Харківський національний університет імені В. Н. Каразіна
Навчально-науковий інститут «Каразінський інститут
міжнародних відносин та туристичного бізнесу»
Кафедра міжнародних відносин

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

на тему: **«Протидія інформаційному тероризму в США»**

Виконала:
студентка 2-го курсу, групи УМІБ-61
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
ОПП «Міжнародна інформаційна безпека»
Белітрова Марія Сергіївна
(прізвище, ім'я, по батькові)

Керівник:
к.п.н., доц. Пересипкіна Ірина Валентинівна
(науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

Рецензент:
д.п.н., проф. Шамраєва Валентина Михайлівна
(науковий ступінь, вчене звання, прізвище, ім'я, по батькові)

ХАРКІВ – 2024 рік

ЗМІСТ

ВСТУП

Актуальність теми протидії інформаційному тероризму в США зумовлена стрімким розвитком інформаційних технологій, що створюють нові можливості для поширення дезінформації, маніпуляції громадською думкою та підриву національної безпеки. Інформаційний тероризм стає одним із ключових інструментів гібридної війни, використовуючи фейкові новини, кібер-атаки та соціальні мережі для дестабілізації суспільства, посилення політичної поляризації та дискредитації державних інституцій. США, як провідна світова держава, є особливо вразливими до таких загроз через відкритість інформаційного простору та високу залежність суспільства від цифрових технологій. Зростання кібератак на критичну інфраструктуру, втручання у виборчі процеси та поширення пропаганди від ворожих держав вимагають оперативних і комплексних рішень. Федеральний уряд США, зокрема через агентства на кшталт Департаменту внутрішньої безпеки (DHS), активно працює над розробкою стратегій і заходів для протидії цим викликам, включаючи впровадження законодавчих ініціатив, посилення кібербезпеки та співпрацю з приватним сектором. Водночас інформаційний тероризм загрожує основним демократичним цінностям США, зокрема свободі слова та довірі до медіа, що підкреслює важливість балансу між безпекою та збереженням прав громадян. Ефективна протидія вимагає не лише технологічних рішень, але й підвищення обізнаності населення, розробки механізмів для перевірки достовірності інформації та міжнародної співпраці. У контексті глобалізації та взаємозалежності інформаційного простору успішна боротьба США з інформаційним тероризмом стане важливим прикладом для інших країн у забезпеченні інформаційної безпеки та стійкості суспільства до сучасних викликів.

Ступінь вивченості теми. Американські науковці, такі як С. Бреннер, Р.Кнейк та Р.Монтасарі, аналізують стратегічну роль інформації в сучасних конфліктах, зосереджуючи увагу на інструментах протидії інформаційним атакам, включаючи законодавчі ініціативи, технологічні засоби та освітні

програми. У роботах зарубіжних авторів, наприклад, Дж.Рейбер та М.Гленн, акцент робиться на транснаціональному характері інформаційного тероризму, ролі соціальних медіа та алгоритмів штучного інтелекту у поширенні фейкових новин і деструктивного контенту. Українські науковці, такі як С. Гнатюк, М.Гуцалюк та С.Стежко, аналізують досвід США у протидії інформаційному тероризму, розглядаючи можливості адаптації цих практик для українських реалій, особливо в умовах війни та гібридних загроз з боку РФ. Їхні праці висвітлюють питання взаємодії державних інститутів, приватного сектора та громадянського суспільства у протидії інформаційним атакам, а також роль міжнародної співпраці у боротьбі з цим явищем.

Мета дослідження – визначити особливості протидії інформаційному тероризму в США.

Завдання дослідження:

– визначити сутність поняття інформаційного тероризму;

– розглянути форми та методи протидії інформаційному тероризму;

– визначити вплив інформаційного тероризму на міжнародну безпеку;

– розглянути законодавчі основи протидії інформаційному тероризму у США;

– розглянути політику США у сфері кібербезпеки та протидії інформаційному тероризму;

– визначити роль недержавних інституцій та організацій у протидії інформаційним атакам;

– розглянути інституційні рамки міжнародної співпраці США в боротьбі з інформаційним тероризмом;

– з’ясувати особливості співпраці США з міжнародними організаціями та іншими державами у протидії інформаційним загрозам;

– розглянути досвід США для України у міжнародній співпраці щодо протидії інформаційному тероризму.

Об’єкт дослідження – процес протидії інформаційному тероризму.

Предмет дослідження – механізми протидії інформаційному тероризму в США.

Теоретико-методологічна база дослідження ґрунтується на міждисциплінарному підході, який поєднує елементи теорії комунікації, інформаційної безпеки, політології, соціології, права та кібербезпеки. Основними теоретичними засадами є концепція інформаційної війни, що висвітлює стратегії використання інформації як інструменту впливу та маніпуляції, теорія тероризму як соціально-політичного феномену, а також підходи до управління ризиками у сфері інформаційної безпеки. Методологічна основа включає системний аналіз, порівняльний метод для вивчення досвіду США та інших країн. Значну роль відіграє використання емпіричних методів, таких як аналіз статистичних даних про кібератаки, дослідження випадків (case study) інформаційних атак та їхніх наслідків. Важливим аспектом є правовий аналіз законодавчої бази США у сфері інформаційної безпеки, зокрема актів, спрямованих на боротьбу з тероризмом і захист критичної інформаційної інфраструктури.

Інформаційна база дослідження включає аналіз законодавчих актів, зокрема USA PATRIOT Act, законів щодо кібербезпеки та протидії тероризму, матеріали державних структур, таких як Департамент внутрішньої безпеки (DHS), Федеральне бюро розслідувань (FBI), Національна агенція безпеки (NSA), а також відкриті дані, аналітичні звіти і дослідження неурядових організацій. Увага приділяється також науковим статтям і монографіям, які аналізують феномен інформаційного тероризму, його інструменти, методи впливу на суспільство та економіку, а також ефективність заходів протидії з боку державних та приватних структур. Використання статистичних даних дозволяє оцінити масштаби проблеми та результативність різних стратегій боротьби. Таким чином, інформаційна база охоплює широке коло джерел, необхідних для комплексного дослідження теми протидії інформаційному тероризму в США.

Практичне значення отриманих результатів. Запропоновані у кваліфікаційній роботі магістра теоретичні положення та висновки можуть

бути використані:

– центральними та місцевими органами виконавчої влади під час розробки законодавчого регулювання щодо протидії інформаційному тероризму в Україні;

– у навчальному процесі Харківського національного університету імені В. Н. Каразіна та інших вищих навчальних закладів при розробці та викладанні дисциплін, за програмами підготовки магістрів міжнародних відносин, суспільних комунікацій та регіональних студій.

Апробація дослідження була здійснена у вигляді публікації тез наукової доповіді для участі у Всеукраїнському науково-практичному круглому столі «Стратегічні напрями зовнішньої політики та дипломатії країн світу» (м. Харків, 21 листопада 2024 р.), на тему: «Countering information terrorism in the United States of America».

Структура роботи. Кваліфікаційна робота магістра складається зі вступу, трьох розділів, висновків, списку використаних джерел, що налічує 82 найменування. Загальний обсяг роботи становить 96 сторінки, з яких основного тексту – 84 сторінки.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ПОНЯТТЯ ІНФОРМАЦІЙНОГО ТЕРОРИЗМУ

1.1. Сутність поняття інформаційного тероризму

Інформаційний тероризм є однією з нових форм загроз у сучасному світі, що виникла в умовах глобалізації, розвитку інформаційних технологій та цифровізації суспільства. Цей феномен охоплює широкий спектр дій, спрямованих на використання інформації або інформаційних систем з метою залякування, маніпуляції, завдання шкоди чи досягнення політичних, економічних або соціальних цілей. Сутність інформаційного тероризму полягає у використанні інформаційних технологій та засобів масової інформації як зброї для досягнення деструктивних цілей. Для кращого розуміння цього явища варто звернутися до визначень, що пропонують різні науковці та міжнародні організації. Інформаційний тероризм є одним із найсучасніших викликів у сфері міжнародної безпеки, що постає на перетині традиційного розуміння тероризму та використання інформаційних технологій. Це явище знаходиться в центрі уваги дослідників, політиків та фахівців у галузі міжнародних відносин, оскільки воно впливає на національні інтереси держав, глобальну стабільність та міжнародну систему в цілому [3].

На думку американського дослідника Р. Тапліна, інформаційний тероризм – це «використання чи загроза використання інформаційних технологій або інформації для здійснення атак на держави, суспільства, окремих осіб чи організації з метою примусу чи залякування». Цей підхід акцентує увагу на стратегічному використанні інформації як інструменту тиску. Інший дослідник, М. Байн, зазначає, що інформаційний тероризм відрізняється від традиційного тероризму тим, що його інструментами є не фізичне насильство, а інформаційні ресурси, включаючи кіберпростір. Байн підкреслює, що основна мета цього явища – дестабілізація суспільства через викривлення або маніпуляцію інформацією [79, p. 55-60].

Однак визначення поняття інформаційного тероризму залишається

складним і дискусійним питанням. Різноманіття підходів до його аналізу зумовлене багатозначністю самого явища, його технологічною природою та різними перспективами оцінки його впливу на міжнародну систему. У цьому тексті розглянуто основні підходи до визначення інформаційного тероризму, їх теоретичні основи та практичне застосування в контексті міжнародних відносин.

Перший підхід до визначення інформаційного тероризму зосереджується на його технологічних аспектах. У межах цього підходу акцент робиться на використанні інформаційно-комунікаційних технологій для здійснення терористичних дій. Інформаційний тероризм у цьому контексті визначається як навмисне використання кіберпростору або цифрових технологій для нанесення шкоди державним або приватним структурам, зокрема шляхом порушення їхньої інформаційної інфраструктури. Це може включати хакерські атаки, спрямовані на знищення або викрадення даних, саботаж важливих інформаційних систем, створення та розповсюдження шкідливого програмного забезпечення. Такий підхід отримав розвиток у працях дослідників кібербезпеки та міжнародних відносин, які аналізують сучасні виклики у сфері глобальної безпеки. Наприклад, кібертероризм часто розглядається як одна з форм інформаційного тероризму, що полягає у використанні комп’ютерних мереж для здійснення атак, спрямованих на досягнення політичних або ідеологічних цілей [5, с. 61-62].

Другий підхід до визначення інформаційного тероризму базується на аналізі його психологічного та соціального впливу. У цьому випадку інформаційний тероризм розглядається як форма психологічної війни, спрямованої на створення страху, паніки та дестабілізації суспільства. Такий тероризм включає дії, пов’язані з розповсюдженням пропаганди, фейкових новин або маніпуляцією інформацією для формування певного сприйняття серед громадськості. Основною метою є не лише завдати прямої шкоди, а й вплинути на громадську думку, підірвати довіру до державних інституцій або мобілізувати підтримку терористичних організацій. Цей підхід часто

використовується у дослідженнях, присвячених інформаційній війні та гібридним конфліктам, які дедалі більше стають важливою частиною міжнародного дискурсу [2, с. 64-71].

Третій підхід до аналізу інформаційного тероризму зосереджується на його правовому аспекті та питаннях міжнародного регулювання. У рамках цього підходу інформаційний тероризм розглядається як порушення міжнародного права та загроза міжнародному миру та безпеці. Однак чітке визначення інформаційного тероризму в міжнародно-правових актах відсутнє, що створює правову невизначеність. Одним із викликів є складність класифікації інформаційних атак як актів тероризму, оскільки вони можуть бути анонімними, транскордонними та не мати очевидних доказів причетності до конкретних суб'єктів. Ця проблема підкреслює необхідність розробки міжнародно-правових механізмів для боротьби з інформаційним тероризмом та встановлення відповідальності за такі дії [4, с. 118-129].

Четвертий підхід акцентує увагу на геополітичному аспекті інформаційного тероризму, розглядаючи його як інструмент гібридної війни та засіб впливу у міждержавних конфліктах. У цьому контексті інформаційний тероризм використовується державами або недержавними акторами для послаблення стратегічних позицій суперників. Наприклад, інформаційні атаки можуть бути спрямовані на маніпуляцію виборчими процесами, втручання у внутрішні справи інших держав або порушення роботи критичної інфраструктури. Це створює нові виклики для міжнародної безпеки, оскільки такі дії часто залишаються безкарними через складність доведення вини або встановлення джерела атаки [4, с. 118-129].

П'ятий підхід до визначення інформаційного тероризму пов'язаний із гуманітарними аспектами та питаннями прав людини. У цьому контексті акцент робиться на захисті людей від наслідків інформаційних атак, які можуть порушувати їхні права, свободи та безпеку. Інформаційний тероризм може проявлятися у формі порушення конфіденційності персональних даних, розповсюдження контенту, що провокує ненависть або насильство, або

використання технологій для пригнічення певних соціальних груп. Цей підхід підкреслює важливість балансу між свободою інформації та необхідністю забезпечення безпеки, що є особливо актуальним у контексті цифровізації суспільства [12, с. 23-26].

Шостий підхід до визначення інформаційного тероризму полягає у його системному аналізі в контексті глобалізації. У цьому випадку інформаційний тероризм розглядається як наслідок розвитку глобальних мереж та інтеграції інформаційних систем. Глобалізація сприяє поширенню інформаційних технологій, що одночасно створює нові можливості для терористів. З одного боку, інформаційний тероризм може використовуватися для глобальної мобілізації підтримки, вербування нових членів та координації дій терористичних організацій. З іншого боку, глобальний характер цього явища ускладнює його контроль та протидію, оскільки інформаційні атаки можуть бути спрямовані з будь-якої точки світу і мати глобальні наслідки [12].

Важливим є також міждисциплінарний підхід до визначення інформаційного тероризму, який інтегрує елементи технологічного, соціального, правового, геополітичного та гуманітарного аналізу. Цей підхід дозволяє розглянути інформаційний тероризм у всій його складності та врахувати взаємодію різних чинників, що його визначають. Наприклад, дослідження, що поєднують аналіз інформаційних технологій, психології масової свідомості та міжнародного права, дозволяють краще зрозуміти механізми впливу інформаційного тероризму на міжнародну систему та розробити ефективні стратегії протидії [13, с. 78-80].

У сучасному світі інформаційний тероризм стає все більшою загрозою, що впливає на міжнародну безпеку, суверенітет держав та глобальну стабільність. Його складна природа вимагає багатовимірного аналізу та міждисциплінарного підходу до розуміння цього явища. Незважаючи на те, що поки що не існує загальноприйнятого визначення інформаційного тероризму, дослідження у цій сфері сприяють розробці нових підходів до протидії та міжнародного регулювання. У цьому контексті важливими залишаються

питання узгодження міжнародних стандартів, посилення співпраці між державами та розвиток технологій захисту від інформаційних атак. Таким чином, інформаційний тероризм не лише є викликом, але й стимулом для формування нових механізмів безпеки у міжнародній системі.

Інформаційний тероризм може проявлятися у різних формах, залежно від цілей та методів, що використовуються. Серед основних видів можна виділити наступні (Табл. 1.1.):

Таблиця 1.1.

