через торговельні війни та припинення поставок ключових ресурсів з метою обмеження спроможності України розвивати економіку, підтримувати соціальну стабільність та забезпечити належне фінансування заходів політики національної безпеки та оборони;

– громадяни Європи, політики та експерти стверджували ідею «громадянської війни» (а не російської агресії) на сході України. З цією метою продовжують відігравати роль квазінаціональні інституції, які займаються інформаційно-рекламною підтримкою так званих «ДНР» і «ЛНР» у європейських країнах;

– продовжувати спроби легалізувати анексію Криму;

– звести до мінімуму міжнародну підтримку (у тому числі фінансову) Україні. Основний акцент робиться на корумпованій частині України, якій не вистачає реформ.

З моменту виникнення журналістики проблема дезінформації в ЗМІ існувала завжди, але в епоху розвитку наших цифрових комунікацій ця проблема особливо актуальна. Не існує загальновизнаного визначення дезінформації, але, звичайно, дезінформація містить твердження, які можуть довести помилку або оману; вона створюється, копіюється та поширюється для економічної вигоди або навмисно вводить в оману аудиторію, що може зашкодити суспільству. «Яка шкода? Розмиваючи межу між правдою і брехнею, дезінформація послаблює довіру громадськості до професійних якісних новин та їх ролі в демократичному суспільстві. Дезінформація руйнує довіру до ЗМІ, а коли довіра зникає, зберігайте зв'язок суспільства зникла , але боротьба з дезінформацією шляхом обмеження прав людини є кроком у неправильному напрямку [2].

У 2017 році низка міжнародних організацій прийняла документ під назвою «Про свободу слова, фейкові новини, дезінформацію та пропаганду». Один із головних аргументів полягає в тому, що держави можуть обмежувати свободу слова лише в межах, дозволених міжнародним правом, і дуже шанобливо . причина. Свободу слова не можуть порушувати приватні компанії (по-перше, це, очевидно, посилаються на соціальні платформи, такі як Google і Facebook).

Штучний інтелект все частіше використовується як інструмент політики, який допомагає людям вирішувати, яку інформацію вони бачать в Інтернеті. Комп'ютери навчилися створювати настільки переконливий контент, що людям важко зрозуміти, де правда, а де брехня.

Чи можна розцінювати поширення дезінформації, спрямованої проти країни, як втручання в її внутрішні справи, обговорюється в експертному середовищі, оскільки неправдива або оманлива інформація може завдати серйозної шкоди країні та здійснювати цілеспрямовані атаки ефективніше,

ніж військові. Німеччина нещодавно офіційно визнала, що дезінформація за певних обставин (наприклад, якщо вона призведе до заворушень або призупинення виборів) може розглядатися як незаконне втручання. У той же час поняття дезінформації в контексті міжнародного права є неоднозначним, оскільки деякі документи розглядають лише неправдиві звинувачення. Крім простої брехні, дезінформація також може бути правдивою або частково правдою, але, наприклад, поміщена в неправильний контекст, навмисно обрані чи маніпулювані заяви. Яскравим прикладом є надмірна увага до важких побічних ефектів або смерті вакцинованих осіб після вакцинації в окремих випадках, навіть якщо немає доказів, що це пов'язано з вакциною. Без належного досвіду такі публікації можуть бути «правдивими», але вони завадять вакцинації людей.

Інтерпретація дезінформації як форми агресії не стосується критики – суб'єктивні оцінки «мають найвищий рівень захисту, навіть ті, які здаються більшості людей абсолютно неправильними.

Правила аудиту стали більш гнучкими і швидко змінюються, щоб адаптуватися до нових форматів шкідливого контенту; з одного боку, платформа намагається сприяти поширенню реальної інформації (в тому числі з офіційних джерел), а з іншого боку, більш потужні автоматизовані аудити.

Таким чином, зменшується можливість оскаржити несправедливе автоматичне видалення непомилкової інформації. Подібні дії керівництва соціальних платформ пов'язані з виборами, особливо в США. Приватні компанії стали суддями і можуть самостійно приймати рішення про обмеження свободи слова користувачів. Слід не тільки боротися зі шкідливою інформацією, але й заохочувати різноманітність думок, підтримувати незалежні ЗМІ та пропагувати здорові форми інформації. Насильницьке втручання необхідне лише в деяких сферах, де дезінформація неодмінно завдасть шкоди: порушення прав дітей, пропаганда тероризму та підрив механізмів чесних виборів [22, с. 576].

Найважливіше питання, яке потрібно задати під час поширення неправдивої або дезінформації, — хто її поширює. Якщо країна це зробить, збитки, завдані брехнею, зростуть у десятки чи сотні разів. Особливий випадок - Танзанія, де влада контролює всі ЗМІ, забороняє лікарям згадувати про епідемію коронавірусу і заперечує його існування. Така поведінка створює загрозу основним правам людини – здоров'ю, життю тощо. Однак це приклади неправдивої інформації з боку влади, спрямованої на жителів однієї країни. Він не назвав прізвище для поширення такої дезінформації).

З одного боку, існує ліберальний погляд на свободу слова: мовляв, держава не має бути арбітром істини, вона має створити ринок, де ідеї зустрічаються – неправда та правда, і правда врешті переможе. З іншого боку, ми знаємо, що ринок, в тому числі і ринок ідей, може зруйнуватися і ним можна маніпулювати за допомогою влади та грошей. У реальному житті правда не завжди перемагає брехню. У деяких країнах брехня вже взяла верх.

Держава має право обмежувати діяльність тих, хто поширює шкідливу брехню, але лише тоді, коли це дійсно необхідно, і в рамках національного законодавства для боротьби з дезінформацією – цього в більшості країн немає. Інакше боротьба з дезінформацією може призвести до переслідувань з боку опозиції та мовчання критиків влади.

Найнебезпечнішими є неоднозначні закони, які чітко не визначають дезінформацію та шкоду, яку вона має завдати, щоб обмежити дезінформацію. Держава не повинна обмежувати нереальність лише тому, що вона нереальність. Захист правди сам по собі є неадекватним виправданням. Вони можуть це зробити, якщо поширення неправдивих слів завдає конкретної шкоди особам, і це потрібно підтвердити. Адміністратори ніколи не повинні визначати, що правда, а що брехня. Це функція незалежного суду або незалежного контролюючого органу. Прикладом неприйнятного регуляторного механізму є Сінгапур, де керівники можуть видаляти пости із соціальних мереж.

Свободу слова не можна розглядати як частину проблеми протидії дезінформації, а основу її вирішення.Рішення полягає у створенні середовища, в якому існуватиме та поширюватиметься якісна та правдива інформація. Для цього необхідно забезпечити безпеку журналістів, допомогти незалежним та громадським ЗМІ, покращити комунікацію між державними органами. Держава зобов'язана надавати повну, правдиву та достатню інформацію.

Для України, яка стикається з інформаційною складовою змішаної війни, питання інформаційної безпеки стає все більш актуальним. Річ у тім, що окупація окремих територій України не лише призвела до глобальних порушень міжнародного права та ескалації регіональної та світової напруженості, а й чітко та систематично порушувала права громадян України на цих територіях. , у тому числі мати право знати.

З огляду на це, розвиток та вдосконалення основ інформаційної безпеки України є одним із найважливіших і особливо важливих завдань країни. У той же час багато питань, пов’язаних з інформаційною безпекою, можна успішно вирішити лише шляхом тісної координації та співпраці з міжнародними організаціями (Організація Об’єднаних Націй, Європейський Союз, НАТО тощо).

Враховуючи глобальну загрозу України інформаційній безпеці, справедливо зазначити, що інформаційні можливості (технології та технології та інформаційна психологія) використовуються міжнародними гравцями у світовій політиці, включаючи не лише Росію, а й іноземні спецслужби. , транснаціональні компанії та терористи. організацій, а також окремих терористів і злочинних угруповань), суперечать національним інтересам України (у тому числі інтересам людей і громадян, суспільства і країни та інших об'єктів національної безпеки) та загрожують національній безпеці України. У більшості випадків технології інформаційного тероризму спрямовані на національну безпеку та національну оборону і становлять

реальну загрозу національному інформаційному простору України, створюючи загрозу суверенітету України [21, с. 251].

Тому, враховуючи стійкість українського народу як нації (національну стійкість) до загрози інформаційного тероризму в умовах змішаної війни, необхідно усвідомлювати, що проблема боротьби з інформаційним тероризмом на тимчасово окупованих територіях полягає в реінтеграції інформації про ці території та населення до вітчизняного інформаційного простору.

Виходячи з цього, інформаційний тероризм – це ідеологічно обґрунтована практика впливу, що лякає населення, на прийняття рішення або вчинення дії (бездіяльності) органом влади, органом місцевого самоврядування, міжнародною організацією, соціальною групою, юридичною особою чи фізичною особою в межах інформаційного простору, пов'язаного з використанням інформації, інформаційних технологій та (або) інформаційних ресурсів.

РОЗДІЛ 2. МІЖНАРОДНИЙ ДОСВІД СПІВРОБІТНИЦТВА ДЕРЖАВ У БОРОТЬБІ З ІНФОРМАЦІЙНИМ ТЕРОРИЗМОМ

2.1. Міжнародні інституційні механізми протидії інформаційному тероризму

У свідомості суспільства сутність інформаційного тероризму розкривається через навмисне застосування чи загрозу застосування різних видів насильства щодо цивільних осіб або держави (окремою особою чи групою осіб) у політичних чи релігійних цілях. Тероризм, як і раніше, є серйозною загрозою, у зв'язку з чим стоїть актуальне завдання вжиття рішучих заходів протидії. Питання полягає в тому, які стратегії та правила повинні застосовуватися у боротьбі проти тероризму, та хто має перевіряти дотримання цих правил.

Без якісної правової підтримки боротьба з тероризмом не може бути ефективною. Система правового забезпечення протидії терористичним злочинам має бути побудована таким чином:

– перша група нормативно-правових актів – законодавство та інші нормативно-правові акти, які визначать теорію антитерористичної безпеки та антитерористичної стратегії та слугуватимуть основою протидії злочинам, спрямованим на терористичність;

– другий комплекс нормативно-правових актів - комплекс антитерористичних та пов'язаних з ними актів, покликаних захистити інтереси країни, усього суспільства та окремих осіб, груп і об'єднань, визначити аналіз загрози терористичної діяльності;

– до третього комплекту нормативних законів увійдуть нормативні акти Служби безпеки України, Національної поліції та інших правоохоронних органів, які відображають тактичні аспекти боротьби з терористичними актами та іншими терористичними злочинами.

Дослідження напрямів та проблем удосконалення державної політики в галузі інформаційної протидії тероризму має на меті виявлення позитивного

досвіду, інформаційної протидії тероризму та вироблення пропозицій щодо вдосконалення організаційних основ аналізованої діяльності. Держави мають відігравати значно активнішу роль у забезпеченні ясних та справедливих правил взаємодії в інформаційному полі, як, наприклад, це здійснюється в галузі цивільно-правових відносин. Необхідно правильно скоординувати діяльність законодавчих та правоохоронних органів, щоб одночасно забезпечити міцний правовий фундамент, що задає параметри розвитку інформаційного середовища, та не скувати цей розвиток зайвою регламентацією.

У Європейському Союзі, починаючи з прийняття «Стратегії безпеки 2003 року», проблема тероризму була піднята на пріоритетний рівень, розширивши при цьому контртерористичну політику, яка існувала з середини 80-х років, і посиливши контртерористичні зв'язки зі США. В даний час виділяються три загальні підходи до боротьби з тероризмом, які пов'язані з трьома різними перспективами в цьому питанні [77].

Перший підхід ґрунтується на поліцейській діяльності та розслідуванні, це найпоширеніший метод у Європі. Він відображає концепцію тероризму, засновану на кримінальному підході, згідно з яким тероризм є повторюваним явищем, яке не можна усунути, але воно може переслідуватися та каратися певними правоохоронними методами.

Другий підхід розглядає тероризм як соціальну хворобу і тому прагне виділити її корінні причини, такі як середовище, в якому розвиваються терористичні групи та від якого вони отримують підтримку.

Цей підхід передбачає розвиток довгострокових стратегій, спрямованих на усунення чи згладжування соціальних диспропорцій.

Третій підхід полягає в тому, щоб розглядати тероризм через призму військової аналогії, маючи на увазі застосування сили, що запобігають ударам (у тому числі проти держав, які вважаються такими, що приймають або захищають терористичні організації) та фізичну ліквідацію його

керівництва. У крайніх випадках, як-от глобальний терор, цей підхід може означати широкомасштабну війну [44].

У свою чергу, у Китаї постійний комітет Всекитайських зборів народних представників розглядає проект першого в історії країни закону про боротьбу з тероризмом, який, зокрема, зобов'язує всі іноземні високотехнологічні компанії, які бажають надавати свої послуги на території Китаю, передавати місцевому уряду ключі шифрування та методи. захисту інформації [37].

У 2004 році керівники американського, британського та австралійського антитерористичних центрів оголосили про намір створити єдину інформаційну мережу, яка «дозволить запобігати акціям «Аль-Каїди» та союзним з нею формуванням на всій території земної кулі». В результаті була створена глобальна антитерористична мережа, учасниками якої є: у США – Національний контртерористичний центр, у Великій Британії – Об'єднаний Центр аналізу тероризму, в Австралії – Національний центр розподілу загроз, у Канаді – Об'єднаний центр розподілу загроз, у Новій Зеландії – Спільна група загроз.

У квітні 2007 року тоді ще прем'єр-міністр Тоні Блер представив зовнішньополітичну доктрину Великобританії, де було оголошено про створення «підрозділу, який відповідатиме за розробку стратегії боротьби з ідеологією «Аль-Каїди» та використанням інших форм екстремістської пропаганди ворожими режимами. яка отримала ім'я RICU (Research, Information and Communication Unit). З метою вдосконалення діяльності Євросоюзу у боротьбі з радикалізацією населення з вересня 2011 року функціонує утворена Комісією ЄС «Мережа попередження радикалізації» (The Radicalization Awareness Network – RAN).

Завданням комісії є обмін передовим досвідом, вироблення рекомендацій та методик для практичних працівників, зайнятих у цій сфері. Практична діяльність RAN здійснюється у рамках восьми робочих груп (діяльність правоохоронних органів, запобігання радикалізації, дерадикалізація, «голос» жертв тероризму, інтернет та ЗМІ, робота у

в'язницях із ув'язненими та особами, які перебувають на випробувальному терміні, медичні програми, внутрішні та зовнішні фактори радикалізації) [10].