Види інформаційного тероризму [13]

Вид	Характеристика
Кібертероризм	Це найпоширеніший вид інформаційного тероризму, який включає атаки на комп'ютерні системи, мережі чи бази даних з метою порушення їхньої роботи або викрадення інформації. Наприклад, хакерські атаки на урядові установи чи критичну інфраструктуру можуть спричинити економічний чи соціальний хаос.
Інформаційно-психологічний тероризм	Цей вид тероризму спрямований на маніпулювання свідомістю громадян через розповсюдження фейкових новин, пропаганди чи дезінформації. Його мета – викликати паніку, розкол у суспільстві або вплинути на прийняття політичних рішень.
Економічний інформаційний тероризм	Він включає маніпуляції з фінансовими даними чи біржовими системами, розповсюдження неправдивої інформації про економічну ситуацію в країні для зниження довіри до уряду чи економічної системи
Соціальний інформаційний тероризм	Цей вид тероризму спрямований на провокування конфліктів між різними соціальними, етнічними чи релігійними групами через інформаційні атаки.

Сутність інформаційного тероризму полягає у використанні інформації як засобу впливу на масову свідомість, дестабілізації суспільства та досягнення власних цілей. Основною рисою інформаційного тероризму є його здатність впливати на великі групи населення за короткий час із мінімальними

витратами ресурсів. У цьому контексті інформаційний тероризм часто називають «асиметричною загрозою», оскільки для його здійснення не потрібні значні матеріальні чи людські ресурси.

З точки зору міжнародних відносин, інформаційний тероризм стає дедалі більш значущим фактором у глобальній політиці. Уряди та міжнародні організації змушені адаптуватися до нових викликів, розробляючи політики кібербезпеки та інформаційного захисту. Наприклад, НАТО визнало кіберпростір п’ятою сферою ведення війни, поряд із сушею, морем, повітрям та космосом. Це свідчить про усвідомлення загрози, яку становить інформаційний тероризм для глобальної безпеки. Одним із важливих аспектів у дослідженні інформаційного тероризму є розуміння його мотивації. Як зазначає П.В. Дайк, терористи використовують інформаційні технології для досягнення максимального резонансу своїх дій. Вони прагнуть привернути увагу до своїх ідей або домогтися політичних поступок шляхом створення атмосфери страху чи невизначеності. Це пояснює, чому інформаційний тероризм часто супроводжується масовими інформаційними кампаніями, спрямованими на залучення уваги громадськості [6, с. 312-317].

Інформаційний тероризм включає різноманітні дії, які базуються на використанні інформаційних технологій для досягнення політичних, соціальних чи ідеологічних цілей. Однією з головних рис інформаційного тероризму є його багатовимірність. Він може бути спрямований як на державні інститути, так і на приватні компанії чи окремих громадян. Інформаційний тероризм часто націлений на критичну інфраструктуру, таку як енергетичні системи, транспорт, фінансові установи та комунікаційні мережі. Зокрема, кібератаки на ці об’єкти можуть призвести до значних економічних втрат, порушення життєдіяльності суспільства та навіть до людських жертв. Крім того, інформаційний тероризм активно використовується для маніпуляції громадською думкою. Через соціальні мережі, новинні сайти та інші платформи терористичні групи та ворожі держави поширюють пропаганду, дезінформацію та панічні настрої. Основна мета таких дій – викликати

недовіру до урядів, посіяти розбрат у суспільстві та підірвати міжнародну співпрацю. Особливу загрозу становить використання алгоритмів, які підбирають персоналізований контент для користувачів, оскільки це дозволяє створювати так звані «інформаційні бульбашки», в яких люди отримують викривлену картину реальності [17, с. 45-54].

Сучасні терористичні організації все частіше використовують інформаційні платформи для рекрутування нових членів. Інтернет дозволяє їм швидко поширювати ідеологічні меседжі серед різних соціальних груп, особливо серед молоді, яка є найбільш вразливою до маніпуляцій. Вони створюють віртуальні спільноти, де поширюються екстремістські ідеї, і таким чином залучають нових прихильників. Для цього використовуються як відкриті, так і закриті платформи, включаючи форуми та месенджери. Особливе місце у феномені інформаційного тероризму займає кібершпигунство та саботаж. Держави та недержавні актори використовують кібератаки для викрадення важливої інформації, порушення роботи урядових систем чи дестабілізації економічних процесів. Наприклад, кібератаки на банки чи енергетичні компанії можуть призвести до значних економічних втрат і викликати паніку серед населення. Крім того, інформаційні атаки можуть використовуватися для дискредитації політичних лідерів чи цілих держав, що має серйозні наслідки для міжнародних відносин. Один із ключових аспектів інформаційного тероризму – це створення умов для психологічного тиску на громадян та політичні еліти. Зокрема, використання фейкових новин, маніпулятивних відео чи сфабрикованих доказів може призвести до масштабної паніки або ж викликати агресію в суспільстві. Інформаційний тероризм спрямований на посилення соціальної напруги, створення атмосфери страху та недовіри, що значно ускладнює управління державою [7, с. 86-88].

Інформаційний тероризм у сучасному світі проявляється через численні приклади, які свідчать про його реальну небезпеку та багатогранність. Ці приклади демонструють, як інформаційні технології використовуються для

досягнення політичних, соціальних чи економічних цілей, зумовлюючи дестабілізацію суспільств і держав. Одним із найвідоміших прикладів *кібертероризму* є атака на енергетичну інфраструктуру України у 2015 році, яка отримала назву BlackEnergy. Хакери, імовірно пов'язані з іноземною державою, проникли в системи управління енергетичними компаніями, що призвело до масштабного відключення електроенергії в кількох регіонах країни. Це стало першим задокументованим випадком використання кіберзброї для ураження критичної інфраструктури держави. Такі атаки спрямовані на дестабілізацію економіки та підрив довіри громадян до здатності уряду захищати населення. Інший приклад – атака вірусу WannaCry у 2017 році, що вразила тисячі організацій у 150 країнах світу, включаючи лікарні, транспортні компанії та банківські установи. Цей вірус блокував доступ до даних і вимагав викуп за їх розшифрування. Хоча атака мала радше економічний характер, її наслідки могли бути використані терористичними організаціями для залякування або підриву довіри до цифрових систем [10, с. 154-160].

Прикладом *інформаційно-психологічного тероризму* є кампанії з дезінформації, які використовуються для впливу на політичні процеси. Наприклад, під час президентських виборів у США у 2016 році виявлено масові кампанії з розповсюдження фейкових новин у соціальних мережах. Ці дії були спрямовані на дискредитацію кандидатів та маніпуляцію громадською думкою. У звіті ФБР зазначено, що організаторами таких кампаній виступали іноземні актори, які мали на меті розкол у американському суспільстві. Ще одним прикладом є використання дезінформації під час пандемії COVID-19. Терористичні угруповання, такі як «Аль-Каїда» чи ІДІЛ, поширювали фейкові повідомлення про те, що вірус створено західними державами для контролю над населенням. Метою таких дій було викликати недовіру до урядів і міжнародних організацій, таких як ВООЗ, та стимулювати соціальні конфлікти [17, с. 46-54].

Приклад *економічного інформаційного тероризму* –2016 році хакерська

атака на Центральний банк Бангладеш призвела до крадіжки 81 мільйона доларів. Зловмисники використовували викрадені дані для проведення транзакцій через міжнародну систему SWIFT. Цей випадок продемонстрував, наскільки вразливою є фінансова система навіть на найвищому рівні. Хоча основна мета атаки була економічною, такі дії можуть бути використані для підриву стабільності цілих держав або їхніх банківських систем. Ще одним випадком є атака на криптовалютні біржі. Наприклад, у 2021 році хакери викрали понад 600 мільйонів доларів із платформи Poly Network. Це створює ризик для економічних відносин, оскільки підриває довіру до цифрових валют та їхніх технологій [24].

Приклад *соціального інформаційного тероризму* – у 2017 році в М'янмі соціальні мережі, зокрема Facebook, стали платформою для поширення ненависті проти етнічної меншини рохінджа. Дезінформація, фейкові новини та мова ворожнечі спричинили ескалацію насильства, що призвело до масових переслідувань і біженців. У цьому випадку інформаційний тероризм став інструментом для загострення етнічних конфліктів і порушення прав людини. У 2020 році у США під час протестів руху Black Lives Matter було зафіксовано численні випадки поширення неправдивих повідомлень через соціальні мережі. Мета таких дій – спровокувати подальше насильство, загострити протистояння між різними соціальними групами та створити хаос [20, с. 58-64].

Таким чином, інформаційний тероризм є складним і багатогранним феноменом, який вимагає глибокого дослідження та ефективних заходів протидії. Його поширення є наслідком технологічного прогресу, і боротьба з ним повинна враховувати всі аспекти сучасного суспільства – технологічні, політичні, соціальні та правові. Міжнародне співробітництво, підвищення обізнаності населення та вдосконалення технологій є ключовими елементами успішної боротьби з цією загрозою.

1.2. Форми та методи протидії інформаційному тероризму

Інформаційний тероризм, як специфічна форма загрози в сучасному світі, є об’єктом пильної уваги в рамках міжнародних відносин, оскільки має глобальний характер і значний вплив на політичну стабільність, економічну безпеку та суспільну згуртованість. Суть інформаційного тероризму полягає у використанні інформаційних ресурсів і технологій для досягнення політичних, ідеологічних чи інших цілей шляхом створення страху, хаосу, дезінформації або маніпуляції свідомістю. Форми прояву інформаційного тероризму можуть варіюватися від кібератак на критичну інфраструктуру до поширення фейкових новин та пропагандистських кампаній. У такому контексті протидія інформаційному тероризму стає ключовим завданням для держав, міжнародних організацій та інших акторів міжнародної політики [16, с. 32-38].

У сучасному світі інформаційний тероризм набуває дедалі більшого значення завдяки поширенню цифрових технологій, що забезпечують доступ до глобальної аудиторії майже миттєво. Його основними проявами є дезінформація, кібернапади, маніпуляція громадською думкою через соціальні мережі, створення фейкових новин і використання пропаганди. Протидія цьому явищу стає одним із головних викликів для держав, організацій та окремих громадян. Перш за все, аналіз форм інформаційного тероризму дозволяє краще зрозуміти його природу. Однією з найбільш поширених форм є кібератаки, спрямовані на порушення функціонування критичної інфраструктури, такої як енергетичні системи, транспортні мережі, банківський сектор чи державні установи. Такі дії можуть бути як самостійними актами, так і частиною масштабніших гібридних конфліктів. Іншою формою є використання соціальних мереж для поширення дезінформації, розпалювання ненависті чи координації радикальних груп. Маніпуляція громадською думкою, зокрема через створення і розповсюдження фейкових новин, є ще одним інструментом інформаційного тероризму, що має на меті посіяти недовіру до урядів або інституцій. Відповідно, усвідомлення широкого спектру форм інформаційного тероризму

є основою для розробки ефективних стратегій протидії (Табл 1.2.).

Таблиця 1.2.

Основні напрями протидії інформаційному тероризму [16]

Категорія методу	Опис методу
Освітні методи	Проведення тренінгів з медіаграмотності та критичного мислення. Інформування громадян про ризики дезінформації.
Технологічні методи	Використання програм для автоматичного виявлення фейків. Захист інформаційних систем від хакерських атак.
Законодавчі методи	Прийняття законів, що регулюють відповідальність за розповсюдження фейків. Співпраця з міжнародними організаціями для боротьби з кіберзлочинністю.
Соціальні методи	Організація інформаційних кампаній для підвищення обізнаності населення. Сприяння довірі до офіційних джерел інформації.
Інформаційні методи	Швидке поширення правдивої інформації для спростування фейків. Використання соціальних мереж для боротьби з пропагандою.
Економічні методи	Фінансування проєктів, спрямованих на розвиток незалежної журналістики. Санкції проти платформ, що підтримують дезінформацію.
Міжнародні методи	Координація з міжнародними організаціями для обміну досвідом та технологіями. Участь у спільних ініціативах протидії інформаційному тероризму.

На міжнародному рівні існують кілька форм протидії інформаційному тероризму, які базуються на багатосторонній взаємодії. По-перше, важливу роль відіграє створення міжнародно-правової бази для регулювання інформаційного простору. Це включає ухвалення угод про боротьбу з кіберзлочинністю, зокрема Будапештської конвенції, яка є одним із ключових

інструментів у цій сфері. Міжнародна спільнота також працює над створенням нових правових механізмів для боротьби з дезінформацією та пропагандою, які можуть бути використані як інструменти тероризму. По-друге, важливими є координаційні механізми між державами для обміну інформацією, технологіями та найкращими практиками. Наприклад, у рамках НАТО чи Європейського Союзу створено платформи для обміну даними про кібератаки та способи їх запобігання. По-третє, значну увагу приділяють підвищенню кіберстійкості через спільні навчання, тренінги та розробку стандартів захисту інформаційних систем [7, с. 86-88].

Окрім того, методи протидії інформаційному тероризму можуть бути поділені на кілька категорій залежно від їхньої специфіки. Для ефективної протидії інформаційному тероризму держави, організації та громадяни розробляють різноманітні методи, які можна умовно поділити на технічні, освітні, правові та інформаційні. *Перша категорія* включає технічні заходи, такі як розвиток сучасних систем кібербезпеки, вдосконалення алгоритмів для виявлення дезінформації та впровадження інноваційних рішень для захисту критичної інфраструктури. Технічні методи передбачають розвиток кібербезпеки, впровадження систем моніторингу інформаційного простору, розробку алгоритмів для виявлення фейкових новин і автоматизоване блокування небажаного контенту. Наприклад, багато компаній, таких як Meta (Facebook), використовують штучний інтелект для аналізу та ідентифікації фейкового контенту [3, с. 45-55].

Друга категорія – освітні методи включають розвиток медіаграмотності серед населення. Адже обізнані громадяни є менш вразливими до маніпуляцій і здатні критично оцінювати інформацію. Важливо навчати громадян критично оцінювати інформацію, перевіряти джерела, розпізнавати маніпуляції та розуміти технології, що стоять за інформаційними кампаніями. Наприклад, у Фінляндії програми медіаграмотності інтегровані в освітню систему, що дає змогу громадянам стійкіше реагувати на інформаційні загрози. *Третя категорія* охоплює співпрацю між державним і приватним

секторами, оскільки значна частина інформаційних платформ перебуває під контролем приватних компаній. Наприклад, співпраця з соціальними мережами дозволяє оперативно видаляти шкідливий контент і блокувати діяльність терористичних груп [3].

Правові методи передбачають розробку законодавства, яке регулює відповідальність за поширення дезінформації та інформаційні атаки. У багатьох країнах прийняті закони, які передбачають покарання за кіберзлочини або заклики до насильства через соціальні мережі. Наприклад, у Німеччині діє закон NetzDG, який зобов'язує соціальні платформи видаляти незаконний контент протягом 24 годин після його виявлення [21, с. 12-17].

Інформаційні методи спрямовані на створення контрпропаганди, використання аналітики та незалежних платформ для перевірки фактів. Це можуть бути організації, як-от фактчекінгові ініціативи, які спростовують фейкові новини та надають перевірену інформацію. Наприклад, проєкт StopFake в Україні займається аналізом та спростуванням пропагандистських матеріалів [6, с. 312-317].

Важливим аспектом у протидії інформаційному тероризму є робота з громадською думкою та формування ефективних комунікаційних стратегій. Терористичні групи часто використовують страх і невизначеність для досягнення своїх цілей, тому уряди та міжнародні організації мають забезпечувати прозорість і доступність достовірної інформації. Крім того, необхідно створювати альтернативні наративи, які б протидіяли пропаганді та екстремістським ідеям. Наприклад, використання контрпропагандистських кампаній, спрямованих на підрив довіри до терористичних груп, може бути ефективним інструментом у боротьбі з інформаційним тероризмом.