Особливе місце серед суб'єктів інформаційної протидії тероризму займають недержавні організації та об'єднання, а також громадяни, які сприяють органам державної влади та органам місцевого самоврядування у здійсненні антитерористичних заходів. Безумовно, значну частину завдань інформаційної протидії тероризму здатна і має вирішувати держава, але слід визнати, що вона не може і не повинна безмежно вторгатися у всі ніші життя. На певному рівні подібне вторгнення починає викликати неприйняття та протидію саме собою, навіть якщо воно здійснюється для досягнення шляхетних соціально значущих цілей.

Крім того, абсолютизація держави у протидії тероризму в інформаційній сфері створює передумови використання її компонентів для формування авторитарних засад управління суспільним розвитком, їхнього переростання в тоталітаризм. Аналіз вітчизняної та зарубіжної практики показує, що активне залучення інститутів громадянського суспільства до національної антитерористичної системи дозволить суттєво підвищити ефективність її роботи.

Ретельного вивчення та аналізу заслуговує досвід США та Євросоюзу щодо використання таких форм участі громадянського суспільства у профілактиці тероризму, як: програми освіти громадян; програми стимулювання активності громадян; програми залучення громадян у діяльність із охорони громадського порядку тощо [93].

На сьогодні тероризм набув всесвітнього масштабу, перетворився на багатовимірне і багатоаспектне явище, яке дуже швидко еволюціонує, а отже набуває міжнародного характеру.

Для забезпечення ефективної протидії деструктивному впливу тероризму на глобалізаційні соціально-політичні процеси необхідно

визначити основні засади цієї протидії, що охоплюють усі три рівні правового сегменту політичної системи:

– Нормативний рівень– інститути, принципи та норми;

– Організації антитерористичної протидії;

– Концептуальний рівень (ідеологія).

– Заходи мають бути об'єктивними, вбудованими у систему міжнародного права, і навіть досить конкретними. А саме:

– політичні заходи – досягнення компромісу щодо глобалізаційних процесів, у т.ч. формалізація системи багатополярного світу, розробка системи її правового закріплення, вироблення механізмів більш раціонального цивілізаційного розвитку, ресурсного балансу;

– правові – розвиток міжнародних систем вирішення глобальних та регіональних соціально-політичних конфліктів;

– розробка системи інформаційно-психологічної безпеки, що не допускає непрямих механізмів інформаційно-психологічних воєн; реалізація гнучких критеріїв щодо контролю за оборотом озброєння (у тому числі ядерного, з формалізацією заборони залякування ядерною зброєю як чинника просування політичних інтересів);

– усунення економічних передумов шляхом припинення каналів непрямого фінансування терористичних організацій та їх союзників [41].

Світова спільнота досить чітко усвідомила, що війна з тероризмом не передбачає локальної перемоги у її сенсі у певній хронологічній точці. У цьому вся сенсі терор будь-коли може бути ліквідований повною мірою. Тому характер цієї війни практично не піддається чіткому рамковому визначенню. Проте можна говорити про два основні напрямки її розвитку в сучасному світі: посилення контртерористичного захисту та запобігання та розсинхронізації терористичних атак.

Це включає не тільки збільшення чисельності поліцейських сил, антитерористичних бар'єрів та ефективність розвідки, але й вжиття заходів

щодо запобігання катастрофічних наслідків у світовій та національній економіках у випадках, коли відбувається терористичний напад [95].

2.2. Міжнародно-правове забезпечення боротьби з актами інформаційного тероризму

На початку XXI століття тероризм став однією з найбільших загроз міжнародній безпеці. Процеси глобалізації призвели до інтернаціоналізації тероризму, трансформації його ідеологічної та інституційної бази, значно розширили форми та способи його існування. У зв'язку з цим одним із актуальних завдань для кожної з держав став перегляд комплексу організаційно-правових та інших заходів на національному рівні з метою їх удосконалення, необхідність підвищення рівня взаємодії на двосторонньому, регіональному рівнях, а також активізація діяльності у рамках міжнародної організації у сфері боротьби із тероризмом. Особливого значення набуває також проблема боротьби з фінансуванням тероризму, створенням відповідного правового поля для контролю за фінансовими потоками неурядових, неприбуткових організацій, офшорних зон тощо.

Важливим питанням у сфері боротьби з тероризмом стає формування відповідної нормативно-правової бази та наявність ефективної системи протидії на національному та міжнародному рівнях. У багатьох державах ухвалено спеціальні закони щодо боротьби з тероризмом. Наприклад, діяльність правоохоронних органів та спеціальних служб Великобританії у сфері боротьби з тероризмом регулюється двома основними законами – «Про тероризм» (2000 р.) та «Про антитероризм, злочини та безпеку» (2001 р.) [37].

Характер та особливості сучасного етапу світового розвитку багато в чому зумовлені тим, що поряд із очевидними благами світова інформаційно-технологічна революція, що відбувається нині, сприяє виникненню принципово нових загроз життєдіяльності як окремих суспільств, держав та їхніх громадян, так і світової спільноти загалом. У найбільш загрозливому

вигляді це виявляється у такому явищі, як тероризм, який у ході своєї еволюції більшою мірою, ніж інші суспільно небезпечні прояви, використовує можливості, що надаються інформаційним суспільством [100].

Оскільки тероризм як суспільне явище має вкрай негативну спрямованість, а інформатизація, як явище і процес, охоплює найширші верстви суспільства, то такого роду зміни в характері тероризму, способах та методах поширення терористичної ідеології, шантажу та тиску на політичну владу з боку терористичних організацій є цілком закономірними. Швидкий розвиток інформаційних технологій суттєво розширило можливості терористичних структур не лише з розробки нових технічних інструментів терористичної діяльності, а й щодо створення та широкого застосування технологій маніпулювання свідомістю населення з терористичною метою.

Як зазначалося раніше, терористичні акти призначені задля досягнення різних політичних цілей і, отже, можуть вважатися серйознішими актами, ніж кримінальні порушення. Крім того, кримінальне право може бути надто слабкою «зброєю» для боротьби з тероризмом, оскільки знищення терористичної інфраструктури та мереж потребує дипломатії, застосування сили, широкого набору соціальних, інформаційних, культурних та економічних заходів та кримінального права разом узятих.

Обмеження, закладені в систему кримінального правосуддя, мають сенс у громадянському суспільстві, де фактором є стримування, але це може не мати місця щодо високотехнологічної терористичної організації. Отже, тероризм може сприйматися як феномен, що представляє велику небезпеку, оскільки він набагато охоче, ніж злочинність, може прагнути до досягнення своїх цілей, аж до самопожертви у певних ситуаціях. Кримінальне законодавство при цьому саме по собі не може бути адекватною платформою для боротьби з тероризмом [45].

Першою міжнародної організацією, що апелювала саме до поняття кіберзлочину став Інтерпол (Конференція в Парижі 1979 році). Під час восьмої презентації на тему комп’ютерного шахрайства було зазначено:

«Природа комп'ютерного злочину є міжнародною, оскільки комунікація між різними державами здійснюється через телефони, супутники і т.д. Міжнародні організації, включно з Інтерполом, повинні приділяти цьому більше уваги». Держави-учасниці Інтерполу взяли участь в опитуванні з питань кіберзлочинів рамках Першого навчального семінару Інтерполу з питань розслідування комп'ютерних злочинів в Парижі 7-11 грудня 1981 року. Це опитування дало можливість виявити прогалини в законодавстві з питань комп'ютерних злочинів, які потребують удосконалення правового регулювання. Це стало першим кроком у гармонізації кримінального законодавства у сфері кіберзлочинності державами світу [102].

ОЕСР В 1982 році в Парижі ОЕСР вирішила створити комітет експертів з метою розглянути концепцію комп'ютерних злочинів та проаналізувати потребу реформування кримінальних законів. Результатом роботи комітету став «Аналіз політики ОЕСР з юридичних питань» 1986. Цей Аналіз зазначав: «Відповідно до активізації комп'ютерної злочинності міжнародного характеру, було виявлено важливі питання, які потребують міжнародного співробітництва щодо контролю такої активності та боротьби із незаконними діяннями. Держави-учасниці повинні самі визначити межі, до яких покарання відповідні діяння повинні бути передбачені в кримінальному законодавстві». Крім того, було визначено перелік діянь, за принципом спільного знаменника відповідно до концепцій, які були представлені державамиучасницями. У такий перелік входили: комп'ютерне шахрайство; комп'ютерна підробка документів; шкода, завдана комп'ютерним даним та програмам; неавторизоване посягання на захищені комп'ютерні програми і неавторизований доступ до або перехоплення комп'ютерних систем [65].

Рада Європи 9 В 1985 році Рада Європи призначена комітет експертів з метою розгляду комп'ютерних злочинів. Було розроблено рекомендації для національних законодавців, щодо виключно злочинів міжнародного характеру (Рекомендація № R (89) 9 – 1989 року). Ця рекомендація включала основний рекомендований список комп'ютерних злочинів та факультативний

список. Крім того, 11 вересня 1995 року Радою Європи було прийнято інші Рекомендації, які стосувались питання процесуального права в рамках інформаційних технологій. Ці Рекомендації налічували 7 розділів: розшук і затримання; технологічне спостереження; зобов'язання зі співробітництва органами розслідування; електронні докази; використання encryption; дослідження; статистика та завчання; міжнародне співробітництво [5]

Разом з тим, в окремих державах, зокрема в Австрії, США, Польщі, Швейцарії, Швеції, та інших , немає єдиного (спеціального) закону щодо протидії тероризму. У цих країнах нормативно-правові документи з питань боротьби з тероризмом охоплює низку законодавчих актів. В Ірландії, наприклад, національне законодавство у сфері боротьби з тероризмом укладено в актах «Про злочини проти держави», ухвалені протягом 1939–1998 років. В даний час на затвердженні Нижньої палати парламенту знаходиться спеціальний закон "Про кримінальну відповідальність за терористичні злочини" (The Criminal Justice and Terrorist Offences Bill). Ухвалення цього закону допоможе Ірландії приєднатися до низки конвенцій ООН щодо протидії тероризму. У Фінляндській Республіці нормативно-правова база з питань боротьби з тероризмом охоплює окремі статті Кримінального кодексу та низку законів щодо боротьби з незаконними антигромадськими проявами, спрямованими проти безпеки цивільної авіації, морської навігації, збереження та використання ядерних матеріалів тощо [94].

У Словаччині основним законодавчим актом із питань протидії тероризму також є Кримінальний кодекс. Основними нормативно-правовими актами, якими регулюється діяльність спеціальних структур у Швейцарії щодо протидії тероризму та його фінансуванню, є Кримінальний кодекс, а також Федеральний закон «Про заходи щодо забезпечення внутрішньої безпеки» та низку розпоряджень уряду.

У США також не існує єдиного всеохоплюючого закону, спрямованого виключно на боротьбу з тероризмом. Події 11 вересня 2001 р. спонукали

керівництво цієї держави до вдосконалення правової бази у сфері боротьби з тероризмом та усунення прогалин у федеральному законодавстві. З цією метою було прийнято низку законодавчих актів, спрямованих на розширення повноважень правоохоронних органів при розслідуванні кримінальних злочинів, пов'язаних із тероризмом та посиленням боротьби з відмиванням «брудних грошей».

Вищезазначеними актами передбачено: створення Міністерства внутрішньої безпеки як головного органу у боротьбі з тероризмом та Групи оцінки ризику біотероризму; імплементацію конвенцій ООН у сфері боротьби з тероризмом; здійснення низки заходів щодо фінансового заохочення розвитку антитерористичних технологій; порядок відшкодування збитків, завданих терористичними актами; а також посилення заходів щодо охорони державного кордону та системи видачі перевірки віз, запровадження системи біометричного контролю при в'їзді на територію США [50, с. 226].

У листопаді 2001 р. уряд ФРН затвердив Закон «Про боротьбу з міжнародним тероризмом» (другий антитерористичний пакет федерального уряду). Його основною метою є зміна більшості положень німецького законодавства, що стосуються безпеки громадян та правил перебування на території країни іноземців для того, щоб закріпити додаткові повноваження та розширити компетенцію силових відомств для захисту населення. Законом передбачено внесення змін до 14 законодавчих та підзаконних актів. Одним із ключових пунктів згаданого пакету є ухвалення Закону «Про головного свідка», який передбачає пом'якшення покарання співучасникам злочину у разі надання ними достовірної інформації про подальші заплановані злочини. У такий спосіб правоохоронні органи ФРН прагнуть отримувати попереджувальну оперативну інформацію про підготовку можливих терористичних актів, виявляти конспіративні квартири, затримувати екстремістів, які ховаються на території ФРН [50, с 227].

В Індії, згідно із законом, прийнятим у березні 2001 р., злочини, пов'язані з терористичною діяльністю або пособництвом терористам,

караються позбавленням волі на строк від п'яти років, а в окремих випадках застосовується виключна міра покарання – смертна кара. Поліції відповідно до закону, прийнятого у 2001 р., надано право без пред'явлення звинувачень затримувати підозрюваних для допиту на строк до 90 діб, а за рішенням суду затримання може бути продовжено ще на 90 діб. Федеральним законом «Про боротьбу з терористичними злочинами» Об'єднаних Арабських Еміратів передбачено довічне ув'язнення або страту особам, які організовують, фінансують або керують угрупуваннями, метою яких є вчинення терористичних актів. Довічному ув'язненню або тривалим термінам ув'язнення підлягають особи, які займаються вербуванням, навчанням чи іншою підготовкою бойовиків для терористичних груп. Законом передбачено, що «терористичним актом» вважається дія чи бездіяльність, що призводить до вчинення одноосібного чи колективного терористичного акта щодо глав держав та урядів, офіційних осіб державних установ чи урядових, міжнародних організацій та членів їх сімей. Поняття «терористичний акт» охоплює також дії щодо заподіяння шкоди державній та приватній нерухомості та рухомій власності, природним ресурсам.

У Франції внесено зміни до низки законів, що доповнили перелік злочинів, які можуть кваліфікуватися як терористичні (зокрема акти екологічного тероризму – забруднення атмосфери, надр, води тощо шкідливими для людського здоров'я чи тваринного світу речовинами). Термін давності у справах, порушених за статтею «тероризм», становить 30 років.

Тому, ґрунтуючись на визначенні тероризму в рамках існуючої системи норм і законів, які вже включені в міжнародні конвенції та прийняті більшістю країн світу, спільнота має досягти нового рівня міжнародної взаємодії як основного інструменту у спільній боротьбі з тероризмом.

Можна дійти висновку, що проблемі інформаційного обміну у рамках ООН згодом стала приділятися достатню увагу, а норми міжнародного права,

що його регламентують, демонструють явний прогрес, зокрема завдяки зусиллям конкретних органів системи ООН.

Прикладом реальних результатів практичної роботи країн у напрямі зміцнення антитерористичного співробітництва на регіональному рівні вважатимуться діяльність Антитерористичного центру СНД (АТЦ СНД). Це спеціальний постійно діючий галузевий орган СНД, завдання якого досить широкі саме в плані інформаційного обміну, серед них: – аналіз інформації, що надходить, про стан, динаміку та тенденції поширення міжнародного тероризму та інших проявів екстремізму в державах — учасницях СНД та інших державах; – формування з урахуванням об'єднаного банку даних органів безпеки, спеціальних служб та інших компетентних органів країн — учасниць СНД [45].

Отже, зі сказаного видно, що тероризм став ключовим аспектом у дебатах безпеки. Це порушує низку проблем, по-перше, щодо можливого поєднання загроз (терористичні атаки в мережах, таких як енергетичні мережі та постачальники енергії, такі як атомні електростанції, використання комп'ютерів тощо).

І, по-друге, щодо форм співробітництва у сфері антитерористичної боротьби. Різні підходи до цього питання призводять до того, що різні суб'єкти вирішуватимуть його по-різному, але очевидно, що певна політика щодо цієї загрози безпеці є необхідним компонентом стратегії забезпечення безпеки в цілому.

Так, «інформаційна протидія тероризму» у досить категоричній формі дає зрозуміти, що інформаційна протидія здійснюється у повному обсязі всім складовим такого явища, як «тероризм» – і на практиці впливу, і на ідеології насильства. Поняття «протидія ідеології тероризму» у разі говорить саме себе.

РОЗДІЛ 3. ШЛЯХИ УДОСКОНАЛЕННЯ МЕТОДІВ ПРОТИДІЇ ІНФОРМАЦІЙНОМУ ТЕРОРИЗМУ В УКРАЇНІ

3.1. Сучасний стан державно політики у сфері інформаційної безпеки в Україні

Процес глобалізації та всебічної інформатизації суспільства справив значний вплив на зміст і форму сучасної інформаційної війни. У свою чергу, це 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 вимагає визначення інноваційних методів формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного потоку інформації.

В умовах всебічної інформизації суспільства всі сфери суспільного життя все більше залежать від інформаційних факторів, і необхідно постійно вдосконалювати методи та засоби ефективної реалізації державної політики щодо забезпечення інформаційної безпеки. З метою захисту та реалізації національних інтересів, державного управління процесами у внутрішньому, міжнародному та світовому інформаційному просторі є нагальною потребою та необхідною умовою захисту країни та суспільства.

Це також можна пояснити тим, що міжнародні та глобальні політичні суб'єкти часто використовують інформаційні можливості для таких цілей і суперечать національним інтересам України (що включають інтереси таких об'єктів національної безпеки, як людина і громадянин, суспільство та держава) та загрожують національній безпеці України [71, с. 50].

В умовах російсько-українського конфлікту захист національного інформаційного простору від негативних інформаційно-психологічних впливів, дій і воєн, забезпечення інформаційної безпеки та інформаційного

суверенітету набули особливої актуальності, а також стали фактором збереження національної ідентичності України та реалізації її суверенітету.

Сучасна політика публічної інформаційної безпеки визначається пріоритетом національних інтересів, системою небезпек і загроз і реалізується шляхом впровадження відповідних теорій, стратегій, концепцій, програм в інформаційній сфері відповідно до чинного законодавства.

Інформаційна безпека є невід'ємною частиною національної безпеки і розглядається як пріоритетна функція країни. З одного боку, інформаційна безпека надає громадянам якісну вичерпну інформацію та вільний доступ до різноманітних джерел інформації, а з іншого — контролює поширення дезінформації, сприяє соціальній цілісності, захищає інформаційний суверенітет, бореться з негативною інформацією та психологічною пропагандою, і захищає національний інформаційний простір, вільний від маніпуляцій, інформаційних війн та операцій [40].

Вирішення комплексного питання інформаційної безпеки сприятиме захисту інтересів суспільства та країни, захисту прав громадян на отримання вичерпної, об’єктивної та якісної інформації.

Сутністю інформаційної безпеки є стан захищеності інформаційного простору України, при якому спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп’ютерні злочини та інший деструктивний інформаційний вплив не завдає суттєвої шкоди національним інтересам [43, с. 14].

Тому пріоритетними напрямами сучасної державної політики щодо забезпечення інформаційної безпеки України мають бути: забезпечення інформаційного суверенітету України, створення стандартизованих правових та економічних передумов для розвитку інформаційної інфраструктури та ресурсів країни, впровадження новітніх технологій у цій сфері, створення уніфікованих правових та економічних передумов для розвитку інформаційної інфраструктури та ресурсів впровадження новітніх технологій

у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активне залучення ЗМІ до запобігання і протидії корупції, зловживанням службовим становищем, іншим явищам, які загрожують національній безпеці України; забезпечення неухильного дотримання конституційних прав на свободу слова, доступ до інформації, захист персональних даних, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність ЗМІ та журналістів, заборони цензури, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції, за виконання професійних обов'язків, за критику; вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України.

З огляду на процес інтеграції України до міжнародної системи інформаційної безпеки, завданням є формування національної політики інформаційної безпеки як регіонального безпекового просторового кластера загальної системи міжнародної безпеки, безумовно, з урахуванням реалізації відповідних національних інтересів (недопущення інформаційної експансії, ефективної координації дій з іноземними партнерами, побудови відкритого інформаційного суспільства, інтеграції у глобальний інформаційний простір та ін.).

Забезпечення інформаційної безпеки України - є спільною справою української держави та українського народу, що крізь призму публічної політики в Україні формує один з її напрямів В умовах глобальних та регіональних інформаційних протиборств сьогодення, деструктивних комунікативних впливів, зіткнення багатогранних національних інформаційних інтересів, поширення інформаційної експансії з боку. агресора, захист національного інформаційного простору та гарантування інформаційної безпеки набувають особливої актуальності та пріоритетності.

Під інформаційною безпекою розуміють: формування національного законодавства щодо інформаційної політики, створення відповідно до

законодавства України можливостей для забезпечення інформаційної адекватності рішень органів державної влади, громадян та об’єднань громадян, інших юридичних осіб в Україні, гарантування свободи інформаційної діяльності та доступу до інформації.

До інформації в українському національному інформаційному просторі Повноцінний розвиток інформаційної структури, підтримка використання досягнень науки і техніки та особливостей духовного та культурного життя українського народу для розвитку національних інформаційних ресурсів України, створення та впровадження безпечних інформаційних технологій; захист прав власності всіх учасників української національної космічної інформаційної діяльності, захист інформаційної бази України

Національна власність на стратегічні цілі об'єктів, захист державної таємниці та обмежений доступ до інформації, що є об'єктом права державної власності або єдиною об'єкти, що перебувають у власності, користуванні чи розпорядженні держави; створення загальної системи захисту інформації, зокрема захисту державної таємниці та іншої інформації з обмеженим доступом; захист національного інформаційного простору України від викривлень чи поширення заборонених законодавством України інформаційних продуктів; прийняття законів до встановити систему доступу іноземних держав або їх представників до національних інформаційних ресурсів України та порядок використання цих ресурсів відповідно до договорів з іноземними державами [54].

Необхідно наголосити, що сучасні виклики інформаційної безпеки України зумовлені як внутрішніми, так і зовнішніми чинниками: внутрішні - найбільшою мірою пов'язаних з відсталістю інформаційних технологій в Україні від провідної країни світу, низьким рівнем інформатизації, розпорошеністю повноважень органів державної влади та законодавства в інформаційній сфері зовнішні - загальносвітові тенденції створення та застосування інформаційних технологій та спроб іноземних суб'єктів впливають на світовий та вітчизняний інформаційний простір із

забезпеченням власних інтересів, залежність від іноземного програмного забезпечення.

Також, увага до проблем інформаційної безпеки України зумовлена антиукраїнськими впливами, які пропагують ідеї сепаратизму, насильства, національного ворожнечі та спробами руйнування національної ідентичності України, знищення міжнаціональних злагод, посягання на конституційний лад України, територіальну цілісність держави. Україна актуалізується в умовах війни на сході, коли з боку Російської Федерації відбувається інформаційна експансія, упереджене та тенденційне висвітлення фактів і явищ, а технології російських інформаційно-психологічних операцій спрямовані на забезпечення домінування в українському (а також у глобальному) інформаційному просторі та на утриманні медійної переваги. Через російські пропагандистські інформаційно - психологічні кампанії, акції, медіазаходи впливають не лише на суспільну свідомість громадян України, а й на світову громадськість.

Представник об'єднання «Інформаційний спротив» В. Гусаров, досліджуючи проблему інформаційної безпеки України, наголошує, що Росія створює інформаційно-психологічні атаки, щоб активізувати ескалацію конфлікту на сході України, чинити тиск на українське керівництво з метою змусити погодитися на його «московський» сценарій урегулювання конфлікту.

В. Гусаров виокремлює напрями інформаційно-психологічних атак проти України: нав'язування думок про неспроможність влади керувати державою та приймати раціональні рішення; формування негативних суджень про воєнно-політичне керівництво України та про те, що хаотичні бойові дії призводять до невиправданих жертв серед сил ООС; поширення поглядів про те, що українська армія на Сході України деморалізована та неспроможна вести бойові дії, а також про недовіру особливого складу до керівництва; нав'язування думки про те, що Україна не обійдеться без російського газу та що сторонам необхідно повернутися для перегляду

газових контрактів. Експерт позначає, що цільовою аудиторією Кремля зараз є населення РФ, російськомовна діаспора за кордоном, населення України, зокрема в окупованих районах Донбасу, громадяни західних країн, а також країн БРІКС та Митного союзу, сусідні Росії за політичними поглядами [15].

Україна стала мішенню інформаційно-психологічних впливів, дій, воєн, її інформаційна безпека знаходиться під загрозою. Необхідно пояснити, що український інформаційний простір не зазнає впливу зовнішньої негативної пропаганди та маніпуляцій, а став об'єктом інформаційної експансії, у світовому медіапросторі немає українського національного інформаційного продукту, який би поширював об'єктивно, справедливо та ефективно. - актуальні відомості про українські події. Як наслідок, міжнародне співтовариство не має інформації або отримує інформацію з інших джерел, які іноді вводять в оману, надають оманливу, спотворену та неповну інформацію.

Водночас проти України активно застосовується потужний медіаресурс, здійснюється експансія іноземних суб'єктів на ринку інформаційних послуг, активізуються негативні інформаційні впливи, які спрямовані на викривлення реальності, заниження міжнародного іміджу держави; діяльність вітчизняних ЗМІ щодо систематичного, об'єктивного висвітлення фактів, подій та явищ є недостатньою та позбавлена стратегічного планування; інформаційно-комунікативна політика України у сфері національної безпеки потребує невідкладного перегляду та удосконалення [13].

Найбільші проблемні напрямки подальшого розвитку «цифрової» частини української економіки потребують правових інновацій та перегляду національної регуляторної політики: розвиток механізмів захисту інтелектуальної власності, стимулювання та підтримка виробництва IT-стартапів, інновацій та виробництва кінцевого продукту «Зроблено в Україні»; систематично залучати інвестиції IT-індустрії, просувати українські IT-продукти на зовнішніх ринках.

На жаль, національному інформаційному простору України загрожують серйозні виклики, які становлять небезпеку діяльності держави, її політичному та економічному розвитку, інтеграції в Європу та євроатлантичні структури.

На цьому етапі Україна має зосередитися на двох основних напрямках: модернізації, безпеці, структурній цілісності та конкурентоспроможності внутрішнього простору України, забезпеченні існування інформації країни у світі та сприянні її позитивному іміджу.

Інформаційна безпека має базуватися на моделі стратегічного мислення: на основі принципів демократії, прав людини та безпечного Інтернету. Слід вживати заходів для захисту, підтримки цілей та забезпечення безпеки. У той же час інформаційна безпека є невід'ємною частиною розвитку інформаційного суспільства. Розвиток інформаційного суспільства має досягатися не лише за рахунок вдосконалення технічних можливостей обміну інформацією, а й через глибоке розуміння різних суб'єктів інформаційного суспільства. інформаційні відносини. Тому такі питання, як інформаційна етика, захист конфіденційності в інформаційному суспільстві, запобігання впливу маніпуляцій з інформацією, почали включати до актуальних питань інформаційної безпеки.

Сьогодні практично всі сфери суспільного життя певною мірою безпосередньо зачіпаються учасниками інформаційної політики всіх рівнів. В умовах посилення впливу інформаційного потоку на реалізацію життєво важливих інтересів особи, суспільства та країни від ефективного управління інформаційним полем держави залежить стан і динаміка практично всіх показників якості державного управління.

Сьогодні у Верховній Раді діють чотири комітети, які займаються питаннями свободи слова, регулювання ЗМІ, інформаційної політики та іншими сферами, пов’язаними із медійною сферою. Серед них: Комітет з питань гуманітарної та інформаційної політики; Комітет з питань свободи слова; Комітет з питань цифрової трансформації; Комітет з прав людини,

деокупації та реінтеграції тимчасово окупованих територій у Донецькій, Луганській областях та Автономної Республіки Крим, міста Севастополя, національних меншин і міжнаціональних відносин [48].

Міністерство культури та інформаційної політики України є основним органом центральної системи органів виконавчої влади у сфері національного мовлення, інформаційного суверенітету України (у частині повноважень щодо управління всім майновим комплексом Українського державного інформаційного агентства "Укрінформ"), інформаційної безпеки, поширення суспільно важливої інформації в Україні та за її межами, а також забезпечення функціонування державних інформаційних ресурсів. Все це являє собою беззаперечне прагнення держави до пошуку шляхів провадження вітчизняної публічної політики в інформаційній сфері, політичні процеси, які реалізуються в публічному просторі, підтримуються інформаційно –комунікаційними ресурсами та представлені комплексом прозорих вертикальних і горизонтальних взаємодій його учасників. Публічна політика є специфічною формою комунікації суб'єктів політичного процесу, яка дає змогу активізувати участь громадян у її виробленні та реалізації політичних рішень» [39].

Іншим органом виконавчої влади є Міністерство цифрової трансформації України, до складу якого входить Національне агентство електронного урядування Міністерство освіти бачить зареєстровану взаємодію (сумісність). Агентство співпрацює з іншими державними органами, органами місцевого самоврядування та міжнародними партнерами, щоб забезпечити взаємодію - принцип, що різні інформаційні ресурси можуть взаємодіяти один з одним на основі єдиних інтерфейсів та угод.

Результати роботи міністерства з оцифровки можна розглядати як потужну базову платформу для розгортання телекомунікаційних компонентів для забезпечення ефективного розвитку інформаційної безпеки України. Звісно, РНБО відіграє координаційну роль як відповідний державний орган.