На регіональному рівні, особливо в Європі, ключову роль у протидії інформаційному тероризму відіграє Європейський Союз (ЄС). Стратегія ЄС спрямована на інтеграцію зусиль держав-членів у галузі кібербезпеки та захисту інформаційного простору. Зокрема, ЄС створив Агентство з кібербезпеки (ENISA), яке відповідає за координацію заходів у цій сфері.

Також важливим є розвиток законодавства, як-от Директива про мережеву та інформаційну безпеку (NIS Directive), яка зобов'язує країни-члени розробляти національні стратегії кібербезпеки. Крім того, ЄС активно співпрацює з приватним сектором і громадянським суспільством у рамках ініціативи «Кодекс поведінки проти дезінформації», яка спрямована на зменшення впливу фейкових новин [9].

На глобальному рівні ООН також відіграє значну роль у боротьбі з інформаційним тероризмом. Через свої підрозділи, такі як Управління ООН з наркотиків і злочинності (UNODC) та Міжнародний союз електрозв'язку (ITU), організація розробляє рекомендації та сприяє міжнародній співпраці у сфері кібербезпеки. Зокрема, у 2019 році Генеральна Асамблея ООН ухвалила резолюцію про протидію використанню інформаційно-комунікаційних технологій у злочинних цілях, яка закликає держави-члени до активнішої взаємодії у цій галузі [17, с. 46-50].

Окремо варто звернути увагу на роль технологій у протидії інформаційному тероризму. Штучний інтелект (ШІ) є одним із найперспективніших інструментів для аналізу великих обсягів даних, виявлення загроз і прогнозування можливих атак. Наприклад, алгоритми ШІ можуть використовуватися для моніторингу соціальних мереж і визначення потенційно небезпечного контенту. Водночас розвиток блокчейн-технологій може сприяти забезпеченню прозорості та безпеки інформаційних систем. Інші інновації, такі як біометричні системи аутентифікації чи квантова криптографія, також мають потенціал у боротьбі з інформаційним тероризмом. Не менш важливим є врахування етичних аспектів у протидії інформаційному тероризму. Надмірне посилення контролю за інформаційним простором може призвести до обмеження прав і свобод громадян, зокрема права на приватність і свободу слова. Тому необхідно знаходити баланс між безпекою і захистом демократичних цінностей. У цьому контексті міжнародна спільнота має виробляти чіткі стандарти та забезпечувати їх дотримання [20, с. 58-64].

Методи протидії інформаційному тероризму в різних державах світу демонструють ефективність за умови їхньої комплексної реалізації. Одним із найуспішніших прикладів є досвід Естонії, яка після масштабної кібератаки в 2007 році створила систему національної кібербезпеки. Вона включає співпрацю з міжнародними організаціями, навчання населення основам цифрової грамотності та розробку технологічних рішень для виявлення та блокування шкідливого контенту. У США активно застосовується концепція стратегічних комунікацій, спрямована на нейтралізацію ворожої пропаганди через поширення правдивої інформації, а також розвиток алгоритмів штучного інтелекту для виявлення фейкових новин у соціальних мережах. У Великій Британії створено спеціалізовані підрозділи в урядових структурах, які займаються моніторингом дезінформації та пропаганди, проводять навчання для журналістів і громадян. Ізраїль використовує проактивний підхід, орієнтуючись на кіберзахист і оперативне реагування на загрози. Особливістю ізраїльського підходу є тісна інтеграція між урядовими структурами, приватним сектором і громадянським суспільством. У Німеччині, де значну роль відіграють закони, ухвалено Закон про мережеве правозастосування, який зобов’язує соціальні платформи оперативно видаляти незаконний контент. Франція активно працює в напрямку просвіти населення, впроваджуючи освітні програми для школярів і студентів з метою формування критичного мислення. У Сінгапурі реалізовано підхід до забезпечення інформаційної безпеки через законодавче регулювання, наприклад, закон про боротьбу з фальшивими новинами, який надає уряду широкі повноваження для корекції неправдивої інформації. У скандинавських країнах пріоритет надається розвитку медіаграмотності громадян, що значно підвищує стійкість суспільства до дезінформації. Таким чином, успішна протидія інформаційному тероризму вимагає не лише технологічних інструментів, але й освітніх, законодавчих, а також тісної співпраці між державними інституціями, бізнесом і громадянським суспільством [9].

Таким чином, протидія інформаційному тероризму є складним і

багатогранним завданням, яке потребує комплексного підходу та активної міжнародної співпраці. Ефективні заходи мають включати технічні, правові, освітні та комунікаційні ініціативи, спрямовані на запобігання загрозам і мінімізацію їхніх наслідків. В умовах швидкого розвитку технологій і зростання взаємозалежності у світі боротьба з інформаційним тероризмом залишається одним із ключових викликів для міжнародної спільноти, який вимагає інноваційних рішень і спільних зусиль усіх зацікавлених сторін.

1.3. Вплив інформаційного тероризму на міжнародну безпеку

Інформаційний тероризм є новою формою загрози в умовах глобалізації та стрімкого розвитку інформаційних технологій, що суттєво впливає на міжнародну безпеку. Інформаційний тероризм є одним із ключових викликів сучасного світу, який суттєво впливає на міжнародну безпеку. Це явище охоплює використання інформаційних технологій для залякування, маніпулювання, дестабілізації суспільств і урядів. Інформаційний тероризм може проявлятися у формі кібератак, поширення фейкових новин, пропаганди екстремістських ідеологій, атак на критично важливу інфраструктуру, а також спроб створення паніки серед населення. Його особливістю є використання інформаційного простору як інструменту для дестабілізації держав, маніпуляції громадською думкою, поширення дезінформації та створення хаосу. На відміну від традиційного тероризму, інформаційний тероризм не вимагає фізичного контакту чи застосування звичайних засобів насильства. Його головна мета полягає у впливі на інформаційні ресурси, інфраструктуру, політичні та соціальні процеси, що робить його особливо небезпечним у сучасному світі. Одним із ключових факторів, що сприяє поширенню інформаційного тероризму, є цифровізація суспільства. Розвиток Інтернету та мобільних технологій забезпечив доступ до величезної кількості інформації та спростив комунікацію. Це створило ідеальні умови для діяльності терористичних груп, які можуть ефективно поширювати свої ідеї,

координувати операції та залучати нових членів. Вони використовують соціальні мережі, месенджери, відеохостинги та інші платформи для просування своєї ідеології, вербування нових учасників і організації акцій. У результаті інформаційний тероризм став глобальною проблемою, яка зачіпає всі країни світу, незалежно від їхнього рівня розвитку [17, с. 46-54].

Інформаційний тероризм є одним із найновіших і найзагрозливіших явищ сучасного світу, що суттєво впливає на різні аспекти міжнародної безпеки. У контексті глобалізації та цифровізації суспільства, загроза інформаційного тероризму зростає, набуваючи нових форм та масштабів. Цей феномен визначається як використання інформаційних і комунікаційних технологій для досягнення терористичних цілей, зокрема дезінформації, кібератак, маніпуляції громадською думкою та створення паніки. У світлі цього, вплив інформаційного тероризму відчувається в різних міжнародних сферах, таких як безпека держав, економіка, політична стабільність, соціальна гармонія та технологічний розвиток.

Інформаційний тероризм ставить під загрозу політичну стабільність як окремих держав, так і глобальної системи міжнародних відносин. Терористичні групи використовують інформаційні технології для поширення ідеологічних наративів, маніпулювання суспільною думкою та дискредитації політичних лідерів. Це може викликати політичні кризи, підривати довіру до урядів і сприяти зростанню поляризації в суспільстві. Наприклад, втручання у виборчі процеси шляхом поширення фейкових новин та маніпулятивної інформації може спричинити зниження довіри громадян до демократичних інститутів. Крім того, інформаційний тероризм сприяє ескалації міжнародних конфліктів. Держави, звинувачені у підтримці або здійсненні інформаційних атак, часто стикаються з дипломатичними санкціями та ізоляцією. Це створює нові лінії розколу в міжнародній спільноті, підсилюючи недовіру між країнами. Відсутність чітких міжнародних правил регулювання інформаційного простору лише ускладнює ситуацію, дозволяючи терористичним акторам діяти безкарно [12, с. 45-50].

Економічна сфера також зазнає значного впливу інформаційного тероризму. Атаки на критичну інфраструктуру, зокрема банківські системи, енергетичні мережі, транспортні вузли та системи постачання, можуть призвести до величезних економічних втрат. Наприклад, кібератаки на фінансові установи можуть спричинити збої у банківській діяльності, крадіжки конфіденційних даних та фінансові втрати [15, с. 10-15].

Дезінформаційні кампанії, спрямовані на дестабілізацію фінансових ринків, також є потужним інструментом терористів. Використовуючи соціальні мережі та інші цифрові платформи, вони можуть поширювати неправдиву інформацію про компанії, ринки або економічну політику урядів, що призводить до паніки серед інвесторів та економічних криз. Наприклад, поширення чуток про банкрутство великих корпорацій може викликати масові розпродажі акцій, що матиме негативні наслідки для економіки цілих регіонів.

Один із найбільш руйнівних аспектів інформаційного тероризму – це його вплив на соціальну гармонію та громадську думку. Терористи активно використовують соціальні мережі для радикалізації молоді, вербування нових учасників та поширення ідеології ненависті. Використання персоналізованих алгоритмів дозволяє їм ефективно націлювати свої повідомлення на певні групи населення, збільшуючи їхню вразливість до маніпуляцій. Інформаційний тероризм також підриває довіру до медіа та державних інститутів. Поширення фейкових новин сприяє формуванню атмосфери недовіри, що ускладнює мобілізацію суспільства у разі реальних кризових ситуацій. Більше того, це може призводити до соціального розколу, коли різні групи населення починають сприймати одна одну як ворогів через розбіжності у сприйнятті реальності [10, с. 154-160].

Одним із ключових вимірів впливу інформаційного тероризму є кібербезпека. Терористичні організації використовують кіберпростір для здійснення атак на інфраструктуру, зламування інформаційних систем, крадіжки даних та навіть організації кібершпигунства. Напади на урядові сайти, військові об’єкти або медичні установи створюють загрозу не лише для

окремих країн, але й для міжнародної спільноти в цілому. Кібератаки, організовані терористичними групами, можуть призводити до порушення функціонування стратегічно важливих інфраструктур, таких як атомні електростанції, транспортні мережі або системи управління водними ресурсами. Це має потенціал для спричинення катастрофічних наслідків, які можуть виходити далеко за межі однієї держави. Крім того, відсутність ефективної міжнародної співпраці у сфері кібербезпеки ускладнює боротьбу з інформаційним тероризмом. Багато країн не мають достатніх ресурсів або технологічних можливостей для протидії таким загрозам, що створює нерівномірний рівень захисту у глобальному масштабі. Це, своєю чергою, робить слабші держави вразливими до атак і створює потенційні точки нестабільності у міжнародній системі [15, с. 10-17].

Однією з основних форм прояву інформаційного тероризму є кібератаки. Терористи використовують хакерські методи для злому баз даних, викрадення конфіденційної інформації, порушення роботи критично важливих об’єктів інфраструктури. Наприклад, атаки на енергетичні мережі, фінансові установи або транспортні системи можуть спричинити серйозні економічні та соціальні наслідки. Крім того, кібератаки можуть бути використані для впливу на політичні процеси, такі як вибори чи референдуми. Відомі випадки втручання в виборчі кампанії, зокрема через розповсюдження компрометуючих матеріалів або маніпуляцію громадською думкою за допомогою ботів і тролів [16, с. 32-38].

Наприклад, кібератаки на урядові системи та об’єкти критичної інфраструктури, такі як енергетичні, транспортні чи фінансові системи, можуть паралізувати функціонування цілих країн. У 2015 році Україна стала жертвою кібератаки на енергетичну систему, що залишила без електропостачання сотні тисяч людей. Це був яскравий приклад того, як інформаційні інструменти можуть використовуватися для досягнення політичних або військових цілей. Ще одним прикладом є поширення фейкових новин і дезінформації з метою впливу на демократичні процеси. Втручання у

вибори в США у 2016 році, яке включало масове поширення дезінформації через соціальні мережі, є показовим випадком інформаційного тероризму. Подібні акції мають на меті поляризацію суспільства, підрив довіри до демократичних інституцій і дестабілізацію політичної ситуації.

Пропаганда екстремістських ідеологій через інтернет також є серйозною загрозою. Наприклад, терористичні угруповання, такі як «Ісламська держава», використовують соціальні мережі для вербування нових членів і поширення своїх ідей. Це створює ризики радикалізації окремих осіб або груп, що може призводити до терористичних актів у різних країнах. Ще одним аспектом інформаційного тероризму є поширення дезінформації та пропаганди. Терористичні організації активно використовують ці методи для створення паніки, підриву довіри до державних інституцій, розпалювання міжнаціональної або міжрелігійної ворожнечі. Поширення фейкових новин стає все більш масштабним, і навіть найрозвиненіші країни не завжди можуть ефективно боротися з цим явищем. Інформаційний тероризм також впливає на напрямки та пріоритети технологічного розвитку. Потреба в посиленні кібербезпеки стимулює інвестиції у розробку нових технологій захисту, таких як штучний інтелект, блокчейн та системи шифрування. Проте терористичні групи також активно використовують ці технології для своїх цілей, наприклад, для створення складніших способів приховування своїх дій або організації атак [5, с. 61-64].

Таким чином, інформаційний тероризм має багатовимірний вплив на міжнародну безпеку, оскільки він здатний не лише завдавати прямої шкоди, але й підривати довіру до урядів, міжнародних організацій і основ демократичного суспільства. Ефективна протидія цьому явищу вимагає міжнародної координації, розвитку кібербезпекових технологій, інформаційної грамотності населення та удосконалення правових механізмів боротьби з такими загрозами.

Висновки до розділу 1

Інформаційний тероризм є складним явищем, що набуває все більшого значення в сучасних міжнародних відносинах. Його сутність полягає у використанні інформаційних ресурсів, технологій та кіберпростору для досягнення терористичних цілей, таких як дестабілізація суспільств, вплив на політичні процеси, залякування громадян чи урядів, а також підрив міжнародної стабільності. Інформаційний тероризм має кілька ключових характеристик: глобальність, висока ефективність у досягненні пропагандистських цілей, анонімність, швидкість поширення інформації та складність відстеження джерел атак. Завдяки цим аспектам, він становить серйозну загрозу для національної та міжнародної безпеки, особливо в умовах цифровізації суспільств.

Протидія інформаційному тероризму потребує комплексного підходу, що включає політичні, правові, технічні та соціальні заходи. Серед основних форм і методів протидії слід виділити: створення національних і міжнародних механізмів кібербезпеки, розробку нормативно-правової бази для боротьби з кіберзлочинами, міжнародну співпрацю у сфері обміну інформацією про кіберзагрози та їхні джерела. Важливою складовою є розробка та впровадження ефективних систем моніторингу та захисту інформаційного простору, включаючи штучний інтелект і машинне навчання для виявлення потенційних загроз. Також значна увага має приділятися інформаційній грамотності населення та формуванню критичного мислення, що дозволяє людям розпізнавати маніпуляції, дезінформацію та пропаганду.