Іншими словами, якщо глобалізація визначає свої правила на світовій арені через соціальну оцифровку, чому б не використати свої переваги у сфері інформаційної безпеки нашого українського суспільства, створивши сучасний національний простір та розгорнувши технічні складові українського суспільства? Механізм захисту інформації.

Таким чином, діяльність із інформаційної безпеки, здається, інтегрована в сучасну цифрову трансформацію через свої завдання.

Крім того, національне агентство спеціального зв'язку та захисту інформації має вибирати окремо від органів виконавчої влади у сфері ЗМІ [53].

Національна комісія з телебачення і радіомовлення також відіграє певну роль у системі органів виконавчої влади. Держкомтелерадіо є головним органом центральної системи виконавчої влади, який бере участь у забезпеченні формування та реалізації державної політики у сферах телебачення і радіомовлення, інформації та видавничої справи.

До органів зі спеціальним статусом у медійній сфері можна віднести Національну раду з питань телебачення і радіомовлення [51] Зокрема, Національна рада здійснює розробку та нагляд за виконанням ліцензійних умов, нагляд за дотриманням законодавства у сфері кінематографії, дотриманням законодавства щодо частки національного продукту, виконанням телерадіоорганізаціями законодавства у мовних питаннях, питаннях захисту суспільної моралі тощо. Як регулятор, у межах своїх повноважень цей орган може застосовувати санкції до порушників.

Крім того, ще одна установа – Рада національної безпеки і оборони України [161], яку очолює Президент України. Відповідно до Конституції України та Закону про РНБО України до складу координаційного органу входять керівники профільних міністерств та інші посадові особи. Повноваження відомства поширюються на інформаційне поле, в тому числі на можливість здійснення інформаційної діяльності за масштабами

потенційних та реальних загроз національним інтересам (за оцінкою Комісії національної безпеки і оборони).

До установ зі спеціальним статусом також належать дві установи, які діють під керівництвом Президента України – Комітет з питань свободи слова та захисту журналістів [60] та Державна комісія з нагляду у сфері зв'язку та інформатизації [57].

Тож, певна система органів влади щодо виявлення та аналізу загроз інформаційної безпеки України, вироблення і вживання заходів, необхідних для адекватної відповіді на них в державі створена. Разом з тим, ефективно протистояти інформаційним загрозам у сучасних умовах може лише добре організована державна система забезпечення інформаційної безпеки, що повинна здійснюватися при повній взаємодії всіх державних органів, недержавних структур і громадян [17] Слід констатувати, що всі ці виклики і загрози, а також наявність систематизованих у законодавчому полі визначень і понять і, на їх основі, роз'яснень вказують на те, що забезпечення інформаційної безпеки України є одним із пріоритетних напрямів сучасної вітчизняної публічної політики.

При цьому, формування національних безпекових спроможностей в інформаційній сфері передбачає розроблення комплексного нормативного документа щодо проведення спеціальних інформаційних операцій, передбачивши узгодження понятійного апарату, визначення профільних структурних підрозділів державних органів та їх завдань і повноважень у мирний, воєнний час. На сьогодні, такого документа ще не зрозроблено.

Як контратаку проти психологічних наслідків, дій та війн широкомасштабної негативної інформації пріоритетними напрямками та важливими кроками державної політики української влади мають бути: інтеграція України у світовий та європейський регіональний інформаційний простір; інтеграція в міжнародну інформацію. , інформаційно-телекомунікаційні системи та організації; створення власної національної моделі інформаційного простору для забезпечення розвитку інформаційного

суспільства; модернізація всієї національної системи інформаційної безпеки та формування та реалізація ефективної інформаційної політики; удосконалення законодавства з інформаційної безпеки, гармонізація національного законодавства з міжнародними стандартами та ефективно впроваджувати інформаційні процеси.

Правовий нагляд; розвиток національної інформаційної інфраструктури; підвищення конкурентоспроможності вітчизняних інформаційних продуктів та інформаційних послуг; впровадження сучасних інформаційно-комунікаційних технологій у публічно-адміністративні процедури; формування, впровадження та коригування національних політики в інформаційній сфері з боку органів державної влади та інститутів громадянського суспільства [35, с. 18].

З метою запобігання поширенню інформації діяльність держави в інформаційному просторі має здійснюватися в таких аспектах: впроваджувати превентивні заходи та тактику (превентивні заходи); впроваджувати контрзаходи (швидке реагувати на інформаційні атаки противника та проактивні атаки); захищати національний інформаційний простір. Головна мета – забезпечити домінування інформаційного простору та перевагу ЗМІ. Крім того, першочерговими завданнями інформаційної структури державних органів мають бути: контроль над інформаційними потоками, надання об’єктивної та вичерпної інформації, надання професійних коментарів та роз’яснень щодо подій, а також система охоплення посадових посад чиновників та політичних лідерів.

Підсумовуючи аналіз ситуації з інформаційною безпекою України, можна відзначити, що національний інформаційний простір України знаходиться під серйозними загрозами, які загрожують діяльності країни, політичному та економічному розвитку країни, інтеграції в Європу та євроатлантичні структури, враховуючи стихійне поширення сучасних телекомунікацій. Для забезпечення ефективної державної політики забезпечення інформаційної безпеки держава має активно брати участь у

впорядкуванні інформаційних продуктів, що розповсюджуються за допомогою телекомунікацій, пріоритетом державної політики щодо забезпечення внутрішньої інформаційної безпеки має бути відповідне вдосконалення інформаційного законодавства. Представники інформації України у сприятливих сферах, громадськість та Участь ЗМІ покращує інформацію, але не існує механізму безпеки, спрямованого на запобігання, запобігання та боротьбу зі злочинністю. Інформаційне середовище, наприклад боротьба з інформаційним тероризмом.

3.2. Правові засади забезпечення інформаційної безпеки в Україні у протидії інформаційному тероризму

Підходячи до аналізу вітчизняного законодавства у сфері інформаційної безпеки, неозброєним оком можна побачити різноманітність спеціального законодавства та загального законодавства, нормативно-правового забезпечення.

Практичний досвід у сфері боротьби з тероризмом за останні кілька років показує, що методику аналізу вітчизняного антитерористичного законодавства можна розділити на два етапи: До 2014 року більшість антитерористичних операцій в Україні здійснювалися по пунктах. А після 2014 року Україна провела у східній частині країни масштабну антитерористичну операцію, яка в квітні 2018 року переросла в спільну військову операцію Об’єднаних сил.

Розглянемо основні закони України у сфері антитерористичної підтримки через призму протидії інформаційним загрозам. Так, Законом України «Про боротьбу з тероризмом» [52] визначено, що антитерористичні операції – це низка узгоджених дій відповідних розвідувальних органів та правоохоронних органів на певній території, які обмежені у часі та в контрзаходах.

З 2014 року Закон України «Про боротьбу з тероризмом» зазнав серйозних змін – до цього часу його переглядали 27 разів. Це дає змогу не лише розглядати антитерористичні операції як діяльність спецслужб та правоохоронних органів, а й реалізовувати низку заходів, реалізація яких покладена на багато вітчизняних правоохоронних органів, органів державної влади та місцевого самоврядування, в межах їх повноважень. Законом вперше передбачено правовий механізм, який дозволяє українським збройним силам і спецназу брати участь у боротьбі з тероризмом з метою усунення загроз національній безпеці.

Закон України «Про боротьбу з тероризмом» визначає терористичні дії: «діяльність, яка охоплює:

– планування, організацію, підготовку та реалізацію терористичних актів;

– підбурювання до вчинення терористичних актів, насильства над фізичними особами або організаціями, знищення матеріальних об'єктів у терористичних цілях; організацію незаконних збройних формувань, злочинних угруповань (злочинних організацій), організованих злочинних груп для вчинення терористичних актів, так само як і участь у таких актах; вербування, озброєння, підготовку та використання терористів;

– пропаганду і поширення ідеології тероризму;

– фінансування та інше сприяння тероризму» [52].

На сучасному етапі основними реальними та потенційними загрозами інформаційної безпеки України є:

1. У сфері зовнішньої політики:

– поширювати у світовому інформаційному просторі викривлену, недостовірну та упереджену інформацію, що завдає шкоди національним інтересам України;

– прояви комп'ютерної злочинності та комп'ютерного тероризму, що загрожують стабільній та безпечній роботі національних інформаційно-телекомунікаційних систем;

– зовнішній негативний інформаційний вплив на обізнаність населення через ЗМІ та Інтернет;

2. У сфері державної безпеки:

– негативні інформаційні впливи, спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності і недоторканності кордонів України;

– використання засобів масової інформації, а також мережі Інтернет для пропаганди сепаратизму за етнічною, мовною, релігійною та іншими ознаками; несанкціонований доступ до інформаційних ресурсів органів державної влади; розголошення інформації, яка становить державну та іншу передбачену законодавством таємницю, а також конфіденційної інформації, що є власністю держави;

3. У воєнній сфері:

– порушення встановленого регламенту збирання, обробки, зберігання і передачі інформації з обмеженим доступом в органах військового управління та на підприємствах оборонно-промислового комплексу України;

– несанкціонований доступ до інформаційних ресурсів, незаконне збирання та використання інформації з питань оборони;

– реалізація програмно-математичних заходів з метою порушення функціонування інформаційних систем у сфері оборони України;

– перехоплення інформації в телекомунікаційних мережах, радіоелектронне глушіння засобів зв'язку та управління;

– інформаційно-психологічний вплив на населення України, у тому числі на особовий склад військових формувань, з метою послаблення їх готовності до оборони держави та погіршення іміджу військової служби;

4. У внутрішньополітичній сфері:

– недостатня розвиненість інститутів громадянського суспільства, недосконаліть партійно-політичної системи, непрозорість політичної та

громадської діяльності, що створює передумови для обмеження свободи слова, маніпулювання суспільною свідомістю;

– негативні інформаційні впливи, в тому числі із застосуванням спеціальних засобів, на індивідуальну та суспільну свідомість;

– поширення суб'єктами інформаційної діяльності викривленої, недостовірної та упередженої інформації [42].

Відсутність чіткого законодавства щодо застосування Збройних Сил України у кризових ситуаціях призвело до вирішення всіх аспектів їхньої участі у боротьбі з тероризмом. Крім того, досить гостро стоїть питання використання озброєння та військової техніки, особливо використання літаків, кораблів та внутрішніх суден, що яскраво продемонстрували дискусії в ЗМІ у 2014 році.

Закон визначає відповідальність організацій за терористичні дії та порядок притягнення терористичних організацій до відповідальності.

Тому все це має призвести до розвитку антитерористичної інформаційної складової, тобто боротьби з інформаційним тероризмом та поглиблення та стандартизації організацій та правових механізмів у цій сфері. Проте, як ми бачимо, основні антитерористичні документи країни у відповідь на інформаційний тероризм поки що не змінилися. Інформаційний тероризм визначається через його відповідність поняттю технологічного тероризму. Технологічний тероризм – це використання електромагнітних засобів, комп’ютерних систем і мереж зв’язку для прямого чи опосередкованого створення або загрози аварійними загрозами через ці дії, створення ризиків для людей, населення та навколишнього середовища або створення умов для аварій та техногенних катастроф.

У статтях 15 і 17 закону визначено фактори, які залучають до проведення антитерористичних операцій для взаємодії з громадськістю, а також встановлені стандарти заборони ЗМІ повідомляти інформацію про форми і методи проведення антитерористичних операцій

Тобто в основних законах країни у сфері боротьби з тероризмом ми бачимо слабку детермінацію, тому законодавство не впливає на визначення дій та повноважень, наданих антитерористичним суб'єктам по боротьбі з тероризмом для здійснення ними практичних дій у справі боротьби з інформаційним тероризмом.

Єдине, що має значення, це те, що відповідно до статті 51 Статуту Організації Об'єднаних Націй та Статуту Міжнародного Суду [75] та/або в умовах воєнного чи надзвичайного стану відповідно до Конституції України [31] та законодавства України.

Якщо основні антитерористичні закони країни не дають чітких відповідей на наші запитання, то, можливо, відповідь криється в інших правових актах?

Тому статтею 17 Конституції України визначено, що інформаційна безпека є «одною з найважливіших функцій держави і справою всього українського народу». Відповідно до Конституції України, Агентством з координації національної безпеки і оборони під керівництвом Президента України є Рада національної безпеки і оборони України, функцією якої є «внесення пропозицій Президентові України щодо реалізації засад внутрішньої і зовнішньої політики у сфері національної безпеки і оборони, координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони у мирний час та координація та здійснення контролю за діяльністю органів виконавчої влади у сфері національної безпеки і оборони в умовах воєнного або надзвичайного стану та при виникненні кризових ситуацій, що загрожують національній безпеці України» [56].

З метою використання наявних ресурсів у стані телекомунікаційної мережі для прийняття ефективних оперативних управлінських рішень у надзвичайних ситуаціях, надзвичайних ситуаціях та воєнному стані, особливо для задоволення потреб управління, оборони та безпеки Указу Президента України від 28.02.2015 № 115/2015 в р. Українська держава

Внесено до рішення Комісії з безпеки і оборони від 25 січня 2015 року «Про створення та функціонування Головного ситуаційного центру в Україні» [61].

Практика показує, що сферу інформаційної безпеки України також необхідно будувати на координаційній ролі РНБО України На жаль, сьогодні в цьому напрямку фактичний рівень реалізації цих заходів є дуже низьким, хоча Комісія національної безпеки і оборони України активно працює над впровадженням заходів щодо координації охоронної діяльності навколо інформаційного простору. Це підтверджують багато регуляторних рішень, а саме:

1. 30 березня 2015 року прийнято Указ Президента України №184 «Про рішення РНБО України від 12 березня 2015 року «Про стан подолання негативних наслідків, спричинених втратою матеріальних носіїв секретної інформації на тимчасово окупованій території України, в районі проведення антитерористичної операції в Донецькій та Луганській областях» [62]. Навіть із самої назви нормативного акту можливо дійти висновку про втрату не просто вагомої для України інформації, а моа йде про втрату відомостей (інформації), що відігравали певну роль у забезпеченні національної безпеки України.

2. 25 лютого 2017 року набрав чинності Указ Президента України № 47 «Про рішення Комісії національної безпеки і оборони України про засади інформаційної безпеки України від 29 грудня 2017 року» [61]. Безпека в системі національної безпеки, з одного боку, як складова частина різних сфер національної безпеки, з іншого боку, як важлива самостійна сфера забезпечення національної безпеки. Ця доктрина має на меті «визначити інноваційні методи формування системи захисту та розвитку інформаційного простору України в умовах глобалізації та вільного потоку інформації», а також «визначити національні інтереси України в інформаційній сфері, загрози його реалізації та Напрямки та пріоритети інформаційної політики країни». Важливим нововведенням цієї доктрини є чітке визначення трьох основних напрямів національної політики щодо забезпечення інформаційної

безпеки України: технологічний розвиток, захист інформації та інформаційна психологія, особливо створення сприятливої психології в національній інформаційній космос Атмосфера. У сучасній загрозі національній безпеці України ця доктрина визначає «інформаційну перевагу країни-агресора на тимчасово окупованих територіях». Ця доктрина викликала різну реакцію експертів, починаючи від визнання її важливості і впевненості, що документ мав бути прийнятий кілька років тому, до порівняння цього документа з аналогічними доктринами інформаційної безпеки, прийнятими Російською Федерацією в грудні 2016 року.

3. 15 березня 2016 року Президент України прийняв рішення КНБО України від 27 січня № 96/2016, яким було сформульовано більш глибоку позицію щодо сил сектору безпеки та оборони для реагування на кризову ситуацію в Україні. кіберпростір, 2016 «Про стратегію кібербезпеки України» [170]. Аналіз документа показує, що національна система кібербезпеки має передусім забезпечити співпрацю державних органів, органів місцевого самоврядування, військових, правоохоронних органів, науково-дослідних установ, навчальних закладів, громадських організацій та суміжних відомств з питань кібербезпеки. Підприємства, установи та організації, які здійснюють діяльність у сферах електронних комунікацій та захисту інформації та/або є власниками (розпорядниками) критично важливої інформаційної інфраструктури, незалежно від форми власності. Практика реалізації цієї стратегії свідчить, що вона носить суто декларативний характер.

4. Іншим декларативним документом, який досі фактично не виконано, є Указ Президента України від 14 березня 2016 р. № 92/2016 про рішення Ради національної безпеки і оборони України від 4 березня 2016 р. «Про концепцію розробка звіту про сектор безпеки та оборони України» [59]. За його словами, план реформування та розвитку Збройних сил України здійснюється в рамках єдиного підходу до формування обороноздатності країни та забезпечення її провідної ролі у виконанні завдань національної

оборони. Концепція передбачає створення необхідних матеріально-технічних резервів для повноцінного реагування на всі виклики та загрози разом з іншими складовими сектору безпеки та оборони, забезпечення можливості реагування на інформаційні, кібератаки, спецоперації противника, активну участь у міжнародна миротворча та безпекова діяльність. Крім того, концепція передбачає, що основною метою реформування та розвитку сектору безпеки та оборони є нарощування та підтримання спроможностей, які забезпечать повне та гнучке реагування на весь спектр загроз національній безпеці України та раціональне використання. наявних можливостей і ресурсів. Для ефективного розвитку сектору безпеки та оборони в сучасних умовах найбільш перспективними є забезпечення ефективної координації та функціонування національної системи реагування на кризи, удосконалення національної системи прогнозування та стратегічного планування на основі принципів і стандартів ЄС та НАТО, та використання військ (військ) Планування системи та засобів управління безпеки та оборони, а також налагодження та підтримання співпраці з відомими міжнародними організаціями та країнами з метою усунення негативних наслідків прямих, нетрадиційних, змішаних та інших агресивних поведінки щодо України.

5. Наступним нормативно-правовим актом у сфері інформаційної безпеки держави є Воєнна доктрина України, яка є «системою поглядів на причини виникнення, сутність і характер сучасних воєнних конфліктів, принципи і шляхи запобігання їх виникненню, підготовку держави до можливого воєнного конфлікту, а також на застосування воєнної сили для захисту державного суверенітету, територіальної цілісності, інших життєво важливих національних інтересів». Нажаль, документ дійсно є лише системою поглядів... Серед основних завдань воєнної політики України також визначено:

- удосконалення державної інформаційної політики у воєнній сфері;
- попередження та ефективна протидія інформаційно-психологічним

впливам іноземних держав, спрямованим на підрив обороноздатності, порушення суверенітету і територіальної цілісності України, дестабілізацію внутрішньої соціально-політичної обстановки, провокування міжетнічних та міжконфесійних конфліктів в Україні.

6. У березні 2019 року Президент України затвердив «Концепцію України щодо боротьби з тероризмом». Концепція спрямована на вдосконалення національної системи боротьби з тероризмом, враховуючи сучасні загрози національній безпеці України від тероризму та прогнозуючи його розвиток. Концепція також визначає мету можливого терористичного акту, який також включає «...інформаційний простір та його складові». Важливим завданням, зазначеним у документі, є необхідність удосконалення інституційних механізмів координації діяльності суб'єктів боротьби з тероризмом.

7. Запобігання терористичній діяльності передбачає вирішення низки завдань, серед яких: удосконалення організаційно-правової бази боротьби з тероризмом, підвищення рівня координації діяльності антитерористичного центру Агентства безпеки України щодо діяльності суб'єктів боротьби з тероризмом; налагодження ефективної взаємодії між антитерористичними органами та іншими державними органами, в основному шляхом впровадження сучасних форм, методів і технологій отримання, обробки та використання інформації для покращення інформаційно-аналітичного забезпечення заходів протидії терористичній діяльності.

Також, слід звернути увагу на Указ Президента України від 14 вересня 2020 року, яким РНБО України від 14 вересня 2020 року № 392/2020 «Про Стратегію національної безпеки України» [59]. В ньому зафіксовано погляди уряду на загрози національній безпеці та шляхи мінімізації (або усунення) цих загроз.

Нова стратегія прийшла на зміну документу 2015 року, який був прийнятий у контексті стрімких змін військово-політичної ситуації –

тривалої агресії Росії та задоволення потреб у нових умовах. Це стосується і сфери інформаційної політики та інформаційної безпеки – однієї з важливих сфер Російської Федерації для боротьби зі змішаною агресією. Стратегія 2015 року визначила дві ключові загрози в цій сфері: розгортання інформаційної війни проти України та відсутність в країні цілісної комунікаційної політики (недостатній рівень культури соціальних медіа). Хоча пріоритети національної політики у цій сфері загалом правильні, вони все ще мають значною мірою декларативний характер. Нова стратегія висуває багато важливих моментів і прояснює питання, які принципово не змінюють ракурс компонентів безпеки, а уточнюють їх.

У статті 4 викладені нові основні принципи стратегії: стримування, стабільність і взаємодія. Це стало зразком розвитку всього сектору безпеки та оборони. Крім того, безпека мережі також привертає велику увагу. У пункті 63 згадується про необхідність «завершити створення національної системи кібербезпеки, встановити наявні можливості учасників кібербезпеки та кіберзахисту, посилити їх систему координації». Слід визнати, що попередня версія стратегії була більш конкретна щодо супутніх завдань зміцнення національної кібербезпеки, хоча це не вплинуло на реальність її реалізації. Деталі місії нової стратегії мають з’явитися в оновленій українській стратегії кібербезпеки. Слід зазначити, що конкретні методи реалізації, зазначені в стратегії, стануть зрозумілішими з 15 документів підстратегії, два з яких – Стратегія інформаційної безпеки та Стратегія кібербезпеки – безпосередньо пов’язані з інформаційними компонентами. Наскільки цим документам вдасться запропонувати не так ефектні, як ефективні засоби протидії ворожій активності, залежить і те, наскільки новоприйнятий стратегічний документ стане дієвим інструментом планування, а не формальною бюрократичною відпискою.

Аналізуючи вищезазначені рішення РНБО України, приходить розуміння, що ці рішення мають суто декларативний характер і не знайшли відображення в більш чітких документах (наприклад, плані його

реалізації).Очевидним є певна правова інформаційна безпека та боротьба з інформаційним тероризмом у цій сфері.

Тому в «Законі України «Про Концепцію Національної програми інформатизації» проголошується, що «інформаційна безпека є частиною політичної, економічної, національної оборони та інших компонентів національної безпеки» [55]. Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» визначає поняття «інформаційна безпека» - це «...стан захисту життєво важливих інтересів людей, суспільства та країни». , і запобігає заподіянню шкоди з таких причин: неповнота, несвоєчасність та недостовірність використовуваної інформації; негативний інформаційний вплив; негативний вплив використання інформаційних технологій; несанкціоноване поширення, використання та порушення цілісності, конфіденційності та доступності інформація» [63]. В українському «інформаційному» законі немає визначення поняття «інформаційна безпека» [64]. «Закон про національну безпеку України», який є основним орієнтиром забезпечення безпеки нашої держави, сутність «інформаційної безпеки» подано як невід'ємний складник національної безпеки України без точного визначення цього поняття [59]. сфера національної безпеки і оборони та покладає відповідні функції на службу безпеки України (ст.19) [64] і Державну службу спеціальної зв'язку та захисту інформації України (ст.22) [53] щодо загальності боротьби з інформаційним тероризмом, то вказується, що норми фахових відомств з цього питання є лише повторами, а підвищення юридичної ефективності в цих аспектах не спостерігається, а питання про відокремлення окупованих загалом немає. територій та реінтеграції інформації.

Як бачимо, ці документи дають лише загальне визначення терміну «інформаційна безпека», до того ж вони не узгоджуються між собою. Проте ці документи не містять системного підходу до української інформаційної безпеки, не визначають суб’єкта інформаційної діяльності та не розподіляють між ними повноваження.

У той же час питання кібербезпеки підлягають більшому нагляду. Тому «Основні принципи забезпечення української кібербезпеки» є однією з кількох розробок у напрямку протидії загрозам кіберпростору.

Вітчизняні законодавці окремо виділили український закон «Про основні засади забезпечення кібербезпеки України» [56]. У ньому було введено поняття кібертероризму — «терористичної діяльності, що здійснюється в кіберпросторі або з його використанням». Беручи до уваги цей закон, можна вважати, що кіберпростір – це середовище (віртуальний простір), яке надає можливості для спілкування та/або зв'язків з громадськістю, і формується в результаті функціонування сумісних (підключених) комунікаційних систем та електронних комунікацій з використанням Інтернету або інших глобальних даних в мережі.

Намагаючись об'єднати законодавчі терміни, спрямовані на роз'яснення можливості антитерористичної діяльності в інформаційній сфері, можна спростити її до поняття «інформаційний тероризм – терористична діяльність, спрямована на тимчасове чи безповоротне зняття інформації з експлуатації за допомогою різних форм і методів». Інфраструктура та її елементи, а також цілеспрямоване використання цієї інфраструктури для створення умов, які будуть мати катастрофічні наслідки для всіх сторін життя суспільства та країни, включаючи використання різноманітних методів і засобів для всіх сторін людського суспільства».

На жаль, ефективність українських організацій та правових механізмів у боротьбі з інформаційним тероризмом сьогодні базується на інформаційному тероризмі та контрзаходах, які чітко не визначені вітчизняним законодавством.

Тому 28 січня 2016 р. було прийнято рішення Державного управління радіомовлення, кіно і телебачення No 101 «Про внесення змін до Плану розвитку національного телерадіоінформаційного простору» [54].

Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 10.06.2008 р. № 94 затверджено «Порядок

координації діяльності органів державної влади, органів місцевого самоврядування, військових організацій, підприємств, установ та організацій незалежно від форм власності щодо запобігання, виявлення та усунення наслідків несанкціонованих дій на національні інформаційні ресурси в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [55].

Метою цієї програми є організація координаційних заходів щодо запобігання вразливостям інформаційної безпеки в ІТС, виявлення та усунення наслідків інших несанкціонованих дій щодо публічних інформаційних ресурсів в ІТС, а також впровадження єдиної програми координації інформації в ІТС. Делегування та/або спроба виконання несанкціонованих операцій над ресурсами інформації про стан в ІТС. Однак цей документ не визначає механізму координації реагування на інформаційні загрози.

Відповідно до розпорядження Кабінету Міністрів України від 20.06.2018 р. № 442-р. аналізується поточна стратегія розвитку оборонно-промислового комплексу України до 2028 року та враховується відсутність національної стратегії громадської безпеки та захисту громадян. в Україні. Зроблено невтішний висновок, що на законодавчому рівні не вистачає творчих можливостей, а отже, фактично відсутні національні механізми реалізації державної політики щодо забезпечення інформаційної безпеки України.

Особливого розгляду потребує законодавство про боротьбу з інформаційним тероризмом у східній частині нашої країни.

Протягом цього періоду українська влада прийняла низку законів та інших нормативно-правових актів для впровадження існуючих та започаткування нових засобів та умов для досягнення майбутнього відділення та реінтеграції окупованих територій. Безперечно, до визначень належать: «Мінська угода», український закон «Про особливий порядок місцевої автономії в окремих районах Донецької та Луганської областей» [58], український закон «Про особливості національної політики»

забезпечують Національний суверенітет України на тимчасово окупованій Донецькій та Луганський територіях. Це ключовий законодавчий акт щодо окупованих територій. Хоча в ньому не йдеться про інформаційний тероризм чи вплив інформації на боротьбу з Росією, на них необхідно звернути увагу, оскільки їхні норми визначають, що мислення громадян, які проживають на території Україна контролює (не тільки це), що впливає на ступінь їх схильності до українського маршруту та ступінь їх ворожості до політики Російської Федерації.

Закон України «Про національну безпеку Україні» визначає принципи національної політики у сфері національної безпеки та національної оборони, зокрема забезпечення військової, зовнішньої політики, держави, економіки, інформаційної, екологічної безпеки, мережевої безпеки тощо.

Закон також визначає склад сектору безпеки і оборони: «Міністерство національної оборони України, Збройні Сили України, Державна спеціальна служба транспорту, Міністерство внутрішніх справ України, Національна гвардія України, Національна поліція України, Державна прикордонна служба України, Державна міграційна служба України, Державна служба України з надзвичайних ситуацій, Служба безпеки України, Управління державної охорони України, Державна служба спеціального зв'язку та захисту інформації України, Апарат Ради національної безпеки і оборони України, розвідувальні органи України, центральний орган виконавчої влади, що забезпечує формування та реалізує державну військово-промислову політику» [61].

Українські «Основні принципи кібербезпеки в Україні» визначають національну систему кібербезпеки як сукупність суб'єктів кібербезпеки, у тому числі Державне агентство спеціального зв'язку та захисту інформації України, Національну поліцію України, Агентство безпеки України, Міністерство національної оборони, та Генерального штабу Міністерства Збройних Сил України, Управління розвідки України та Національного банку України. Проте законом визначено, що координацію національної системи

кібербезпеки здійснює Національний координаційний центр кібербезпеки України через спеціально створену робочу організацію – РНБО.