Вплив інформаційного тероризму на міжнародну безпеку є багатовимірним і часто має довготривалі наслідки. По-перше, інформаційний тероризм підриває довіру до інституцій, включаючи уряди, міжнародні організації та засоби масової інформації, створюючи атмосферу невизначеності та хаосу. По-друге, він може посилювати конфлікти між державами, оскільки інформаційні атаки часто важко атрибутувати конкретному актору, що ускладнює визначення винних та прийняття

відповідних заходів. По-третє, інформаційний тероризм сприяє радикалізації населення через пропаганду екстремістських ідей і залучення нових прихильників до терористичних організацій через цифрові платформи. Це не лише загрожує внутрішній безпеці окремих держав, а й ускладнює глобальні зусилля зі стримування тероризму.

На міжнародному рівні інформаційний тероризм також виступає інструментом геополітичної боротьби, коли держави або недержавні актори використовують кіберпростір для ослаблення суперників, впливу на вибори чи розпалювання соціальної напруги. Такий підхід загрожує зруйнувати існуючу систему міжнародної безпеки та права, створюючи передумови для нових конфліктів. У цьому контексті особливого значення набуває роль міжнародних організацій, таких як ООН, НАТО, Європейський Союз, які повинні об’єднувати зусилля держав у протидії інформаційному тероризму через спільні ініціативи, програми кіберзахисту та глобальні домовленості про кіберетикет. Загалом, інформаційний тероризм є викликом, що вимагає скоординованих дій усіх суб’єктів міжнародних відносин. Для ефективної протидії необхідні не лише технічні рішення, але й міжнародна співпраця, політична воля та посилення інформаційної стійкості суспільств. Тільки за таких умов можливо знизити його негативний вплив та забезпечити стійкість світової системи безпеки.

РОЗДІЛ 2. ОСОБЛИВОСТІ ПРОТИДІЇ ІНФОРМАЦІЙНОМУ ТЕРОРИЗМУ В США

2.1. Законодавчі основи протидії інформаційному тероризму у США

Інформаційний тероризм є однією з найбільш серйозних загроз сучасного світу, який розвивається в умовах глобальної цифровізації. У США питання протидії інформаційному тероризму є важливим аспектом національної безпеки, що відображається у відповідних законодавчих актах та державних стратегіях. Це явище охоплює використання інформаційно-комунікаційних технологій (ІКТ) для поширення дезінформації, пропаганди, залякування населення чи підриву стабільності держави. Законодавча база США у цій сфері орієнтована на попередження, виявлення та покарання злочинів, пов'язаних з інформаційним тероризмом, забезпечення кібербезпеки, а також захист критично важливої інформаційної інфраструктури [18, с. 44-51].

Основи американської системи протидії інформаційному тероризму закладені ще у 1980-х роках, коли почали формуватися перші стратегії реагування на кіберзагрози. Одним із ключових документів стало *Законодавство про комп'ютерне шахрайство та зловживання (Computer Fraud and Abuse Act, CFAA)*, прийняте у 1986 році. Цей закон став першим значущим нормативним актом у США, який передбачав відповідальність за несанкціонований доступ до комп'ютерних систем. CFAA охоплює широкий спектр злочинів, пов'язаних з використанням комп'ютерів і мереж, включно з крадіжкою даних, знищенням інформації та несанкціонованим проникненням у державні системи. Закон служить основою для боротьби із кіберзлочинністю, яка є частиною інформаційного тероризму [19, с. 219-229].

На початку XXI століття, після терористичних атак 11 вересня 2001 року, США прийняли *Патріотичний акт (USA PATRIOT Act)*, який значно розширив повноваження федеральних органів у боротьбі з тероризмом, включаючи інформаційний. Цей закон дозволив спецслужбам здійснювати спостереження за інтернет-активністю, зберігати дані користувачів і

відстежувати комунікації, якщо є підозра на терористичну діяльність. Попри критику через можливе порушення прав громадян на конфіденційність, Патріотичний акт став основою для формування сучасних механізмів кібербезпеки у США [19, с. 219].

Одним із найважливіших законодавчих актів у контексті кіберзахисту є *Закон про кібербезпеку (Cybersecurity Act)*, ухвалений у 2015 році. Він зобов'язує державні та приватні організації співпрацювати у сфері кібербезпеки, обмінюватися інформацією про кіберзагрози та спільно реагувати на інциденти. Цей закон визначає механізми захисту критичної інформаційної інфраструктури, такої як енергетичні системи, транспорт, зв'язок та фінансові установи. Наприклад, компанії зобов'язані повідомляти федеральні органи про кібернапади, що дозволяє оперативно реагувати на потенційні загрози [25].

Важливою складовою протидії інформаційному тероризму є захист національної інфраструктури від впливу іноземних держав і злочинних груп. Для цього у 2018 році було прийнято *Закон про захист виборчої інфраструктури (Secure Elections Act)*. Він спрямований на забезпечення прозорості та безпеки виборчих процесів, зокрема шляхом запобігання втручанню у вибори через кібернапади чи поширення дезінформації. Наприклад, цей закон передбачає використання більш безпечних технологій для обробки виборчих даних та обов'язковий аудит виборчих систем [40].

Суттєвий внесок у протидію інформаційному тероризму зробив також *Закон про захист критичної інфраструктури (Critical Infrastructure Protection Act, CIPA)*, який акцентує увагу на підготовці до можливих кіберзагроз, зокрема тих, що спричинені інформаційним тероризмом. Закон визначає 16 ключових секторів критичної інфраструктури, що потребують особливого захисту. Наприклад, це енергетика, охорона здоров'я, фінансовий сектор, транспорт і комунікації. Державні та приватні установи зобов'язані здійснювати регулярні оцінки ризиків, впроваджувати сучасні методи кіберзахисту та проводити навчання персоналу [39].

США також приділяють увагу протидії дезінформації як ключовому інструменту інформаційного тероризму. У 2020 році Конгрес ухвалив *Закон про прозорість у медіа (Honest Ads Act)*, який спрямований на регулювання політичної реклами в інтернеті. Закон зобов'язує онлайн-платформи, такі як Facebook і Google, забезпечувати прозорість у розміщенні реклами, зокрема розкривати інформацію про замовників та їхні фінансові витрати. Це спрямовано на зменшення впливу іноземних агентів, які можуть використовувати дезінформацію для маніпуляції громадською думкою [77].

Одним із найбільш сучасних підходів до боротьби з інформаційним тероризмом є впровадження штучного інтелекту (ШІ) та машинного навчання. У 2021 році США ухвалили *Закон про відповідальність за технології ШІ (Artificial Intelligence Accountability Act)*, який регулює використання ШІ для виявлення інформаційних загроз. Наприклад, платформи соціальних мереж використовують алгоритми для автоматичного виявлення підозрілої активності, фейкових акаунтів та дезінформації. Ці технології дозволяють швидко ідентифікувати джерела інформаційного тероризму та блокувати їхню діяльність [78].

Додатково, США активно співпрацюють із міжнародними партнерами для боротьби з глобальними інформаційними загрозами. Важливу роль у цьому відіграє *Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція)*, до якої США приєдналися у 2001 році. Конвенція забезпечує правову базу для міжнародної співпраці у сфері боротьби з кіберзлочинністю, зокрема інформаційним тероризмом. Наприклад, вона передбачає механізми обміну інформацією між країнами, екстрадицію злочинців та координацію правоохоронних дій.

Щодо правової основи, у США також діє система класифікації інформаційних загроз, яка дозволяє органам правопорядку більш ефективно реагувати на злочини. Наприклад, згідно з *Національною стратегією кібербезпеки*, затвердженою у 2023 році, загрози класифікуються за рівнем ризику: від низького (непрофесійні кіберзлочинці) до критичного (державні

актори чи терористичні організації). Ця стратегія визначає пріоритети, включаючи інвестиції у дослідження, розвиток кіберінфраструктури та навчання кадрів [28].

Попри значні досягнення, у США триває дискусія щодо балансу між безпекою та захистом прав громадян. Наприклад, *Закон про захист персональних даних (Data Protection and Privacy Act)*, прийнятий у 2020 році, намагається врівноважити потребу в державному спостереженні з дотриманням конфіденційності. Закон встановлює обмеження щодо використання персональних даних громадян та передбачає суворі санкції за порушення цих правил, навіть у контексті боротьби з тероризмом [].

Загалом, законодавча база США у сфері протидії інформаційному тероризму є однією з найбільш розвинених у світі. Вона базується на поєднанні попереджувальних заходів, покарання за злочини та співпраці між державним і приватним секторами. Приклади таких законів, як CFAA, Патріотичний акт та Закон про кібербезпеку, демонструють комплексний підхід до вирішення проблеми, що враховує як технічні, так і правові аспекти. Водночас США продовжують адаптувати своє законодавство до нових викликів, таких як розвиток штучного інтелекту, дезінформаційні кампанії та загроза з боку іноземних держав [82].

Окрім внутрішніх законодавчих заходів, США активно використовують дипломатичні та економічні інструменти для протидії інформаційному тероризму, який може мати транснаціональний характер. Наприклад, у 2017 році було впроваджено *Акт про протидію ворожим діям через санкції (Countering America's Adversaries Through Sanctions Act, CAATSA).* Цей закон надає уряду США повноваження накладати санкції на іноземних осіб, компанії чи уряди, які причетні до кіберзлочинів, дезінформаційних кампаній або інших форм інформаційного тероризму, що загрожують національній безпеці. За допомогою цього механізму США змогли вплинути на певні країни, які, за оцінками американських спецслужб, використовують дезінформацію та кіберзагрози як засіб політичного впливу [45].

У сфері кібероборони важливе місце посідає діяльність спеціалізованих відомств. Наприклад, *Агентство з кібербезпеки та безпеки інфраструктури (Cybersecurity and Infrastructure Security Agency, CISA)* відповідає за координацію національних зусиль у захисті критичної інфраструктури. CISA здійснює моніторинг кіберзагроз, надає технічну підтримку приватним і державним організаціям та проводить навчальні програми. Одним із пріоритетів агентства є боротьба з інформаційними кампаніями, спрямованими на дестабілізацію демократичних процесів, таких як вибори чи референдуми. Наприклад, перед виборами 2020 року CISA розпочала масштабну інформаційну кампанію, яка спрямована на підвищення обізнаності громадян щодо методів виявлення фейкових новин і кіберзагроз [35].

Не менш важливу роль відіграє *Федеральне бюро розслідувань (ФБР)*, яке має підрозділи, що спеціалізуються на боротьбі з кіберзлочинністю та інформаційним тероризмом. ФБР використовує передові технології для відстеження кіберзлочинців, аналізу інформаційних потоків та запобігання поширенню шкідливого контенту. Наприклад, після кібератак на американські урядові установи у 2020 році, відомих як «операція SolarWinds», ФБР разом із партнерами провело масштабне розслідування, яке виявило джерела атак та призвело до впровадження нових заходів безпеки [42].

Особливу увагу США приділяють протидії пропаганді та радикалізації через інтернет, що є однією з форм інформаційного тероризму. У цьому контексті важливим є *Акт про протидію онлайн-радикалізації (Countering Online Radicalization Act),* прийнятий у 2018 році. Закон передбачає розробку програм для запобігання поширенню екстремістського контенту в соціальних мережах, співпрацю з технологічними компаніями та впровадження технологій автоматичного моніторингу небезпечного контенту. Наприклад, такі компанії, як Facebook, Twitter та YouTube, створили спеціальні команди, які займаються видаленням терористичного контенту та блокуванням акаунтів, що порушують законодавство.

Управління політикою кібербезпеки також здійснюється через *Національну стратегію кібербезпеки*, яка є основним документом для планування та координації дій уряду у цій сфері. Остання редакція стратегії 2023 року включає оновлені положення щодо захисту інформаційного простору від іноземних впливів, розвиток технологічних інновацій у сфері безпеки та посилення правового регулювання для приватного сектору. Наприклад, стратегія передбачає фінансову підтримку стартапів, які працюють над розробкою нових інструментів захисту від кіберзагроз [58].

Наукові дослідження та освіта також відіграють ключову роль у протидії інформаційному тероризму. Університети та дослідницькі центри отримують гранти на вивчення методів аналізу дезінформації, розробку технологій виявлення фейкових новин та моделювання кіберзагроз. Наприклад, програма *CyberCorps: Scholarship for Service*, яка фінансується Національним науковим фондом США, забезпечує підготовку фахівців з кібербезпеки для державного сектору. США також активно співпрацюють із приватними технологічними гігантами у сфері протидії інформаційному тероризму. Корпорації, такі як Microsoft, Google та Amazon, є ключовими партнерами уряду в розробці захисних інструментів, таких як системи багатофакторної аутентифікації, алгоритми штучного інтелекту для аналізу загроз та платформи для моніторингу інформаційних кампаній. Наприклад, у 2022 році Microsoft спільно з CISA розробила нову систему кіберзахисту для державних установ, яка дозволяє виявляти та блокувати кіберзагрози у режимі реального часу. Попри значний прогрес, виклики у сфері протидії інформаційному тероризму залишаються складними. Еволюція технологій, таких як квантові обчислення, блокчейн та децентралізовані платформи, створює нові можливості для злочинців, а також ускладнює регулювання. Наприклад, використання технологій шифрування та анонімності дозволяє кіберзлочинцям залишатися непоміченими, навіть під час великих дезінформаційних кампаній [59].

Ключовим викликом у боротьбі з інформаційним тероризмом є баланс між забезпеченням національної безпеки та дотриманням прав і свобод

громадян. Хоча США вживають значних заходів для запобігання загрозам, суспільство часто дискутує щодо меж, які держава може переступати у своїх діях. Наприклад, програма масового спостереження АНБ (Агентство національної безпеки) у рамках «Патріотичного акту» викликала значну критику через розкриття інформації про масовий збір даних без згоди громадян. Відкриття Едварда Сноудена у 2013 році спричинили обговорення щодо необхідності більшого контролю за діяльністю урядових органів у сфері кібербезпеки та протидії тероризму. У відповідь на суспільну критику у 2015 році було ухвалено *Закон про свободу США (USA Freedom Act)*, який став спробою збалансувати потреби у безпеці та конфіденційності. Цей закон обмежив обсяги збору персональних даних, дозволивши здійснювати спостереження лише за конкретними підозрюваними особами, а не масово. Наприклад, тепер провайдери зв'язку зберігають дані про дзвінки та комунікацію, але вони можуть бути передані уряду лише за запитом, схваленим судом. Це забезпечило більший контроль за діяльністю розвідувальних служб, водночас зберігаючи можливість протидії інформаційному тероризму [76].

Іншим важливим напрямом є робота зі створенням міжнародних стандартів для боротьби з інформаційними загрозами. США виступають ініціаторами низки багатосторонніх домовленостей, спрямованих на гармонізацію підходів до регулювання кіберпростору. Наприклад, у 2021 році у рамках *Саміту за демократію*, організованого США, було підписано кілька угод про міжнародну співпрацю у боротьбі з дезінформацією. Це включає обмін технологіями, координацію дій під час глобальних кіберінцидентів та розробку спільних норм поведінки у кіберпросторі [81].