Такий підхід певною мірою збільшує ланцюжок управлінських рішень у національній системі протидії інформаційному тероризму, але також передає координацію однієї зі складових боротьби з інформаційним тероризмом (інформаційних технологій) Комісії національної безпеки і оборони України. Виключити внутрішній антитерористичний механізм Служби безпеки України. У координації інформаційно-технічної складової боротьби з інформаційним тероризмом відбувається своєрідна децентралізація законодавства між різними державними органами. У зв'язку з цим, шляхом більш глибокого аналізу, ми сміливо припускаємо, що український закон «Основні принципи української кібербезпеки», загалом виглядає неефективною концепцією боротьби України з кіберзагрозами.

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

Слід зазначити, що в умовах стрімкого поширення глобалізації макроекономічного простору збільшується можливість впливу інформації на окремих людей, суспільства та країни. Безперервне широкомасштабне поширення інформації сприяє поширенню на великі території в найкоротші терміни. Хоча це і вважається одним із важливих досягнень людства, воно все ж має свої недоліки, оскільки глобалізація інформатизації збільшила можливості інформаційних загроз. Інформаційна ера розширила сферу інформаційно-комунікаційної війни, що призвело до появи інформаційного тероризму як засобу інформаційної війни, що поєднує процес роздвоєння фізичного тероризму, пов'язаний з інформаційними системами та свідоме зловживання кіберпростором, мережами або їх компонентами, з метою сприяння здійсненню терористичних операцій.

Факти свідчать про те, що інформаційний тероризм набув нової форми загрози, причиною його швидкого поширення є активізація соціального зомбування та сепаратистських рухів, що в кінцевому підсумку може призвести до втрати національного суверенітету, незалежності та територіальної цілісності.

На думку експертів НАТО, «гібридна операція» скоординована за цілями, завданнями, місцем і часом і має на меті здійснити необхідний вплив на країну без прямого і явного застосування сили [28].

Механізм формування та реалізації українськими науковцями національної політики у сфері боротьби з інформаційним тероризмом не був повністю розглянутий або висвітлений при розробці проблем інформаційної безпеки України, а також боротьби з тероризмом в цілому. Тому у вітчизняному науковому середовищі майже немає узагальнюючих праць, що значно збільшує вирішення практичних проблем у формуванні та реалізації державної політики у сфері боротьби з інформаційним тероризмом.

Прогрес у національних інформаційних контрзаходах, у тому числі з урахуванням конфлікту на сході України, незначний, в основному через невдоволення існуючою моделлю систем національної інформаційної політики та нормативного забезпечення.

Українським ЗМІ не вистачає фінансування та безперервного процесу становлення, що в свою чергу призведе до нерозвиненості корпоративних традицій та «шкіл», надмірної залежності від поточних умов ведення бізнесу, недостатнього професіоналізму журналістів, низької якості контенту, слабкості громадського мовнику та неефективність мережі державних телерадіоорганізацій, мінімальна можливість інтеграції на благо країни.

Законодавча база України у сфері інформаційної безпеки, особливо у сфері боротьби з інформаційним тероризмом, має велику кількість документів, але більшість з них не мають певного правового статусу. Положення, що містяться в них, не відображені у вітчизняному законодавстві, а знайшли своє відображення у У фактичних діях, що

розуміються під конкретно визначеним суб’єктом, інформаційної діяльності (у тому числі правового суб’єкта антитерористичної діяльності) відсутня. У законодавстві немає заходів, спрямованих на боротьбу з суб'єктами інформаційного тероризму.

Навпаки, реалізація інформаційних технологій та інформаційної психології є явно незбалансованою та фрагментарною (іншими словами, відокремлюючи та «фазуючи» інформаційне протистояння та мережеву безпеку), що знижує ефективність інформаційного протистояння.

У країні відсутній комплексний національний механізм координації діяльності у сфері боротьби з інформаційним тероризмом.

Ретельне вивчення роботи вітчизняних спецслужб, до повноважень яких відносяться завдання протидії інформаційній агресії, вказує на вкрай низьке ресурсне їх забезпечення, а реалізація їх функцій на низькому рівні та часто дублюється у практичних заходах.

У боротьбі з інформаційним тероризмом взаємодія влади, ЗМІ та суспільства носить малоконструктивний характер, що виявляється в хаотичних, неузгоджених і неактуальних діях.

Тому слід зазначити, що сформулювати спільні профілактичні, профілактичні та спеціальні кримінально-правові, адміністративно-правові, організаційно-економічні, технічні та технічні заходи щодо боротьби з інформаційним тероризмом важко. Вищезазначена ситуація яскраво проявляється у слабкому та неефективному інформаційному протистоянні інформаційній агресії на сході України та забезпеченні практичних заходів щодо реінтеграції інформації на окупованих територіях.

Тому безпосередня постановка питання «формування та реалізації державної політики боротьби з інформаційним тероризмом в Україні та організаційно-правових засад» є актуальною на сьогоднішній день. Тобто вибір нашої тези зумовлений гострою потребою розвивати українські теорії державної політики, на основі наукової раціоналізації вдосконалювати діяльність суб'єктів її реалізації [4, с.414].

Отже, відповіддю на питання про організаційно-правові основи формування та реалізації державної політики боротьби з інформаційним тероризмом в Україні є створення та розгляд перспективної моделі комплексного механізму боротьби з інформаційним тероризмом, за результатами чого наукова думка повинна відобразити своє послідовне бачення означених процесів у практичній реалізації вітчизняного державотворення.

Комплексний механізм боротьби з інформаційним тероризмом в Україні має включати інституційно-правові та методичні ресурси. Іншими словами, враховуючи цей механізм, ми повинні чітко визначити сферу дії так званої структури-учасника (або суб'єкта, який має боротися з інформаційним тероризмом), а також має забезпечити чітко визначену нормативну базу для її діяльності (включаючи механізми нормативної координації), Ресурси (людські ресурси, фінансові ресурси, матеріали тощо), а також чітко визначити процес його діяльності (запуск механізму в дію, взаємодія між собою, тощо).

З 1998 року створена, законодавчо закріплена та впроваджена на базі національних інституцій, відіграє свою роль і розвивається національна антитерористична система «під прапором» Антитерористичного центру Служби безпеки України. Проте експерти ООН та НАТО схвально відгукувалися про систему боротьби з тероризмом України на початку 2000-х років. Вони вважали її зразковою та запропонували поширити цей позитивний досвід у створенні механізмів координації та управління на інші країни, але це не означає її ідеальність і не заперечує наявність проблем у даний час. З часом будь-яка система потребує вдосконалення та розвитку.

Вітчизняна антитерористична система охоплює необхідний набір повноважень, сукупність правових, політичних, соціально-економічних, пропагандистських, функцій, правоохоронних та інших можливостей, таким чином будуючи ефективний національний механізм боротьби з тероризмом.

Відповідно до Закону України «Про боротьбу з тероризмом», Служба безпеки України [47] є основним органом національної системи боротьби з терористичною діяльністю [7, с. 230]. Для виконання цієї функції Агентством безпеки України створено постійно діючу організацію – Антитерористичний центр, який відповідає за координацію діяльності антитерористичних суб'єктів, запобігання терористичним актам проти політиків, критично важливих закладів життєзабезпечення, підвищеної небезпеки. об'єкти, загрожуючи життю великої кількості людей [18].

Законом чітко визначено суб'єктів, які безпосередньо здійснюють антитерористичні операції або можуть брати участь у антитерористичних операціях у межах своїх повноважень: Служба безпеки України, МВС України, Національна поліція, Міноборони України, Центральний орган виконавчої влади, що реалізує державну політику у сфері цивільного захисту та центральний орган виконавчої влади, що реалізує державну політику у сфері охорони кордону, центральний орган виконавчої влади, що реалізує державну політику у сфері кримінального покарання, Національне агентство захисту України , центральний адміністративний орган реалізує державну податкову політику та виконує кримінальні покарання, Міністерство національного захисту України, центральний орган виконавчої влади, що реалізує державну податкову політику, державну політику у сфері національної митної справи, центральний орган виконавчої влади реалізує національну податкову політику політики у сфері запобігання та протидії легалізації доходів, одержаних злочинним шляхом, або фінансуванню тероризму (відмиванню грошей), Бюро зовнішньої розвідки України.

Крім того, інші центральні та місцеві органи виконавчої влади, органи місцевого самоврядування, підприємства, установи та організації незалежно від їх належності та форми власності, їх посадові особи та громадяни можуть брати участь у антитерористичних операціях за їхньою згодою.

Іншими словами, чинне антитерористичне законодавство України жодним чином не обмежує коло та юридичні можливості суб'єктів, які

можуть брати участь у боротьбі України з тероризмом. При цьому законом визначено, що боротьба з тероризмом ґрунтується на принципі всебічного використання правових, політичних, соціально-економічних, пропагандистських та інших можливостей. Це означає, що всі вищезазначені суб'єкти боротьби з тероризмом в Україні мають об'єднатися, використовуючи особливий комплекс своїх правових, політичних, соціально-економічних, пропагандистських, функцій та інших можливостей.

Визначення цього «набору можливостей» вимагає організатора та вимог, а його налаштування необхідні для його створення та функціонування. На це питання відповідає і закон [18]: боротьба з тероризмом ґрунтується на принципі єдиного управління силами і засобами, які беруть участь у антитерористичних операціях. Відповідно до закону, антитерористичний центр координує боротьбу з тероризмом, а конкретні антитерористичні операції очолює керівник антитерористичного центру Служби безпеки України (якщо операція проводиться в регіоні, її очолює керівник координуючого органу). Так що організатор дуже чіткий.

Щодо можливостей, то закон визначає антитерористичний центр та його міжвідомчий координаційний комітет (включаючи керівника антитерористичної служби) та антитерористичний орган (на регіональному рівні - регіональна схема: регіональна координаційна група з числа регіональних підрозділів суб'єктів боротьби з тероризмом). Під час проведення антитерористичної операції в законі були прописані права посадових осіб, причетних до операції.

Отже, національний антитерористичний механізм має чітку простежуваність (діяльність антитерористичних суб'єктів знаходиться на чіткому законодавчому рівні, а людські, фінансові та матеріальні ресурси, залучені до антитерористичної діяльності, регулюються відповідним законодавством кожного контртерористичної діяльності. - терористична служба). -терористичні утворення) тероризм). Кожна тема боротьби з тероризмом). Нинішній антитерористичний механізм країни «активується»

розгортанням антитерористичних операцій (згідно з положеннями Кримінального кодексу України).

Керівництво антитерористичною операцією здійснює оперативний штаб, до складу якого входять Міжвідомчий координаційний комітет управління повітряним рухом, центральний штаб, регіональна координаційна група та її штаб за масштабами терористичного акту. Завдання та алгоритми роботи Оперативного штабу визначаються рішенням Кабінету Міністрів України.

Оцінка діяльності та діяльності Антитерористичного центру як координуючого органу показує, що створення Центру є дуже ефективним вибором, який може мобілізувати наявні сили країни та організувати їх для цілеспрямованого використання та управління в боротьбі з тероризмом. Національний механізм боротьби з тероризмом в Україні дуже простий, практичний та ефективний, а його структура здатна швидко реагувати на терористичні виклики та загрози [19].

Таким чином, підхід України до боротьби з інформаційним тероризмом полягає в реформуванні існуючої внутрішньої системи боротьби з тероризмом — розподіл цієї діяльності як окремого компонента загальної внутрішньої системи боротьби з тероризмом. З моменту заснування у 1998 році система заходів, сформульована системою управління повітряним рухом при Раді Безпеки України, безперечно є ефективною, оскільки її функції та готовність є превентивними та можуть адекватно реагувати на терористичні загрози. Перевагою цієї системи є її низька вартість, а завдяки надійній організації та механізму координації управління вона може найбільш ефективно використовувати наявні можливості правоохоронних органів та інших центральних органів виконавчої влади [34, с. 18].

Як ми бачимо, існуюча вітчизняна антитерористична система, яка координується органами управління повітряним рухом Ради Безпеки України, за умови реформування організаційно-правового забезпечення, очевидно, є основою для реалізації ефективної державної політики в Україні. Україна. У цьому напрямку в Україні.

Тому для створення перспективної моделі комплексного механізму боротьби з інформаційним тероризмом в Україні, тобто його нормативно-правової складової, це поняття має бути включено до чинного Закону України «Про боротьбу з тероризмом».

У свою чергу, це стане основою для змістовного наповнення іншої антитерористичної нормативної бази в Україні та вжиття активних заходів щодо боротьби з інформаційним тероризмом (тобто будемо брати участь у стандартизації відповідних законодавчих дій суб'єктів антитерористичної діяльності). інформаційна та інші пов'язані з національною інформаційною безпекою Нагляд та правове забезпечення (концепції, принципи тощо та плани впровадження)).

Законодавство щодо інформаційної безпеки розподіляється між уповноваженими суб'єктами для забезпечення виконання завдань у цій сфері в межах їх функціональних сфер. Хоча українські законодавці реагують на сучасні інформаційні виклики, шкода, що нормативна база не отримала змістовного змісту про активні заходи боротьби з інформаційним тероризмом. З огляду на координуючу роль головного органу УВС України у боротьбі з інформаційним тероризмом, законодавство неминуче призведе до вироблення єдиного комплексного підходу до всіх складових вітчизняного антитерористичного механізму.

Тому вдосконалення існуючої структури антитерористичної системи України полягає у створенні та виділенні окремого поля для боротьби з інформаційним тероризмом. Не порушуючи встановленої та існуючої структури національного антитерористичного механізму, його реформування передбачає виділення окремої ролі як інституційної складової комплексного механізму боротьби з інформаційним тероризмом України, тобто суб'єктів боротьби з інформаційним тероризмом.

Цей метод також дозволить національному механізму боротьби з інформаційним тероризмом вийти на належний та ефективний сучасний рівень управління - як частина національного механізму боротьби з

інформаційним тероризмом, його завданням є координація повсякденної діяльності та управління інформаційною антитероризмом. Дія та розвиток та забезпечення вищого національного керівництва мають необхідні можливості для боротьби з інформаційним тероризмом. Крім того, інформаційні антитерористичні операції можуть проводитися як окрема операція, так і в складі більш складної та більш масштабної антитерористичної операції [36].

Тому для забезпечення виконання та виконання завдання боротьби з інформаційним тероризмом потребує модернізації структура штабу Контртерористичного центру при Агентстві безпеки України. Як виконавча робоча організація центру, штаб здійснює поточну організаційну роботу, виконує покладені на управління повітряним рухом завдання та відповідно визначає функції штабу. Крім того, слід звернути увагу на функції штабу щодо організації науково-методичної роботи з удосконалення форм і методів антитерористичної діяльності. Тому для впровадження сучасного, ефективного та необхідного сучасного національного антитерористичного механізму необхідно оптимізувати структуру штабу управління повітряним рухом.