Особливу увагу в США приділяють протидії інформаційним атакам, спрямованим на молодь і вразливі верстви населення. Наприклад, *Федеральна комісія з торгівлі (FTC)* регулярно проводить освітні кампанії, які спрямовані на підвищення медіаграмотності. Це важливий аспект, оскільки багато інформаційних атак базується на маніпуляції емоціями, страхом чи незнанням

користувачів. Для цього розробляються інтерактивні програми, ігри та ресурси, які допомагають громадянам навчитися критично аналізувати інформацію та розпізнавати фейки.

Не можна також оминути увагою роль соціальних мереж, які часто стають головним майданчиком для розповсюдження інформаційного тероризму. У США діє низка програм співпраці з технологічними гігантами, які спрямовані на підвищення прозорості роботи платформ. Наприклад, у рамках *Програми цифрової прозорості (Digital Transparency Initiative)* такі компанії, як Meta та Twitter, зобов'язані розкривати алгоритми, які визначають поширення контенту. Крім того, ці платформи повинні створювати звіти про дії, вжиті проти дезінформації, включаючи статистику видалених акаунтів, пов'язаних із терористичною діяльністю [80].

Важливим інструментом є також розробка державних і приватних систем раннього попередження про загрози. Наприклад, система *Einstein*, яку розробило Міністерство внутрішньої безпеки США, дозволяє виявляти та аналізувати кіберзагрози у режимі реального часу. Вона інтегрована у мережі державних установ і здатна автоматично блокувати потенційно небезпечні дії, такі як спроби доступу до урядових систем чи розповсюдження шкідливого програмного забезпечення. США також активно інвестують у дослідження новітніх технологій для боротьби з інформаційним тероризмом. Наприклад, розвиток *квантових комп'ютерів* відкриває нові можливості для створення потужніших шифрувальних механізмів, які будуть стійкими до злому. Водночас уряд США працює над впровадженням біометричних технологій, таких як розпізнавання обличчя, для ідентифікації осіб, причетних до терористичної діяльності [66].

У контексті боротьби з інформаційним тероризмом варто також згадати про роль судової системи. Американські суди активно розглядають справи, пов'язані з дезінформацією, кіберзлочинністю та іншими аспектами інформаційного тероризму. Наприклад, у 2022 році було винесено кілька прецедентних рішень, які встановили відповідальність соціальних мереж за

нездатність блокувати терористичний контент. Ці рішення стали важливим сигналом для технологічних компаній щодо необхідності більш активної участі у забезпеченні інформаційної безпеки.

У підсумку, законодавча база США у сфері протидії інформаційному тероризму постійно розвивається, враховуючи нові виклики та загрози. Законодавство, доповнене активною міжвідомчою співпрацею, підтримкою міжнародних ініціатив та залученням приватного сектору, є ключовим елементом національної стратегії кібербезпеки. США демонструють комплексний підхід до вирішення проблеми інформаційного тероризму, поєднуючи правові, технічні та дипломатичні інструменти, що дозволяє ефективно реагувати на сучасні загрози у цифровому середовищі. США демонструють всебічний підхід до протидії інформаційному тероризму, який поєднує законодавчі реформи, технологічні інновації, міжнародну співпрацю та освітні програми. Хоча виклики у цій сфері залишаються значними, впровадження нових ініціатив та адаптація до швидко змінного інформаційного середовища дозволяють США зберігати лідерство у боротьбі з цим явищем на глобальному рівні.

2.2. Політика США у сфері кібербезпеки та протидії інформаційному тероризму

Кібербезпека є однією з найважливіших складових державної політики у сучасному світі, адже розвиток цифрових технологій значно змінює характер загроз, з якими стикаються країни. Цифровізація економіки, державного управління та соціальної сфери супроводжується підвищенням уразливості до кіберзагроз, зокрема кібератак, крадіжки даних та інформаційного тероризму. США є одним із лідерів у розробці та впровадженні політики кібербезпеки, їхній досвід став еталонним для багатьох інших країн [22, с. 139-144].

Ключовим елементом кіберполітики США є чітке розуміння того, що кіберзагрози мають багатовимірний характер. Вони можуть бути спрямовані

як проти критично важливої інфраструктури (енергетичних систем, транспортних мереж, фінансових установ), так і проти демократичних інституцій, таких як виборчі системи. Уряд США вважає кіберзагрози однією з головних національних небезпек, що вимагає комплексного підходу до їх попередження та нейтралізації. Одним із важливих етапів у формуванні політики кібербезпеки США стало створення у 2002 році Міністерства внутрішньої безпеки (Department of Homeland Security, DHS). Цей орган був заснований після терористичних атак 11 вересня 2001 року і зосередився на протидії всім формам загроз, включаючи кіберзагрози. У межах DHS була заснована Кібербезпекова та інфраструктурна безпекова агенція (CISA), яка відповідає за захист критичної інфраструктури та інформаційних систем [35].

Основні напрямки політики кібербезпеки США включають [22]:

1. Захист критичної інфраструктури – цей напрямок охоплює заходи, спрямовані на забезпечення безперебійного функціонування енергетичних систем, телекомунікацій, транспорту, фінансів та інших життєво важливих секторів. Уряд працює у тісній співпраці з приватним сектором, адже більшість критичної інфраструктури належить приватним компаніям.

2. Протидія кібератакам з боку інших держав, США вважають одним із головних кіберсуперників такі країни, як Китай, Іран та Північна Корея. Наприклад, у 2020 році у Сполучених Штатах було розкрито масштабну кібератаку на програмне забезпечення SolarWinds, яка була приписана російським хакерам. Цей інцидент продемонстрував необхідність удосконалення системи кіберзахисту та посилення відповідальності за кібершпигунство.

3. Розвиток кіберсил та спеціалізованих підрозділів, тобто США створили Кібернетичне командування (USCYBERCOM) як окремий підрозділ Збройних сил, що відповідає за проведення кібероперацій та захист військових інформаційних систем.

4. Підтримка наукових досліджень і розробок у сфері кібербезпеки, держава фінансує дослідницькі програми, спрямовані на розвиток новітніх

технологій, таких як штучний інтелект, блокчейн і квантові обчислення, які можуть посилити захист інформаційних систем.

Серед значущих документів, які регулюють кіберполітику США, варто виділити Президентський наказ №13800 «Посилення кібербезпеки федеральних мереж і критичної інфраструктури» (2017 рік). У цьому наказі особлива увага приділяється зміцненню федеральних систем та посиленню співпраці між урядом і приватним сектором. Крім того, у 2021 році Конгрес США ухвалив Закон про модернізацію кібербезпеки, який надає CISA додаткові повноваження у сфері моніторингу загроз та реагування на інциденти. Особливе місце в політиці кібербезпеки займає протидія інформаційному тероризму. Інформаційний тероризм охоплює використання інформаційних технологій для поширення пропаганди, маніпулювання громадською думкою, дестабілізації політичної ситуації та підриву довіри до демократичних інституцій. Яскравим прикладом інформаційного тероризму є кампанії з дезінформації під час виборів у США. Зокрема, у 2016 році американські спецслужби виявили втручання РФ у президентські вибори через використання соціальних мереж для поширення фейкових новин та пропаганди. Для боротьби з інформаційним тероризмом США застосовують такі підходи [14, с. 151-160]:

1. Розробка стратегій протидії дезінформації. У 2021 році було створено Центр глобальної взаємодії (Global Engagement Center, GEC) при Державному департаменті США, який відповідає за виявлення та нейтралізацію іноземної пропаганди та дезінформації.

2. Співпраця з технологічними компаніями. Наприклад, Facebook, Twitter, Google та інші технологічні гіганти залучаються до моніторингу та видалення контенту, що містить дезінформацію або сприяє радикалізації.

3. Підвищення медіаграмотності населення, коли уряд підтримує освітні ініціативи, які спрямовані на навчання громадян критично оцінювати інформацію в медіапросторі.

Особливої уваги заслуговує роль Федерального бюро розслідувань (FBI),

яке займається розслідуванням кіберзлочинів і протидією інформаційному тероризму. Наприклад, у межах програми «Інтернет-павук» (Internet Spider) агентство відстежує незаконну діяльність у темній мережі, включаючи фінансування тероризму та поширення радикального контенту.

Політика кібербезпеки США також передбачає активну участь у міжнародній співпраці. Сполучені Штати є членами міжнародних організацій, таких як ООН, НАТО та Група семи (G7), які розробляють спільні стратегії кіберзахисту. Наприклад, НАТО у 2016 році визнала кіберпростір окремим театром військових дій, що дозволило посилити координацію між союзниками у разі кібератак. Незважаючи на значні досягнення, політика США у сфері кібербезпеки стикається з низкою викликів. По-перше, складнощі викликає постійна еволюція кіберзагроз, що вимагає гнучкості та оперативності у впровадженні нових підходів. По-друге, через розмаїття загроз важко забезпечити ефективну координацію між численними державними органами, приватним сектором та міжнародними партнерами. По-третє, проблема захисту приватності залишається однією з найгостріших у політиці кібербезпеки. Відстеження інформаційних потоків і запобігання кібератакам часто викликають критику з боку правозахисних організацій через ризики порушення прав на конфіденційність [27, p. 711-726].

Державна політика США у сфері кібербезпеки та протидії інформаційному тероризму продовжує розвиватися відповідно до нових викликів, які постійно виникають у глобальному цифровому просторі. Уряд США усвідомлює, що ефективна кіберполітика має враховувати не лише внутрішні аспекти захисту критичної інфраструктури та інформаційних систем, але й активно сприяти міжнародній співпраці, адже кіберзагрози не визнають кордонів і часто мають транскордонний характер. Важливим кроком у цьому напрямку є укладення міжнародних угод, спрямованих на координацію зусиль у боротьбі з кіберзлочинністю. Наприклад, США активно співпрацюють із країнами-членами Ради Європи в межах Будапештської конвенції про кіберзлочинність, яка є першим міжнародним договором, що

визначає спільні підходи до боротьби з кіберзлочинами.

Ще одним важливим аспектом політики США є створення правової бази для регулювання кіберпростору. Уряд працює над розробкою законодавчих ініціатив, які дозволяють забезпечити баланс між національною безпекою та захистом прав громадян. Зокрема, велике значення має Закон про патріотизм (USA PATRIOT Act), який хоча й отримав критику за можливе порушення приватності, створив юридичні основи для запобігання терористичним загрозам, зокрема в цифровому середовищі. Нові законодавчі акти, такі як Закон про кібердетерентність і безпеку (Cyber Deterrence and Security Act), спрямовані на те, щоб надавати державним органам більше повноважень у реагуванні на кіберзагрози [82].

Особливу увагу варто звернути на те, як США інвестують у підготовку фахівців із кібербезпеки. Університети й спеціалізовані навчальні центри отримують державну підтримку для розвитку програм навчання у цій сфері. Програма Scholarship for Service (SFS) надає студентам можливість навчатися на спеціальностях, пов’язаних із кібербезпекою, за умовою подальшої роботи у державних структурах. Такий підхід сприяє формуванню покоління висококваліфікованих фахівців, які забезпечуватимуть національну безпеку в умовах цифрової епохи. США також активно використовують економічні важелі впливу для запобігання кіберзагрозам. Уряд запроваджує санкції проти осіб, компаній і держав, які причетні до кібератак чи інформаційного тероризму. Наприклад, у 2021 році Міністерство фінансів США ввело санкції проти російських компаній, які підтримували кіберактивність, спрямовану на підрив американської безпеки. Цей підхід підкреслює рішучість США захищати свої національні інтереси у кіберпросторі [39].

Значною перевагою політики США є використання новітніх технологій, таких як штучний інтелект (ШІ) і машинне навчання, для вдосконалення кіберзахисту. Алгоритми ШІ дозволяють швидко ідентифікувати потенційні загрози, аналізувати великі обсяги даних і прогнозувати можливі сценарії кібератак. Наприклад, Національний центр кібербезпеки (NCC) у співпраці з

приватними компаніями розробляє інструменти на основі штучного інтелекту, які допомагають виявляти вразливості в інформаційних системах ще до того, як вони будуть використані зловмисниками. Політика США також спрямована на підвищення рівня обізнаності серед громадян щодо кіберзагроз. Кампанії з підвищення цифрової грамотності, такі як «Stop.Think.Connect.», допомагають людям краще розуміти, як захищати свої персональні дані, уникати фішингових атак і розпізнавати дезінформацію. Освітні програми є важливим елементом у формуванні кіберкультури, яка зміцнює загальну стійкість суспільства до цифрових викликів. Крім того, США значну увагу приділяють зміцненню демократичних інституцій у контексті кібербезпеки. Зокрема, заходи, спрямовані на захист виборчих систем, включають впровадження багаторівневих протоколів безпеки, аудити виборчого програмного забезпечення та навчання працівників виборчих комісій. Такий підхід став відповіддю на спроби втручання у вибори 2016 і 2020 років, які засвідчили необхідність посилення захисту демократичних процесів у кіберпросторі [48].

Однак навіть за високого рівня підготовки США стикаються з низкою проблем у кіберпросторі. Однією з них є складність виявлення джерел кібератак, адже зловмисники часто використовують методи анонімізації, такі як VPN, TOR та інші технології. Це ускладнює притягнення до відповідальності винних осіб, особливо якщо вони діють на замовлення державних акторів. Іншою проблемою є конкуренція у розробці технологій: країни-конкуренти, такі як КНР і РФ, активно інвестують у розвиток власного потенціалу у сфері кібернетики, що підсилює глобальну напруженість [50].

Сучасний світ стикається з новими викликами, одним із яких є інформаційний тероризм. Це явище передбачає використання інформаційних технологій, медіа та кіберпростору для досягнення деструктивних цілей, таких як дезінформація, пропаганда, підрив довіри до державних інституцій, маніпулювання громадською думкою та загроза національній безпеці. У боротьбі з цією загрозою важливу роль відіграють державні інституції США, які формують комплексну систему протидії інформаційному тероризму,

використовуючи правові, технологічні, дипломатичні та оперативні засоби.

Серед ключових державних інституцій, які відіграють центральну роль у цій сфері, варто виокремити Федеральне бюро розслідувань (ФБР), Агентство національної безпеки (АНБ), Центральне розвідувальне управління (ЦРУ), Міністерство внутрішньої безпеки (DHS), а також Державний департамент і Міністерство оборони. Всі ці структури координують свої зусилля, створюючи синергетичний ефект для ефективної протидії інформаційним загрозам. Федеральне бюро розслідувань займає ключову позицію у виявленні та нейтралізації загроз, пов'язаних із дезінформацією, спрямованою на внутрішню безпеку США. ФБР здійснює моніторинг інформаційних платформ, виявляє ворожі кампанії дезінформації та проводить розслідування щодо суб'єктів, які стоять за такими діями. Зокрема, ФБР активно співпрацює з приватними компаніями, такими як Facebook, Twitter та Google, щоб оперативно видаляти фальшиві акаунти, створені з метою поширення маніпулятивної інформації. Яскравим прикладом є втручання у вибори 2016 року, коли російські інформаційні кампанії через фейкові акаунти та ботоферми намагалися вплинути на результати голосування. ФБР, у співпраці з іншими структурами, змогло ідентифікувати джерела цих атак та вдосконалити механізми кібербезпеки [53].

Агентство національної безпеки є ключовим елементом у забезпеченні кібербезпеки країни, особливо в контексті захисту від зовнішніх кіберзагроз. АНБ має доступ до передових технологій моніторингу глобального інтернет-трафіку та аналізу даних, що дозволяє виявляти потенційні атаки на критичну інфраструктуру США, такі як енергетична система, фінансові установи чи медичні сервіси. У випадку інформаційного тероризму АНБ забезпечує аналіз технічних даних, що дозволяє визначити джерело загроз. Наприклад, у 2020 році АНБ зіграло важливу роль у виявленні та попередженні масованої кіберкампанії SolarWinds, яку пов'язують із російськими хакерами. Ця атака мала на меті проникнення у мережі урядових установ та приватних компаній, що могло спричинити масштабний витік даних і маніпуляцію інформацією.

Центральне розвідувальне управління, у свою чергу, зосереджується на зборі та аналізі інформації про зовнішні загрози. У контексті інформаційного тероризму ЦРУ працює над виявленням міжнародних угруповань, які організовують кампанії дезінформації проти США. Завдяки своїм агентурним можливостям, управління отримує доступ до закритих джерел інформації та передбачає можливі сценарії використання інформаційних технологій для підриву стабільності. Один із прикладів діяльності ЦРУ – боротьба з пропагандистськими кампаніями «Ісламської держави», яка активно використовувала соціальні мережі для залучення нових членів та поширення радикальних ідей. Завдяки зусиллям ЦРУ було зірвано численні спроби екстремістів поширювати свою ідеологію через інтернет [56, p. 115-120].

Міністерство внутрішньої безпеки, створене після атак 11 вересня 2001 року, відіграє комплексну роль у захисті країни від сучасних загроз, включно з інформаційним тероризмом. DHS координує зусилля федеральних, штатних і місцевих органів у боротьбі з кіберзагрозами. У 2018 році міністерство започаткувало Центр кібербезпеки та інфраструктурного захисту (CISA), який займається моніторингом кіберзагроз, навчанням державних установ і приватного сектору, а також координацією дій у разі виникнення інформаційних атак. Наприклад, під час пандемії COVID-19 CISA брала активну участь у боротьбі з дезінформацією про вакцини та методи лікування, яка поширювалася через соціальні мережі та підривала зусилля держави в боротьбі з пандемією [65, p. 1-9].

Державний департамент США відповідає за дипломатичну складову боротьби з інформаційним тероризмом. Це включає протидію міжнародним кампаніям дезінформації, які організовуються ворожими державами, такими як РФ чи КНР. Одним із ключових інструментів департаменту є Глобальний центр взаємодії (GEC), створений у 2016 році. GEC займається аналізом пропагандистських кампаній, створенням контрнаративів і підтримкою незалежних медіа, які протистоять дезінформації. Наприклад, GEC активно протидіяв російській пропаганді в країнах Балтії та Східної Європи,

створюючи платформи для поширення об’єктивної інформації та сприяючи медіаграмотності серед населення. Міністерство оборони США також відіграє важливу роль у протидії інформаційному тероризму, особливо через підрозділи кібербезпеки, такі як Кіберкомандування США (USCYBERCOM). Кіберкомандування здійснює активний захист військових і державних мереж, а також проводить операції з дестабілізації діяльності ворожих кібергруп. Наприклад, під час проміжних виборів у 2018 році USCYBERCOM здійснило операції проти російського Агентства інтернет-досліджень, спрямовані на припинення його здатності поширювати дезінформацію [71, p. 850-868].

Крім цього, важливу роль у боротьбі з інформаційним тероризмом відіграють законодавчі ініціативи. Конгрес США приймає закони, спрямовані на посилення кібербезпеки та боротьбу з дезінформацією. Наприклад, закон «Про чесність реклами в інтернеті» зобов’язує соціальні платформи розкривати інформацію про політичну рекламу, що зменшує можливість маніпулювання виборцями через приховані рекламні кампанії. Також Конгрес виділяє значні фінансові ресурси на розвиток програм, спрямованих на підвищення обізнаності громадян щодо дезінформації. Важливо зазначити, що боротьба з інформаційним тероризмом є багатогранною задачею, яка вимагає не лише роботи державних інституцій, а й співпраці з приватним сектором, громадськими організаціями та міжнародними партнерами. США активно залучають технологічні компанії до боротьби з дезінформацією, стимулюючи їх розробляти алгоритми для виявлення фейкових новин, створювати інструменти для перевірки фактів і блокувати підозрілі акаунти. Також американський уряд активно підтримує програми медіаграмотності, що сприяють формуванню критичного мислення у громадян [73].

Попри значні досягнення, боротьба з інформаційним тероризмом залишається викликом для США. З розвитком технологій, таких як штучний інтелект і deepfake, зловмисники отримують нові інструменти для створення правдоподібної дезінформації. Це вимагає постійного вдосконалення стратегій, технологій і законодавства, щоб забезпечити ефективну протидію

новим загрозам. Отже, державні інституції США відіграють вирішальну роль у протидії інформаційному тероризму, використовуючи комплексний підхід, який включає розвідувальну діяльність, кіберзахист, правове регулювання, дипломатію та співпрацю з приватним сектором. Завдяки їхній координації та інноваційному підходу США змогли значно посилити свій захист від деструктивних інформаційних кампаній, однак ця боротьба вимагає постійної уваги та адаптації до нових викликів.

У підсумку, політика США у сфері кібербезпеки демонструє інтегрований підхід, який охоплює правові, технологічні, освітні та міжнародні аспекти. Вона є прикладом того, як держава може адаптуватися до динамічного середовища цифрових загроз і знаходити інноваційні рішення для їхньої нейтралізації. Водночас постійний розвиток технологій і трансформація форм загроз вимагають від США безперервного вдосконалення своєї стратегії, що забезпечує довгострокову ефективність і стійкість у кіберпросторі. Зазначимо, що державна політика США у сфері кібербезпеки є одним із найкращих прикладів комплексного підходу до захисту національної безпеки у цифрову епоху. Завдяки поєднанню технічних, організаційних та освітніх заходів, Сполучені Штати вдосконалюють механізми протидії кіберзагрозам та інформаційному тероризму, сприяючи зміцненню як внутрішньої, так і глобальної безпеки.

2.3. Роль недержавних інституцій та організацій у протидії інформаційним атакам

У сучасному світі інформаційний тероризм стає однією з найгостріших загроз національній безпеці держав. США, як один із світових лідерів у галузі цифрових технологій, стикається з цим викликом особливо гостро. Протидія інформаційному тероризму вимагає комплексного підходу, який включає зусилля державних структур, приватного сектору та громадянського суспільства. У цьому контексті особливу роль відіграють недержавні

інституції та організації. Вони стають не лише партнерами уряду в забезпеченні інформаційної безпеки, а й автономними суб'єктами, які самостійно реалізують ініціативи, спрямовані на протидію дезінформації, пропаганді та кіберзагрозам.

Недержавні організації США відіграють ключову роль у створенні технологічних, освітніх та правових інструментів, що допомагають боротися з інформаційним тероризмом. Однією з найвідоміших є *Electronic Frontier Foundation (EFF).* Ця організація займається захистом цифрових прав, включаючи приватність користувачів, свободу слова в Інтернеті та протидію цензурі. У межах боротьби з інформаційним тероризмом EFF розробляє інструменти, які допомагають ідентифікувати фейковий контент, аналізувати походження інформації та захищати конфіденційність користувачів, які стають об'єктами інформаційних атак [75].

Не менш важливу роль відіграє *Center for Strategic and International Studies (CSIS),* який займається аналітикою та дослідженнями у сфері кібербезпеки та інформаційної політики. Центр публікує доповіді про сучасні методи, що використовуються терористами для поширення дезінформації, та розробляє рекомендації для урядових і приватних структур щодо підвищення стійкості до таких загроз. Одним із значущих внесків CSIS є розробка стратегій для мінімізації впливу пропаганди в соціальних мережах, а також пропозиції щодо регуляції онлайн-платформ [69, p. 1417-1435].

Соціальні медіа є однією з головних арен для ведення інформаційного тероризму. У цьому контексті недержавні організації співпрацюють із технологічними компаніями для забезпечення кібербезпеки. Наприклад, *Cyber Threat Alliance (CTA)* об'єднує експертів з кібербезпеки для обміну даними про кіберзагрози, включаючи кампанії дезінформації. Організація активно співпрацює з урядом США та приватними компаніями, допомагаючи створювати стандарти реагування на загрози в інформаційному просторі. Їхня діяльність включає аналіз алгоритмів, які використовують терористичні організації для поширення фейкових новин, та впровадження технологій для

швидкого їх виявлення. Окремо варто згадати *Atlantic Council*, міжнародний аналітичний центр, який у рамках проєкту *Digital Forensic Research Lab (DFRLab)* досліджує методи поширення дезінформації в глобальному масштабі. Їхні спеціалісти проводять розслідування щодо походження та структури дезінформаційних кампаній, які використовуються терористичними організаціями. DFRLab працює у відкритому форматі, надаючи суспільству та медіа доступ до своїх звітів і висновків. Це сприяє прозорості та залученню громадян до боротьби з інформаційним тероризмом [55, p. 89-109].

Іншою важливою організацією є *Freedom House*, яка займається моніторингом рівня свободи в Інтернеті та протидією пропаганді. Freedom House оцінює, як різні країни використовують інформаційний простір для впливу на інші держави або своїх громадян. Їхні звіти допомагають ідентифікувати зони ризику, де терористи можуть використовувати дезінформацію для дестабілізації ситуації. Freedom House також організовує навчальні програми для журналістів і громадських активістів, спрямовані на підвищення обізнаності щодо методів боротьби з дезінформацією. Значущу роль відіграють і університети, які працюють як автономні науково-дослідні центри. Наприклад, *Беркман-Кляйн Центр з питань Інтернету та суспільства* при Гарвардському університеті проводить дослідження про вплив алгоритмів соціальних мереж на поширення пропаганди та екстремістських матеріалів. Їхня робота допомагає розробляти рекомендації для технологічних компаній і державних органів, спрямовані на зменшення впливу терористичних матеріалів [46].

Варто зазначити, що недержавні організації часто виконують роль посередників між урядом, бізнесом і громадянським суспільством. Наприклад, *National Cyber Security Alliance (NCSA)* працює над об’єднанням урядових і приватних ресурсів для підвищення рівня цифрової грамотності громадян. Їхня ініціатива *Stop.Think.Connect.* спрямована на навчання користувачів основам інформаційної безпеки, що включає виявлення фейкових новин та

уникнення шахрайських схем [70, p. 35-48].

Крім того, важливу роль у боротьбі з інформаційним тероризмом відіграють міжнародні ініціативи, у яких беруть участь недержавні інституції США. Наприклад, *Global Internet Forum to Counter Terrorism (GIFCT)* є партнерством між провідними технологічними компаніями та громадськими організаціями. Метою GIFCT є запобігання використанню цифрових платформ терористами, зокрема шляхом видалення екстремістського контенту та блокування облікових записів, які поширюють дезінформацію.

Окремо слід виділити роль громадських ініціатив, таких як *First Draft*, організація, яка спеціалізується на перевірці фактів та навчанні журналістів і громадян боротьбі з фейковими новинами. First Draft працює з різними платформами, зокрема Facebook, Twitter та Google, для створення алгоритмів, які можуть ідентифікувати та позначати недостовірну інформацію.

Недержавні організації також мають значну перевагу у гнучкості та оперативності, що дозволяє їм швидко реагувати на нові форми інформаційного тероризму. Наприклад, коли терористичні угруповання почали активно використовувати криптографію для приховування своїх комунікацій або створення дезінформаційних мереж у даркнеті, такі організації, як *The Tor Project*, почали не лише працювати над удосконаленням своїх технологій, але й співпрацювати з правоохоронними органами для виявлення злочинних активностей у таких середовищах. Хоча Tor відомий як інструмент забезпечення анонімності, його фахівці активно підтримують ініціативи, спрямовані на боротьбу з незаконною діяльністю в даркнеті [67].

Крім технічних аспектів, важливим напрямом діяльності недержавних інституцій є робота з суспільною думкою та медіаграмотністю. Наприклад, організація *Media Literacy Now* проводить активну роботу в галузі освіти, спрямовану на навчання громадян критично сприймати інформацію в медіапросторі. Вона розробляє навчальні матеріали для шкіл та університетів, які допомагають молоді аналізувати інформацію, розрізняти фейкові новини та уникати маніпулятивного контенту.

Ще одним прикладом успішної діяльності у сфері протидії інформаційному тероризму є діяльність організації *Access Now*, яка захищає цифрові права користувачів у всьому світі. Вона надає юридичну підтримку жертвам інформаційних атак, консультує компанії та уряди щодо впровадження політик, які запобігають використанню технологій для пропаганди чи терористичних дій. Крім того, Access Now проводить кампанії з просвіти громадян щодо їхніх цифрових прав і способів захисту від кіберзагроз. Особливу увагу варто приділити також громадським рухам, які займаються боротьбою з мовою ворожнечі, що часто стає інструментом інформаційного тероризму. Наприклад, організація *Anti-Defamation League (ADL)* активно працює над моніторингом та викриттям екстремістського контенту в Інтернеті. Вона співпрацює з технологічними компаніями для ідентифікації мови ворожнечі та видалення її з платформ, а також проводить освітні програми, спрямовані на формування культури взаємоповаги та толерантності в Інтернеті [52, p. 333-355].

Інноваційні технології відіграють вирішальну роль у протидії інформаційному тероризму, і багато недержавних організацій зосереджують свої зусилля саме на розробці та впровадженні таких інструментів. Наприклад, платформа *NewsGuard* створює базу даних новинних сайтів, оцінюючи їхню достовірність за допомогою аналітиків та автоматизованих алгоритмів. Користувачі можуть перевіряти, наскільки надійними є джерела, з яких вони отримують інформацію, що сприяє боротьбі з фейковими новинами [52, p. 333-355].

Важливою є й участь громадянських ініціатив у підтримці журналістів-розслідувачів, які часто стають першою лінією захисту від дезінформації. Такі організації, як *Committee to Protect Journalists (CPJ)*, надають підтримку журналістам, які розслідують випадки поширення пропаганди чи інформаційних атак. Вони пропонують юридичну допомогу, забезпечують безпеку журналістів у конфліктних зонах та організовують навчання щодо безпечного використання цифрових інструментів [52, p. 333-355].

Співпраця між недержавними організаціями та урядом США також є важливим аспектом у протидії інформаційному тероризму. Наприклад, у рамках ініціативи *Tech Against Terrorism*, створеної за підтримки ООН, американські технологічні компанії та громадські організації розробляють спільні стратегії для виявлення та блокування терористичного контенту. Ця ініціатива допомагає малим та середнім платформам посилити свої механізми безпеки, забезпечуючи більшу стійкість до інформаційних атак [57, p. 115-125].

Особливої уваги заслуговує роль волонтерських мереж, які займаються перевіркою фактів та розвінчанням міфів у соціальних мережах. Такі ініціативи, як *FactCheck.org*, зосереджуються на перевірці заяв, що поширюються у медіа, та надають користувачам можливість отримати достовірну інформацію. Їхня діяльність не лише зменшує вплив дезінформації, а й підвищує довіру до інформаційних джерел, що є критично важливим у боротьбі з інформаційним тероризмом. Недержавні організації також активно беруть участь у розробці міжнародних стандартів та етичних норм, які регулюють використання інформаційних технологій. Наприклад, організація *Internet Governance Forum (IGF)* забезпечує платформу для діалогу між урядами, приватним сектором і громадянським суспільством щодо питань безпеки в Інтернеті. Завдяки їхнім зусиллям розробляються рекомендації для країн і компаній, які сприяють зменшенню ризиків використання інформаційного простору для терористичних цілей [29].