Сприятливою реакцією на ці виступи вважалося створення окремого підрозділу під керівництвом начальника штабу в штабі. Аналізувати діяльність суб’єктів боротьби з інформаційним тероризмом та вносити пропозиції щодо вдосконалення їх діяльності у встановленому порядку, сформулювати концептуальні засади та плани боротьби з інформаційним тероризмом, висувати пропозиції щодо підвищення ефективності заходів щодо виявлення та ліквідації інформаційного тероризму. Причини та умови здійснення інформаційного тероризму; навчання на тему боротьби з інформаційним тероризмом (плани, методи, навчання та виховання); підготовка та проведення антитерористичних операцій в інформаційному полі, сили та засоби, необхідні для цього. мета боротьби з інформаційним

тероризмом Участь, взаємодія з представниками громадських організацій, ЗМІ, громадянами з питань боротьби з інформаційним тероризмом [92].

Такі підрозділи, які взаємодіють з головним органом боротьби з інформаційним тероризмом, іншими державними органами, представниками засобів масової інформації, громадськими організаціями та окремими громадянами, повинні формувати та забезпечувати організаційно-правові основи реалізації, функціонування та функціонування державної політики боротьби з інформаційним тероризмом. в Україні. Розвиток національних механізмів протидії, інформаційного тероризму.

Завдяки двом складовим, координатор повинен формувати роль і позицію кожного суб'єкта, який здійснюватиме боротьбу з інформаційним тероризмом у загальній національній системі: перша — необхідна конкретна нормативно-правова база; друга — спільна організація і проведення практичних заходів протидії інформаційному тероризму.

Наступною розробкою першої складової штабу Антитерористичного центру Служби безпеки України з боротьби з інформаційним тероризмом є узагальнення, реорганізація та вдосконалення вітчизняного законодавства щодо боротьби з інформаційним тероризмом. Необхідно визнати той факт, що сьогодні в Україні немає дієвого та практичного законодавства щодо боротьби з інформаційним тероризмом. Через призму інформаційної психології інформаційного тероризму та складових інформаційних технологій аналіз перших кількох розділів чинного законодавства виявляє досить насичену, але неструктуровану «національну управлінську картину процесу реагування на інформаційні загрози». Новоствореному штабу АТЦ необхідно на законодавчому рівні закріпити поняття інформаційного тероризму, модернізувати діюче законодавство, створити нормативно-правову базу для правової діяльності національного механізму боротьби з інформаційним тероризмом.

У цій роботі повинні брати участь фахівці з боротьби з тероризмом та експерти з науковим потенціалом. Більше того, дослідження, проведені

школами в країні та за кордоном, показують, що існує величезний потенціал для наукових досліджень у сфері інформаційної безпеки. Одним словом, механізм формування та реалізації українськими науковцями національної політики у сфері боротьби з інформаційним тероризмом не був повністю розглянутий або висвітлений при розробці проблем інформаційної безпеки України, а також боротьби з тероризмом в цілому.

Тому у вітчизняному науковому середовищі майже немає узагальнюючих праць, що значно збільшує вирішення практичних проблем у формуванні та реалізації національної політики у сфері боротьби з інформаційним тероризмом.

Щоб пояснити зміст управлінської модернізації національного механізму боротьби з інформаційним тероризмом, необхідно насамперед зрозуміти його природу та завдання. Щодо суті, то, підсумовуючи, очевидно, що національний лідер (Президент України) повинен якомога швидше дізнатися про загрози національній безпеці, в тому числі тероризм, щоб швидко приймати управлінські рішення. Тому реалізація місії має забезпечити механізм управління національним механізмом боротьби з інформаційним тероризмом: ефективність інформаційного потоку; цілісність обробки інформації; своєчасне реагування на зміни та отримання додаткової інформації; інформація оцінюється настільки ж комплексно, як можливе; в сучасних умовах приймаються ефективні управлінські рішення та вчасно доводяться підлеглим; контроль за чітким виконанням управлінських рішень; забезпечуються вжиття заходів щодо координації підлеглих сил [83].

Цифрова трансформація покращить оперативні можливості для концентрації та участі в необхідних силах і засобах контртерористичних суб’єктів (наприклад, шляхом усунення неправдивої та спотвореної інформації або реагування шляхом надання точної та об’єктивної інформації громадськості). Тому потужна платформа автоматизації телекомунікаційного аналізу інформації може бути використана як технічний компонент інформаційної антитерористичної системи управління інформацією.

До речі, це відповідає положенням Указу Президента України № 379/99, затвердженого Указом Президента України № 379/99 щодо Регіонального агентства Контртерористичного центру Агентства безпеки України та його координаційної групи. згідно з яким АТЦ має право створювати та використовувати спільну автоматизовану інформаційну систему [84].

Звісно, необхідно розробити технічну складову, що включає систему управління інформаційною антитерористичною інформацією, тобто платформу аналізу інформації та телекомунікаційної автоматизації для суб'єктів, які беруть участь у боротьбі з інформаційним тероризмом. Платформа є так званим технічним інструментом створеного Україною адміністративного підрозділу національного механізму боротьби з інформаційним тероризмом, від якого певною мірою залежить ефективність прийняття управлінських рішень національного керівництва у боротьбі з тероризмом в Україні. розвитку.

Крім того, оскільки зрозуміла логіка побудови компонента технології управління, очевидно, що він органічно інтегрований в систему ситуаційних центрів, очолюваних головним ситуаційним центром України, який діє при РНБО №115/2015 [65, с. 72]. Тобто, не витрачаючи великих коштів на побудову окремого антитерористичного інформаційного центру, його готовий Український ситуаційний центр GSC можна розмістити для підтримки координації інформаційного антитерористичного центру та координаційного центру.

Разом з тим, як зазначалося вище, відповідно до Закону України «Про боротьбу з тероризмом», у разі потреби та з законних підстав керівник АТЦ вносить РНБО України пропозицію про введення надзвичайного стану в Україны чи окремі місцевостях. При цьому механізм координації та управління боротьбою з інформаційним тероризмом органічно реалізований в більш глобалізованій системі, тобто в головному ситуаційному центрі України, як програмно-апаратний комплекс для збору, накопичення та

обробки інформації, необхідної для підготовки та прийняття рішень у сфері національної безпеки і оборони.

З організаційної точки зору створення штаб-квартири АТЦ окремого управління, що взаємодіє з головним органом боротьби з інформаційним тероризмом та іншими національними установами, створило інформаційно-технологічну платформу вищезгаданого національного механізму боротьби з інформаційним тероризмом. медіа, соціальні. Представники груп та громадян забезпечуватимуть ефективне функціонування організаційно-правової бази національного механізму боротьби з інформаційним тероризмом, а координація діяльності основного органу боротьби з інформаційним тероризмом здійснюватиметься його загальною системою. Проводити антитерористичні розвідувальні роботи.

Крім того, штаб АТЦ зможе підготувати узгоджені інформаційно-аналітичні матеріали, варіанти прогнозування розвитку терористичної кризи та варіанти прийняття рішень для швидкого прийняття національними лідерами. Слід пам’ятати, що управління повітряним рухом «відповідно до його місії подає рекомендації керівнику центру, приймає рішення про вжиття заходів щодо запобігання та придушення терористичних актів і продовжує вживати таких заходів у разі потреби» [65].

Крім того, в контексті побудови демократичного суспільства в Україні та процесу європейської інтеграції цей метод посилить реалізацію політики державного управління та виведе на більш ефективний рівень ще одну функцію АТЦ: здійснення у встановленому порядку контактів з засобами масової інформації і громадськістю, участь у попереджувально-профілактичних заходах антитерористичної спрямованості, що, безумовно, призведе не тільки до інформування та підготовки населення до дій в умовах загрози або вчинення терористичного акту, а й до спільної взаємодії з питань профілактики тероризму, у тому числі інформаційного.

У контексті реформування системи боротьби з тероризмом в Україні розглядається інформаційно-технологічна складова (як ресурсна складова

механізму боротьби з інформаційним тероризмом) в Україні. Для того, щоб висвітлити процес боротьби з інформаційним тероризмом, слід також наголосити на удосконалення аналітичної складової прийняття управлінських рішень. Впровадження нового підрозділу Штабу АТЦ при СБ України забезпечить виконання іншої функції. За професійним рівнем склад підрозділу повинен бути спроможним організувати такі заходи для подальшої реалізації діяльності.

Міжвідомчою координаційною комісією і Керівником АТЦ наступні заходи: надавати правову оцінку діяльності, організовувати збори членів МКК відповідно до рішення керівника штабу; в країні (або в окремих регіонах) запроваджувати відповідні рівні терористичної загрози та давати рекомендації; сформулювати та надати вищому керівництву країни необхідні варіанти рішень щодо боротьби з інформаційним тероризмом; здійснення комплексу попередніх дій для приведення в готовність сил і засобів суб'єктів боротьби з інформаційним тероризмом; рішення про підготовку до інформаційної антитерористичної операції (за однією з трьох вищенаведених ситуацієм). У необхідних випадках підрозділом вносяться пропозиції щодо введення відповідного ступеня готовності для суб'єктів, що безпосередньо проводять боротьбу з тероризмом та залучаються до неї.

Тому інтенсивний інформаційний потік, що базується на цілодобовому моніторингу та супроводі терористичної ситуації в Україні (і світі), підрозділом слід розділити на три потоки відповідно до етапу реагування: Перспективна інформація – для стратегічної оцінки та прогнозування ; середньостроковий-на тактичному рівні Визначити та коригувати боротьбу з інформаційним тероризмом; актуальна інформація, яка потребує щоденного реагування.

Аналітики, що працюють у моделі трьох потоків, також повинні відповідати професійним стандартам, щоб забезпечити відповідний аналіз потоків.

Україна – не єдина країна у світі, яка стикається з таким глобалізованим інформаційним злом, тому шлях повного вирішення проблеми боротьби з інформаційним тероризмом лежить у колективному об'єднанні процесу інформаційного тероризму шляхом міжнародної спільноти. Розробцы ефективних міжнародних контрзаходів.

Такий національний механізм дозволяє організувати міжнародне співробітництво по суті у формуванні та реалізації єдиного антитерористичного інформаційного закону. У ряді заходів, спрямованих на ліквідацію інформаційного тероризму як важливого чинника сучасного міжнародного життя, пріоритетне значення має надаватися прийняттю міжнародних політичних рішень, передбачених відповідними антитерористичними законами та нормативними актами.

Загальна теорія, що визначає національну безпеку, відводить особливе місце системі інформаційної безпеки. За сучасних умов для України це абсолютно розумно, і недарма, адже поява загроз, пов'язаних із геополітичними змінами чи тиском потужних іноземних держав, потребує негайного реагування.

Як соціально-політичне явище, інформаційний фактор став невід'ємною частиною інформаційного тероризму, дослідження останнього свідчать про необхідність створення дієвого національного механізму протидії загрозі тероризму національним інтересам України. У контексті збройного конфлікту на сході України аналіз державної політики України щодо боротьби з інформаційним тероризмом також свідчить про відсутність чітких і послідовних національних заторів у її реалізації.

Удосконалення механізму інформаційного протистояння полягає у формуванні та реалізації єдиної національної політики боротьби з інформаційним тероризмом в Україні. Основним аспектом цієї політики має стати реформування внутрішнього антитерористичного механізму, за його структурою (без порушення існуючої антитерористичної системи), чітке

визначення комплексного механізму боротьби з інформаційним тероризмом в Україні та покращення управління цим механізмом.

Водночас, якщо не буде створено якісного правового забезпечення на основі поглибленого кримінального розслідування детермінантів цих злочинів, боротьба з інформаційним тероризмом та протидія терористичній діяльності не буде ефективною, в порушення загальновизнаних цивілізованих цінностей. Нормативно-правова база повинна повністю відображати визначення інформаційного тероризму та кримінально-правову складову, що зафіксована в чинному національному законодавстві.

Факти довели, що інформаційний тероризм є природним продуктом сучасного суспільства. Проблема інформаційного тероризму пов'язана не лише з новітнім характером цього явища, а й з тим, що інформаційний тероризм став невід'ємною частиною сучасної політичної практики.

Поширення інформаційного тероризму може підірвати все суспільно-політичне життя, підірвати державні та політичні інститути. У зв’язку з цим національна безпека України стикається з дедалі більше довгостроковими викликами та загрозами, де ключовим фактором є інформаційний фактор: збройний конфлікт на сході, змішана війна Російської Федерації, нестабільна ситуація в Україні, дестабілізація внутрішньополітичної ситуації.

Реакція держави на інформаційні загрози та агресивну та ворожу пропаганду проти України свідчить про слабку її ефективність: органи державної влади не в змозі сформулювати загальну стратегію інформаційно-комунікаційної політики, не захищають власний інформаційний простір, постійно шукають баланс між свободою слова та необхідним рівнем контролю в інтересах національної безпеки.Усі ці ситуації підкреслюють актуальність боротьби з інформаційним тероризмом як функцію національної системи антикризового реагування та її зв’язок із найважливішими практичними завданнями сучасного державного управління у сфері інформаційної безпеки.

Для забезпечення належного рівня інформаційної безпеки необхідно вжити певні політичні, економічні та організаційні заходи щодо запобігання, виявлення та ліквідації таких ситуацій, факторів і дій, які можуть зашкодити чи перешкодити реалізації інформаційних прав, потреб та інтересів країни, її громадян.

Факти засвідчили, що в умовах постійно зростаючої загрози з боку світових, міжнародних та регіональних терористичних організацій уряди багатьох країн активно вживають додаткових антитерористичних заходів та виділяють додаткові ресурси. На міжнародному та регіональному (європейському) рівнях спостерігається тенденція до поглиблення співпраці у сфері боротьби з тероризмом. В основному це стосується обміну інформацією, покращення взаємодії спецслужб і правоохоронних органів, посилення транскордонного контролю, боротьби з фінансуванням тероризму.

Міжнародне співробітництво у сфері боротьби з тероризмом зараз набуває особливого значення, у тому числі в контексті забезпечення національної стабільності.

Досліджуючи міжнародне право, було встановлено, що навіть на цьому рівні всеосяжного документа з питань боротьби з інформаційним теризмом, який був спеціально спрямований на запобігання та використання телекомунікаційних технологій терористами, поки не існує.

На міжнародному рівні існує потреба у створенні та впровадженні уніфікованого нормативно-правового забезпечення (так званого типового законодавства), яке, не створюючи юридичних зобов’язань, носило б характер рекомендаційних керівних принципів, відігравало б важливу роль в процесі приведення у відповідність прийнятих державами правових стандартів. Країни Європи, з урахуванням терактів, працюють над модернізацією свого антитерористичного законодавства, включаючи норми, що регулюють механізми протидії інформаційному тероризму (збір даних, відеоспостереження, прослуховування, реєстрація і передача даних про неповнолітніх і т.д.).

ВИСНОВКИ

Бурхливий розвиток інформаційно-комунікаційних технологій наприкінці XX – на початку XXI століть став основою не лише для формування основ глобального інформаційного суспільства, а й стимулював активізацію інформаційних воєн та створив реальні загрози для всіх сфер суспільного життя. Тому питання захисту від інформаційних загроз стало актуальним у контексті загальної національної безпеки.

Передумовами виникнення інформаційного тероризму стали фінансова сторона – дешевизна, доступність будь-якої категорії фахівців у медіа-просторі та психології тощо, розвиток інформаційного суспільства у міжнародному просторі, прості методи та технології втілення, ефективність, скритність, безкарність. У свою чергу, інформаційний тероризм поділяється на інформаційно-психологічний тероризм та інформаційно-технічний тероризм.

Контролювати ЗМІ для поширення дезінформації, чуток, демонстрації могутності терористичних організацій, шкоди окремим елементам і всьому інформаційному середовищу всього противника: знищувати елементні бази, активно придушувати лінії зв’язку, штучно перезавантажувати вузли зв’язку тощо.

Цілісне подання проблем забезпечення державної безпеки від терористичних загроз в інформаційній сфері в рамках державної політики, сформоване на основі системного аналізу теоретико-методологічних підходів до аналізованої проблематики у вітчизняній політологічній науці, політичній соціології, конфліктології, детермінує сутність інформаційної протидії тероризму як політичного явища.

Кібертероризм, або в загальному розумінні - інтернет-тероризм так бачать зарубіжні вчені та правознавці визначення будь-якого прояву агресії, спраги до насильства та маніпулятивного впливу на населення через використання інформаційного ресурсу та інформаційної зброї.

Технічні досягнення інформаційної епохи надали якісно нові можливості засобам масової інформації та комунікації, перетворили їх на потужний інструмент впливу. Характерною особливістю є те, що в інформаційному середовищі в інтегрованому вигляді та різноманітних, найчастіше досить химерних поєднаннях одночасно функціонує інформація, що адекватно відображає існуючий світ, а також деформована, спотворена інформація. Цей обумовлено як складністю самого процесу пізнання та неповнотою знання про світ, так і упередженістю, суб'єктивністю людей, а найчастіше – цілеспрямованим використанням інформаційних процесів при досягненні власних аморальних цілей та ігноруванні завданих своїми діями збитків іншим людям.

Виходячи з досвіду вивчення зарубіжних дослідників можна провести аналогію до кібертероризму, тобто в нашому розумінні інформаційний тероризм – прямий вплив на психіку та свідомість людей з метою формування потрібних думок та суджень, певним чином викликаючи потрібну поведінку людей. На практиці під інформаційним тероризмом зазвичай мають на увазі такий насильницький пропагандистський вплив на психіку, який не залишає для людини можливостей критичного сприйняття реальності подій.

Інформаційний тероризм, будучи предметом вивчення даного дослідження, зайняв своє «місце» серед форм тероризму на підставі двох критеріїв – простору здійснення (інакше – середовища протікання) та засобів (інструментів), що застосовуються терористами, терористичними організаціями (спільнотами).

Один із найефективніших у довгостроковій перспективі заходом протидії тероризму у світі експерти вважають боротьбу з пропагандою радикального Ісламу. Трансформуючи досвід Європейських спецслужб, щодо протидії інформаційному тероризму на ситуацію, що складається навколо вітчизняних проблем у цій сфері, у тому числі пропаганди російських спецслужб, формування народних думок навколо ситуації на

Сході України, то такі підходи, нашу думку, необхідно застосовувати вітчизняними підрозділами боротьби з інформаційним тероризмом. Необхідно приділити більше уваги питанню взаємодії з недержавними організаціями, як вагомий провідник і зв'язуюча ланка між державою та громадянами у протидії тероризму та інформаційному тероризму зокрема. Така форма взаємодії громадських організацій у взаємодії з профільними спецслужбами, на наш погляд, на сьогодні є дуже актуальною для України на шляху побудови публічної політики протидії інформаційному тероризму, особливо протидії йому стосовно проявам навколо конфлікту на Сході країни. Конструктивно вибудовувати організаційно-правовий механізм протидії інформаційному тероризму необхідно саме профільній державній інституції, що відповідає за це - Антитерористичному центру при Службі безпеки України.

З'ясовано, що одним з ключових напрямків модернізації роботи Штабу АТЦ при СБ України повинен відбутись перегляд процесу отримання та аналізу інформації про терористичні загрози і прояви з метою підвищення функціональних можливостей вироблення та надання керівництву держави не тільки варіантів оперативного прийняття рішень щодо подолання кризових ситуацій терористичного характеру в інформаційній сфері, а й прогнозування наслідків їх застосування; підвищення ефективності превентивних та профілактичних антитерористичних заходів у повсякденній діяльності, бачення стратегічних цілей. Тобто модернізації підлягає інформаційно-аналітична управлінська складова антитерористичного державного механізму.

Антитерористичні системи та громадські організації повинні передбачати можливості популяризації інформаційного тероризму як суспільно небезпечного явища для суспільства, прагнути до створення атмосфери, яка не сприймає всі форми тероризму, особливо в частині інформаційного тероризму. поле. У міру зростання загрози тероризму

держава і громадянське суспільство повинні домовитися про найкращий баланс між безпекою, свободою слова та демократичною свободою.

На шляху реформування системи інформаційної безпеки України управління та розвиток національного механізму боротьби з інформаційним тероризмом, як невід'ємної частини національного механізму боротьби з інформаційним тероризмом, координує завдання у повсякденній діяльності та при появі ознак інформаційного тероризму. управління, боротися з інформаційним тероризмом, а також сформулювати та подати вищому керівництву країни необхідні варіанти боротьби з інформаційним тероризмом. Національним керівникам, Раді національної безпеки і оборони України та УВС Агентства безпеки України необхідно оцінити доцільність формування та впровадження окремої державної політики щодо боротьби з інформаційним тероризмом у загальній внутрішньодержавній боротьбі з тероризмом.

За результатами таких оцінок вбачаються відповідні зміни в законодавстві та інших нормативно-правових актах у сфері протидії тероризму, а також забезпечення інформаційної безпеки України, а саме: удосконалення законодавства шляхом запровадження додаткових концептуальних засобів та усунення суперечностей і прогалин. в Україні під координаційною функцією Комісії національної безпеки і оборони на базі АТЦ Агентства безпеки України створити, організувати та законодавчо закріпити та запровадити національний комплексний механізм боротьби з інформаційним тероризмом, організувати та удосконалити управління національний механізм боротьби з інформаційним тероризмом відповідно до законодавства.

На міжнародному рівні, як державі, що перебуває в стані активного збройного конфлікту зі «змішаним» інформаційним протистоянням, необхідно розпочати єдиний законодавчий процес у сфері боротьби з інформаційним тероризмом та запровадити єдину систему та боротьбу з цим злочинним явищем.

Розкрито конкретну реалізацію політики боротьби з інформаційним тероризмом в умовах сучасних глобальних викликів і загроз, показує, що головною метою системи антитерористичної безпеки України є забезпечення безпеки людей, суспільства та країни від тероризму. держава. Люди виявили, що сучасна модель глобалізації дає змогу поширювати міжнародний тероризм та міжнародну злочинність. У глобальній геополітичній системі, широко розгорнутій у процесі глобалізації, міжнародний тероризм відіграє особливу роль з початку XXI століття. Станьте глобальною руйнівною силою, що загрожує фундаменту людської цивілізації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Актуальні проблеми управління інформаційною безпекою держави: зб. тез наук. доп. наук.-практ. конф. (Київ, 4 квітня 2019 р.). [Електронне видання]. – Київ : Нац. акад. СБУ, 2019. – с. 70-73

2. Армія FM Військове радіо. URL: http://mediasat.info/2016/03/16/armiya-fm-vij skove-radio.

3. Бабенко Ю. Інформаційний тероризм / Ю. Бабенко URL: http://www.aratta-ukraine.com/text_ua.php?id=149.

4. Баланда А.Л. Соціальні детермінанти національної безпеки України: Монографія. – Інститут демографії та соціальних досліджень НАН України. К., 2008. – 414 с.

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

6. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник / за ред. Кривуци В.Г. – Київ: ООО «Д.В.К.», 2004. – 508 с.

7. Бойченко О. В. Кібертероризм у складі сучасних проблем національної безпеки / О. В. Бойченко, О. О. Ончурова // Форум права. – 2010. – № 2. – С. 57–62.

8. Бойченко О. В. Медіа-тероризм: особливості сучасних ознак інформаційній безпеці / О. В. Бойченко // Інтегровані інтелектуальні робото технічні комплекси (ПРТК-2009): Друга міжнародна наук.-практ. конф. (25–28 травня 2009 р.). – К.: НАУ, 2009. – С. 230–232.

9. Бочарніков І. В. Інформаційна протидія тероризму в сучасних умовах / Електронний науковий журнал Проблеми безпеки, 2013 № 3 (21).

10. 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, 12-13 лютого 2016 року). Одеса: ГО «Причорноморська фундація права», 2016. С. 104-108.

11. Воронцова Л.В., Фролов Д.Б.. Історія і сучасність протиборства. М. : Гаряча лінія Телеком. 2006. 192 с.

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

13. 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.

14. Горбань Ю.О. Інформаційна війна проти України та засоби її ведення.URL:http://www.visnyk.academy.gov.ua/wpcontent/uploads/2015/04/20.pdf.

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

16. Діордіці І. В. Кібертероризм як елемент дестабілізації системи стратегічних комунікацій / І. В. Діордіці. – 2016. – URL: https://goal-int.org/kiberterorizm-yak-elementi-destabilizacii-sistemi-strategichnix-komunikacij/.

17. 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.

18. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25.02.2017 р. № 47/2017 URL: http://president.gov.ua.

19. Дослідження медіа-ситуації в південних і східних областях України 2017. - Інститут масової інформації. URL: https://imi.org.ua/monitorings/doslidzhennya-media-sytuatsiji-v-pivdennyh-i-shidnyh-oblastyahukrajiny2017.

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

21. 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.

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

23. 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/політ-2021/.

24. Інформаційний простір – 2019. – URL: https://uk.wikipedia.org/wiki/Інформаційний_простір.

25. 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)

26. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний 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.

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

28. 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

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

30. 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.

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

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

33. 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

34. 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.

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

36. Костіхін А. А. Інтернет як інструмент терористичних та екстремістських організацій у психологічній війні URL: http://www.iimes.ru/?p=4737

37. Кубишкін О. В. Міжнародно-правові проблеми забезпечення інформаційної безпеки держави URL: http://pravolib.pp.ua/mejdunarodnopravovyie-problemyi obespecheniya.html/

38. 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

39. Логвінець В. Епоха інформаційно-психологічних операцій: Лівія. URL: http://psyfactor.org/psyops/psyops5.htm.

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

41. Майоров В.В. Розмежування терористської та екстремістської діяльності. URL: http://goal-int.org/rozmezhuvannya-teroristskoi-ta-ekstremistskoi-diyalnosti

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

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

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

45. 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-informatsijnoho-teroryzmu-yakzahrozy-natsionalnij-ta-mizhnarodnij-bezpetsi/.

46. Методи інформаційного захисту простору. Інформаційна безпека України. URL: http://www.uatextreferat.com/referat-7471.html.

47. 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

48. 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

49. Моїсеєв А. І. Проблема міжнародного інформаційного обміну у боротьбі з тероризмом / А. І. Моїсеєв. // Актуальні проблеми російського права. - 2014. - №11. - С. 2612-2616.

50. 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.

51. 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.

52. Про боротьбу з тероризмом: Закон України від 24.11.2021 р. № 25/ Верховна Рада України URL: https://zakon.rada.gov.ua/laws/show/638-15#Text

53. 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/3475-15#Text.

54. 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/341-2014-%D0%BF#Text

55. 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

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

57. Про Національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації: Указ Президента України від 23.11.2011 №

1067/2011/ Верховна Рада України. Законодавство України. URL: https://zakon.rada.gov.ua/laws/show/1067/2011#Text

58. 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.

59. 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

60. 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.

61. 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.

62. 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

63. 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

64. 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

65. Проблеми забезпечення національної безпеки України на сучасному етапі державотворення : матеріали круглого столу (Київ, 21 жовт.

2010 р.) ; НАДУ при Президентові України ; за заг. ред. Г. П. Ситника. – К. : НАДУ, 2011. – 72 с

66. 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/.

67. 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/.

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

69. 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.

70. 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.

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

72. 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.

73. Слюсаревський М. М. Інформаційний простір : критика існуючих визначень і спроба побудови теорії. Вісн. ХДУ. Серія «Психологія, політологія» : Особистість і трансформаційні процеси в суспільстві.

Психолого-педагогічні проблеми сучасної освіти. Харків. 1999. Ч. 4-5. С. 337-342.

74. Сологуб Р. - Як захистити критичну інфраструктуру країни у кіберпросторі / Р. Сологуб / URL: https://biz.nv.ua/ukr/experts/jakzakhistiti-najtsinnishu-informatsiju-u-kiberprostori-2510093.html

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

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

77. Статут Організації Об’єднаних Націй і статут Міжнародного суду: від 26.06.1945. URL: https://zakon.rada.gov.ua/laws/show/995_010#Text.

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

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

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

81. 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.

82. 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.

83. 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.

84. 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.

85. Фурсов А.І Психоісторична війна. URL: https://firtka.if.ua/blog/view/a-i-fursov-psihoistoricna-vijna45613.

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

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

88. 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.

89. 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.

90. 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.

91. 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.

92. Defining cyber terrorism URL: https://www.i-policy.org/2009/07/defining-cyber-terrorism.html.

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

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

95. Human Rights Watch: Росія масово порушує права людини в Криму. URL: http://krymsos.com/news/human-rights-watch-rosiya-masovo-porushuye-prava-lyudini-v-krimu.

96. 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.

97. 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.

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

99. 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.

100. NATO Strategic Communication: More to be Done? / Steve Tatham, Rita Le Page; National Defence Academy of Latvia Center for Security and Strategic Research. – Rīga, 2014. URL: http://www.academia.edu/6808986/NATO_Strategic_Communication_More_to_be_done.

101. Proposed policy recommendations for the high level conference. – RAN.2012.December. – URL: http//ec.europa.eu/dgs/home-affairs.

102. Terrorism – URL: https://www.britannica.com/topic/terrorism.