Насамкінець слід зазначити, що роль недержавних організацій у протидії інформаційному тероризму продовжує зростати, оскільки загрози у цифровому просторі стають дедалі складнішими. Їхній внесок охоплює широкий спектр діяльності: від створення технологічних рішень до формування культури критичного мислення. Завдяки їхнім зусиллям громадяни, уряди та приватний сектор отримують потужні інструменти для боротьби з цією загрозою, що забезпечує стійкість суспільства перед викликами інформаційного тероризму. Таким чином, роль недержавних інституцій у протидії інформаційному тероризму є багатогранною. Вони

забезпечують технологічну підтримку, проводять дослідження, впроваджують навчальні програми та сприяють співпраці між урядом, приватним сектором і громадянським суспільством. Завдяки таким зусиллям США вдалося створити ефективну мережу для протидії сучасним інформаційним загрозам, де недержавні організації відіграють ключову роль у забезпеченні стабільності та безпеки інформаційного простору.

Висновки до розділу 2

Законодавчі основи протидії інформаційному тероризму у США демонструють системний підхід, спрямований на забезпечення національної безпеки у цифрову епоху. Ключовими актами є Закон про патріотизм США (USA PATRIOT Act), що надає розширені повноваження правоохоронним органам у моніторингу та розслідуванні кіберзагроз, і Закон про кібербезпеку 2015 року, який сприяє обміну інформацією між урядом і приватним сектором. Важливим інструментом є також Національна стратегія з безпеки кіберпростору, яка регламентує міжвідомчу співпрацю та визначає пріоритети у боротьбі з інформаційним тероризмом. Законодавча база США націлена на забезпечення прозорості, захист громадянських прав і впровадження сучасних технологій для попередження кібератак.

Політика США у сфері кібербезпеки базується на інтегрованому підході, де ключову роль відіграють державні інституції. Агентство кібербезпеки та інфраструктурної безпеки (CISA) є центральним органом, який координує національні зусилля з протидії інформаційним загрозам, включаючи кібершпіонаж та дезінформацію. У свою чергу, Національне агентство безпеки (NSA) та Федеральне бюро розслідувань (FBI) відповідають за виявлення та нейтралізацію загроз, що виходять за межі національного рівня. Державні органи США активно співпрацюють на міжнародному рівні, укладаючи угоди з союзниками для обміну розвідувальними даними та спільної протидії кіберзагрозам. Значну увагу приділено превентивним заходам, включаючи

навчання кадрів, впровадження новітніх технологій і розробку аналітичних платформ для моніторингу кіберпростору.

Роль недержавних інституцій у США також є критично важливою для протидії інформаційним атакам. Великі корпорації, зокрема Microsoft, Google і Meta, активно розробляють програмне забезпечення для кіберзахисту, інвестують у дослідження штучного інтелекту та аналіз великих даних. Вони також є партнерами уряду у впровадженні стандартів кібербезпеки та захисту критично важливої інфраструктури. Недержавні організації, такі як Electronic Frontier Foundation (EFF), сприяють підвищенню обізнаності громадян про загрози дезінформації та порушення конфіденційності. Університети та дослідницькі центри, наприклад Центр стратегічних і міжнародних досліджень (CSIS), аналізують тренди в інформаційній війні, пропонуючи інноваційні стратегії для протидії кібертероризму. Крім того, громадянське суспільство бере участь у моніторингу інформаційних атак, що дозволяє швидко виявляти та блокувати ворожі кампанії.

У підсумку, протидія інформаційному тероризму у США є багатовимірною стратегією, що включає законодавчі ініціативи, активну роль державних інституцій та взаємодію з недержавними організаціями. Ця комплексна модель дозволяє ефективно адаптуватися до динамічних змін у цифровому середовищі, мінімізуючи загрози національній безпеці та забезпечуючи захист демократичних цінностей. У той же час, головними викликами залишаються баланс між безпекою та приватністю, координація зусиль між різними секторами та вдосконалення технологій для оперативної протидії новим типам кіберзагроз.

РОЗДІЛ 3. МІЖНАРОДНА СПІВПРАЦЯ США У СФЕРІ ПРОТИДІЇ ІНФОРМАЦІЙНОМУ ТЕРОРИЗМУ

3.1. Інституційні рамки міжнародної співпраці США в боротьбі з інформаційним тероризмом

У сучасному світі інформаційний тероризм стає все більш значущою загрозою для національної безпеки держав і міжнародної стабільності. США, як провідна держава у сфері інформаційних технологій та глобальної політики, відіграють ключову роль у формуванні міжнародної співпраці у боротьбі з цим явищем. Зазначимо, що інституційні рамки міжнародної співпраці – це сукупність правил, норм, процедур, а також організаційних структур, які забезпечують узгоджене функціонування міжнародних акторів у спільній діяльності. Вони створюють основу для ефективної взаємодії між державами, міжнародними організаціями, неурядовими структурами та іншими учасниками міжнародних відносин. Ці рамки визначають правила поведінки сторін, механізми прийняття рішень, шляхи вирішення конфліктів, а також формують загальні принципи, на яких будується співпраця. Інституційні рамки можуть бути формальними, коли їх встановлюють через підписання міжнародних договорів чи створення міжнародних організацій, або неформальними, коли вони базуються на традиціях, звичаях чи неписаних угодах. Вони забезпечують стабільність, передбачуваність та ефективність у міжнародній взаємодії, сприяючи вирішенню глобальних проблем, таких як зміна клімату, забезпечення миру, боротьба з бідністю чи пандеміями. Інституційні рамки, в межах яких відбувається така співпраця, охоплюють як багатосторонні, так і двосторонні механізми, що базуються на принципах міжнародного права, колективної безпеки та спільної відповідальності. Аналіз цих інституційних механізмів дозволяє зрозуміти, яким чином США реалізують свої стратегічні інтереси, одночасно сприяючи глобальній безпеці.

Інституційні рамки боротьби США з інформаційним тероризмом можна розділити на кілька основних рівнів: національний, двосторонній,

багатосторонній і глобальний.

На національному рівні США створили потужну правову та організаційну базу для протидії кіберзагрозам, що є основою їхньої міжнародної стратегії. Законодавчі ініціативи, такі як «Закон про кібербезпеку» (Cybersecurity Act), та створення ключових структур, як-от Агентство кібербезпеки та безпеки інфраструктури (CISA), дозволяють США ефективно реагувати на загрози в цифровому просторі. Однак боротьба з інформаційним тероризмом вимагає ширшого підходу, оскільки такі загрози є транскордонними за своєю природою [35].

На міжнародному рівні США беруть активну участь у роботі ключових організацій, таких як Організація Об'єднаних Націй (ООН), НАТО та Група семи (G7). У межах ООН Сполучені Штати підтримують діяльність Контртерористичного управління, яке займається моніторингом кібертероризму та розробкою рекомендацій для держав-членів. Крім того, США активно працюють у рамках Резолюції Ради Безпеки ООН 2341, яка спрямована на захист критичної інфраструктури від терористичних атак, зокрема кібернетичних. У рамках НАТО США просувають ідею кібербезпеки як колективної відповідальності. Ключовим інструментом у цьому є Центр передового досвіду з кібербезпеки в Таллінні (CCDCOE), який займається аналізом кіберзагроз, розробкою спільних стратегій та проведенням тренувань для країн-членів Альянсу. Співпраця в рамках НАТО дозволяє США забезпечити координацію дій із союзниками, посилюючи їхню спроможність протистояти інформаційному тероризму. США також активно співпрацюють із партнерами в рамках G7, зокрема у створенні механізмів протидії дезінформації. З 2018 року в межах G7 функціонує Ініціатива з кібербезпеки, яка спрямована на обмін інформацією між країнами-членами щодо кіберзагроз, у тому числі тих, що пов'язані з тероризмом. Окремо варто зазначити роль Сполучених Штатів у створенні Глобального форуму для боротьби з тероризмом (GCTF), який розробляє практичні рекомендації для держав щодо запобігання та протидії тероризму, зокрема інформаційному [34].

Двосторонні угоди є ще одним важливим елементом інституційних рамок співпраці США. Яскравим прикладом є їхнє партнерство з Європейським Союзом у рамках Програми з питань кібербезпеки та боротьби з тероризмом. У межах цього партнерства здійснюється обмін інформацією про загрози, спільна розробка технологій для виявлення дезінформації, а також проведення спільних навчань. Аналогічно, Сполучені Штати мають угоди з окремими країнами, такими як Велика Британія, Японія та Австралія, які передбачають координацію дій у боротьбі з кіберзагрозами [57, p. 115-125].

Особливе місце займає співпраця США з приватним сектором і громадянським суспільством. Визнання ролі технологічних компаній у формуванні інформаційного простору привело до активного залучення таких корпорацій, як Google, Meta (Facebook), Microsoft і Twitter, до боротьби з інформаційним тероризмом. У рамках ініціативи Tech Against Terrorism, яка підтримується ООН і США, технологічні компанії отримують рекомендації щодо виявлення та видалення терористичного контенту. Крім того, США ініціювали створення Глобального альянсу з протидії дезінформації, що об’єднує держави, міжнародні організації та приватний сектор для боротьби з поширенням фейкової інформації, яка може бути інструментом терористів [74].

Інституційні рамки міжнародної співпраці США також включають активну участь у багатосторонніх угодах, таких як Будапештська конвенція про кіберзлочинність. Цей документ є першим міжнародним договором, що визначає юридичну базу для боротьби з кіберзлочинами, зокрема тероризмом, та передбачає механізми екстрадиції та обміну інформацією між країнами. США активно просувають ідею універсалізації цієї конвенції, залучаючи нових учасників до її підписання. Успішна співпраця США з іншими країнами у боротьбі з інформаційним тероризмом також демонструється на прикладі окремих кейсів. Наприклад, у 2020 році була проведена спільна операція США, Європолу та кількох країн ЄС проти терористичної мережі «Аль-Каїда», яка використовувала соціальні мережі для вербування прихильників і поширення

ідеології. У результаті цієї операції вдалося ліквідувати понад 26 тисяч облікових записів, які належали терористам, та запобігти масштабним атакам.

Інший важливий приклад – співпраця США з Австралією та Новою Зеландією у форматі Альянсу п’яти очей (Five Eyes). У межах цього партнерства країни обмінюються розвідувальною інформацією, що дозволяє оперативно виявляти кіберзагрози та координувати дії у відповідь. Зокрема, у 2021 році Альянс успішно зупинив масштабну атаку на критичну інфраструктуру в регіоні Азії та Тихого океану, що була організована терористичними групами [22, с. 139-144].

У глобальному контексті США ініціюють створення нових інституційних механізмів для протидії інформаційному тероризму. Однією з таких ініціатив є Паризький заклик до довіри та безпеки в кіберпросторі, до якого приєдналися десятки країн. США активно підтримують цю ініціативу, яка спрямована на формування етичних норм поведінки в кіберпросторі та протидію використанню технологій для терористичних цілей. Водночас боротьба з інформаційним тероризмом стикається з низкою викликів. По-перше, різні країни мають різні правові та культурні підходи до регулювання інформаційного простору, що ускладнює досягнення консенсусу на міжнародному рівні. По-друге, швидка еволюція технологій і методів кібертероризму вимагає постійного вдосконалення механізмів співпраці. І, нарешті, проблема захисту персональних даних і свободи слова в контексті боротьби з тероризмом залишається відкритою і викликає дебати серед експертів. Попри ці виклики, США продовжують відігравати провідну роль у створенні інституційних рамок для міжнародної співпраці в боротьбі з інформаційним тероризмом. Їхній підхід, що поєднує дипломатичні зусилля, правове регулювання, військову координацію та участь приватного сектора, є прикладом комплексного підходу до вирішення глобальних загроз. В умовах зростаючого значення кіберпростору для національної та міжнародної безпеки важливість таких рамок лише зростатиме, забезпечуючи ефективну протидію інформаційному тероризму у майбутньому [19, p. 219-229].

Значну увагу США приділяють і науково-дослідним проектам у сфері кібербезпеки. Університети, дослідницькі інститути та технологічні центри отримують фінансування для розробки нових методів виявлення та запобігання інформаційному тероризму. Співпраця з міжнародними партнерами у сфері науки й технологій дозволяє США інтегрувати інноваційні підходи у свої стратегії боротьби. У контексті геополітичної конкуренції особливу увагу привертає роль Китаю та РФ, які пропонують альтернативні підходи до регулювання кіберпростору, базуючись на принципах суверенітету в цифровій сфері. Це створює додаткові труднощі для США у формуванні глобальної коаліції проти інформаційного тероризму, адже країни з авторитарними режимами можуть використовувати концепцію інформаційної безпеки як інструмент для посилення контролю над власним населенням [61].

Попри ці виклики, США продовжують удосконалювати інституційні механізми боротьби з інформаційним тероризмом. Створення нових платформ для співпраці, розвиток технологій штучного інтелекту для моніторингу загроз і просування ідей міжнародної солідарності залишаються основними пріоритетами. Сполучені Штати усвідомлюють, що ефективна протидія інформаційному тероризму можлива лише через широке міжнародне співробітництво, побудоване на довірі, взаєморозумінні та спільних інтересах.

Продовжуючи розгляд інституційних рамок міжнародної співпраці США в боротьбі з інформаційним тероризмом, важливо звернути увагу на їхню роль у регулюванні глобальної інформаційної архітектури. Основним принципом, який США відстоюють на міжнародній арені, є забезпечення відкритості, доступності та безпеки Інтернету. Цей підхід відображений у численних ініціативах, таких як «Цифровий порядок денний» (Digital Agenda) і «Стратегія міжнародної кіберполітики» (International Cyber Strategy). Сполучені Штати активно залучають міжнародних партнерів до обговорення способів протидії інформаційному тероризму, включаючи використання штучного інтелекту, машинного навчання та блокчейн-технологій для забезпечення кібербезпеки [47].

Одним із важливих інструментів співпраці США є участь у спеціалізованих агенціях і організаціях, таких як Міжнародний союз електрозв'язку (ITU) та Інтернет-корпорація з присвоєння імен і номерів (ICANN). Через ці інституції США впливають на розробку міжнародних стандартів, що регулюють функціонування Інтернету та телекомунікаційних мереж. Особливу увагу приділяють питанням забезпечення безпеки критичних інфраструктур і створення систем раннього виявлення кібератак, спрямованих на підрив суспільної стабільності [44].

Важливо відзначити і роль міжнародних економічних організацій у протидії фінансовим аспектам інформаційного тероризму. У рамках Міжнародного валютного фонду (МВФ) і Світового банку США просувають ініціативи, спрямовані на захист фінансових систем від кібератак, які можуть паралізувати національні економіки або сприяти фінансуванню терористичних угруповань. Окрему роль відіграє Група розробки фінансових заходів боротьби з відмиванням грошей (FATF), у якій США ініціюють посилення моніторингу транзакцій, що проходять через криптовалютні платформи, які нерідко використовуються терористами [44].

Крім багатосторонніх механізмів, США велику увагу приділяють побудові регіональних партнерств у сфері боротьби з інформаційним тероризмом. У Південно-Східній Азії, де кіберзлочинність набуває особливої актуальності, Сполучені Штати співпрацюють з країнами АСЕАН у межах Ініціативи з кібербезпеки (ASEAN Cybersecurity Initiative). Спільні програми спрямовані на підвищення спроможностей регіональних держав до протидії кіберзагрозам, включаючи проведення навчань, розробку законодавчих баз і посилення технічної інфраструктури. Особливого значення в рамках міжнародної співпраці набуває використання публічно-приватного партнерства. США розуміють, що боротьба з інформаційним тероризмом вимагає залучення ресурсів і експертизи технологічних компаній, які мають ключові позиції на світовому ринку. Однією з таких ініціатив є програмне забезпечення для виявлення шкідливого контенту та протидії пропаганді,

розроблене у співпраці з технологічними корпораціями.

США також приділяють значну увагу освіті та підготовці кадрів у сфері кібербезпеки. Програми, такі як CyberCorps, спрямовані на підготовку фахівців, які володіють найсучаснішими знаннями у сфері протидії інформаційному тероризму. Інститути, такі як Національний інститут стандартів і технологій (NIST), співпрацюють із міжнародними партнерами для обміну найкращими практиками та розробки нових підходів до забезпечення безпеки інформаційного простору [51].

Окремим напрямком є використання міжнародних санкцій для стримування держав і недержавних акторів, які сприяють поширенню інформаційного тероризму. США активно застосовують санкційні механізми для обмеження доступу до фінансових ресурсів і технологій суб'єктів, які підозрюються у сприянні терористичним групам. Ці заходи, як правило, ухвалюються в координації з союзниками, що дозволяє досягти більшого ефекту у глобальному масштабі. Проте ефективність цих інституційних рамок залежить від здатності США адаптуватися до нових викликів. Швидкий розвиток технологій, зокрема квантових обчислень і розширеного штучного інтелекту, створює нові загрози, які вимагають адекватної реакції. Крім того, зростання популярності децентралізованих платформ і технологій, таких як блокчейн, ставить нові питання щодо регулювання їхнього використання в контексті кіберзлочинності. На тлі цих викликів США активно працюють над створенням нових глобальних коаліцій, які об'єднують держави, технологічні компанії, наукові інституції та громадянське суспільство. Ініціативи, такі як «Партнерство заради кіберзахисту» (Partnership for Cybersecurity Resilience), демонструють прагнення США формувати інклюзивні механізми міжнародної співпраці. Одним із перспективних напрямків є також інтеграція штучного інтелекту для аналізу даних, прогнозування потенційних загроз і автоматизації реагування на інформаційні атаки [38].

Водночас довгострокова успішність інституційних рамок міжнародної співпраці залежить від здатності США формувати довіру серед міжнародних

партнерів, розвивати діалог і уникати односторонніх рішень, які можуть викликати опір. Складність сучасного кіберсередовища вимагає тісної координації між усіма учасниками, а також пошуку компромісів у сферах, де інтереси різних держав і організацій не збігаються. Таким чином, інституційні рамки міжнародної співпраці США в боротьбі з інформаційним тероризмом є складною і багатогранною системою, що охоплює різні рівні взаємодії – від глобальних до локальних ініціатив. Незважаючи на виклики, пов'язані з геополітичними протиріччями та технологічними змінами, Сполучені Штати продовжують відігравати провідну роль у формуванні міжнародного порядку денного в цій сфері. Ефективність цих рамок залежить від здатності США сприяти інтеграції інновацій, посилювати міжнародну координацію та забезпечувати баланс між безпекою та свободою в інформаційному просторі.

3.2. Співпраця США з міжнародними організаціями та іншими державами у протидії інформаційним загрозам

У сучасному світі інформаційні загрози стали однією з найбільш актуальних проблем у сфері міжнародної безпеки. Розвиток цифрових технологій і глобальна мережевізація створили умови для маніпулювання інформацією на міжнародному рівні, що впливає на громадську думку, політичні процеси та міждержавні відносини. У відповідь на ці виклики США значно активізували свою діяльність у сфері протидії дезінформації та інших інформаційних загроз, співпрацюючи з міжнародними організаціями, союзниками та партнерами. У даному тексті розглянемо ключові аспекти такої співпраці, стратегічні підходи США та конкретні приклади, які ілюструють успішність міжнародних зусиль у боротьбі з інформаційними загрозами [31].

Інформаційні загрози, такі як дезінформація, пропаганда, кібератаки та інформаційні маніпуляції, часто мають транснаціональний характер. Вони виходять за межі національних кордонів, ускладнюючи їхнє попередження та протидію. США визнають, що ефективна боротьба з цими загрозами можлива

лише через тісну співпрацю з міжнародними організаціями, такими як Організація Об'єднаних Націй (ООН), НАТО, Європейський Союз (ЄС), а також з іншими державами, які мають спільні інтереси у захисті демократії та міжнародного порядку. Співпраця США з НАТО у протидії інформаційному тероризму є одним із ключових аспектів сучасної системи міжнародної безпеки. Інформаційний тероризм, як частина гібридної війни, виявляється через поширення дезінформації, фейкових новин, маніпуляцій із суспільною свідомістю, кібератак на державні та приватні інформаційні ресурси. Ці дії спрямовані на підрив довіри до демократичних інститутів, розпалювання соціальних конфліктів і дестабілізацію політичних систем. У цьому контексті співпраця між США та НАТО виявляється критично важливою для забезпечення стійкості демократичних країн до загроз, пов'язаних з інформаційним тероризмом [37].

Інформаційний тероризм, як явище, набув широкого поширення у XXI столітті, зокрема завдяки технологічному прогресу, який забезпечив зростання впливу соціальних мереж, цифрових медіа і засобів масової інформації. Уразливість інформаційного простору демократичних країн полягає в його відкритості та залежності від свободи слова. У цих умовах США та НАТО стали ключовими акторами у створенні стратегій, спрямованих на протидію інформаційним загрозам, зокрема через колективні зусилля, засновані на міжнародному співробітництві, технологічному прогресі й обміні розвідувальними даними [40].

Першим кроком у боротьбі з інформаційним тероризмом стало усвідомлення загрози. Кібернапади, кампанії дезінформації і цілеспрямовані інформаційні операції з боку недемократичних режимів, таких як РФ та Китай, створили прецеденти, що вплинули на політику безпеки НАТО. Наприклад, кібератака на Естонію у 2007 році, яку приписують російським хакерам, стала першим серйозним сигналом для Альянсу щодо вразливості кіберпростору. Цей інцидент підштовхнув НАТО до створення Центру передового досвіду з кібероборони (CCDCOE) у Таллінні, де США стали одним із ключових

партнерів. Завдяки цьому центру проводяться навчання, тренінги і симуляції, спрямовані на підвищення спроможності членів Альянсу протидіяти кібератакам [47].

США активно використовують свої технічні можливості та експертизу для підтримки НАТО. Американські кіберкомандування (USCYBERCOM) і Агентство національної безпеки (NSA) відіграють провідну роль у виявленні та нейтралізації загроз, що виникають у кіберпросторі. Наприклад, під час президентських виборів у США у 2016 році було зафіксовано масовані кампанії дезінформації та кібератак, які, за висновками американської розвідки, мали російське походження. Ці події стали поштовхом до подальшої співпраці між США і НАТО у сфері кібербезпеки. Зокрема, була розроблена концепція «п’ятої статті» Північноатлантичного договору, згідно з якою кібернапади на членів Альянсу можуть розглядатися як акт агресії, що вимагає колективної відповіді [64, p. 169-172].

Ще одним важливим напрямом співпраці є протидія дезінформації. Сполучені Штати та НАТО спільно працюють над розробкою стратегій інформаційної стійкості, включаючи освітні програми для громадськості, розробку інструментів для перевірки фактів і активну роботу з технологічними компаніями. Наприклад, Центр стратегічних комунікацій НАТО (NATO StratCom COE), який знаходиться у Ризі, Латвія, займається вивченням методів протидії пропаганді та фейковим новинам. США, як провідний партнер, підтримують фінансування і надають експертів для цього центру, розширюючи його можливості в аналізі інформаційних потоків та розробці відповідних заходів. США також активно сприяють створенню нових технологічних рішень для виявлення й нейтралізації інформаційних загроз. Зокрема, американські корпорації, такі як Microsoft, Google і Meta, співпрацюють із урядовими структурами і НАТО, розробляючи алгоритми штучного інтелекту для виявлення ботів, фейкових акаунтів та кампаній дезінформації. Наприклад, Facebook (нині Meta) працює над покращенням системи модерації контенту, яка дозволяє ідентифікувати скоординовану

поведінку з боку зловмисників. НАТО активно інтегрує ці технології у свої стратегії, роблячи їх доступними для всіх членів Альянсу.

Важливим аспектом є також спільні навчання та симуляції, які дозволяють удосконалювати навички реагування на інформаційні загрози. Наприклад, щорічні навчання NATO Cyber Coalition, що проводяться за участі США, об'єднують експертів із різних країн для тестування протоколів кіберзахисту та реагування на інформаційні атаки. Ці заходи допомагають виявляти слабкі місця в системах безпеки країн-членів і вдосконалювати механізми захисту. Не менш важливим є аспект правового регулювання. США та НАТО активно співпрацюють у напрямі створення міжнародних норм і стандартів поведінки в кіберпросторі. Одним із таких прикладів є Талліннський маніфест з кіберправа, який став основою для розробки принципів міжнародного права у сфері кібербезпеки. США надають експертну підтримку у формуванні цих документів, що дозволяє інтегрувати їх у національні законодавства країн-членів НАТО. Окрему увагу заслуговує участь США у програмі НАТО з розширення партнерства за межами Альянсу. У рамках цієї програми США надають підтримку країнам-партнерам, зокрема Україні, Грузії та Молдові, які також стикаються з інформаційними загрозами. Наприклад, у контексті російської агресії проти України США допомагають у створенні центрів інформаційної безпеки та кіберзахисту, а також забезпечують технологічну підтримку для моніторингу інформаційного простору [32].

Слід також зазначити, що співпраця США з НАТО у протидії інформаційному тероризму має виклики. По-перше, це координація дій між країнами з різним рівнем технологічного розвитку і національними підходами до регулювання кіберпростору. По-друге, існує проблема балансу між забезпеченням інформаційної безпеки та збереженням демократичних свобод, зокрема свободи слова. По-третє, зловмисники постійно удосконалюють свої методи, що вимагає від США та НАТО постійного оновлення стратегій і технологій. Отже, співпраця США та НАТО у протидії інформаційному

тероризму є важливим елементом міжнародної безпеки, що базується на спільних зусиллях, технологічному прогресі та міжнародному праві. Хоча перед Альянсом стоять значні виклики, колективна відповідь на інформаційні загрози дозволяє зміцнювати стійкість демократичних суспільств і забезпечувати мир та стабільність у світі [33].

Співпраця США з ЄС у цій сфері також заслуговує на увагу. Наприклад, у рамках Європейської служби зовнішніх дій функціонує група East StratCom, яка займається моніторингом та аналізом дезінформації, що надходить із третіх країн, зокрема з РФ. США не лише фінансово підтримують цю ініціативу, а й активно співпрацюють із ЄС у питаннях розробки стандартів протидії інформаційним атакам. Спільні тренінги, семінари та обмін даними між американськими та європейськими експертами підвищують ефективність боротьби з маніпуляціями у цифровому просторі. Ще одним важливим напрямком співпраці є кібербезпека. США визнали кібератаки одним із головних викликів національній безпеці, що потребує міжнародного реагування. У 2021 році адміністрація Дж. Байдена ініціювала проведення саміту «Ренесанс кібербезпеки» з метою об’єднання зусиль провідних держав у боротьбі з кібератаками. Одним із результатів цього саміту стало укладення угод із ЄС про спільну протидію хакерським групам, які працюють з територій країн, що не дотримуються міжнародних стандартів. Наприклад, США та Великобританія у 2022 році організували спільну операцію з викриття російської хакерської групи «Evil Corp», яка спеціалізувалася на фінансових кіберзлочинах. Ця операція демонструє здатність США працювати з союзниками в рамках складних транснаціональних розслідувань [62].

Співпраця між США та ЄС у протидії інформаційному тероризму є одним із ключових аспектів їхньої стратегічної взаємодії у сфері безпеки. Інформаційний тероризм, що включає використання інформаційних технологій для поширення пропаганди, дезінформації, кібератак та маніпуляцій громадською думкою, став викликом глобального масштабу. Це явище впливає на політичну стабільність, соціальну згуртованість та

економічну безпеку країн по обидва боки Атлантики. Враховуючи це, США та ЄС об'єднали свої зусилля для розробки комплексних стратегій та інструментів боротьби з цим видом тероризму.

Інформаційний тероризм є багатогранним явищем, яке включає як використання кіберзброї, так і організацію інформаційних кампаній для дестабілізації ситуації в інших країнах. Одним із головних викликів стала діяльність недержавних акторів та держав, які прагнуть використати інформаційні технології для підриву демократичних процесів, таких як вибори, або для послаблення довіри до урядів. РФ, Китай та інші геополітичні конкуренти Заходу активно використовують інформаційний простір як частину своїх гібридних стратегій. Для США та ЄС це стало сигналом до необхідності створення системи колективної безпеки в інформаційному середовищі. Співпраця між США та ЄС у цій сфері почала активно розвиватися після подій 2016 року, коли російські інформаційні кампанії вплинули на результати президентських виборів у США, а також на політичну динаміку в Європі, зокрема в контексті референдуму щодо Brexit. Європейські країни також зіткнулися з викликами у вигляді поширення фейкових новин, що спрямовані на посилення радикалізації та соціального розколу. Як відповідь, у 2018 році ЄС запустив План дій проти дезінформації, який став однією з основ для трансатлантичної співпраці у цій сфері. Ключовими напрямами співпраці стали обмін інформацією, координація політик та впровадження технологічних інновацій для протидії загрозам в інформаційному просторі. Одним із найбільш показових прикладів такої співпраці є створення Трансатлантичної робочої групи з дезінформації, яка об'єднує експертів, представників урядів та приватного сектору з обох боків Атлантики. Ця група спрямована на вивчення тактик і методів, що використовуються дезінформаторами, розробку інструментів для їх нейтралізації, а також надання рекомендацій урядам США та країн ЄС [62].

Іншим важливим елементом трансатлантичної співпраці є спільні навчання та тренінги, спрямовані на зміцнення кіберзахисту та підготовку до

реагування на кризові ситуації в інформаційному середовищі. Наприклад, навчання Cyber Europe та Locked Shields, які проводяться у співпраці з НАТО, залучають представників США та ЄС до моделювання ситуацій, пов'язаних із кібератаками та інформаційними загрозами. Це дозволяє покращити взаємодію між партнерами, перевірити ефективність існуючих протоколів і виявити прогалини в захисті. Приватний сектор відіграє важливу роль у боротьбі з інформаційним тероризмом, і співпраця з технологічними компаніями є ще одним важливим напрямом взаємодії між США та ЄС. Провідні американські технологічні гіганти, такі як Google, Facebook і Twitter, працюють у тісній співпраці з Європейською комісією та іншими організаціями для впровадження механізмів моніторингу та видалення шкідливого контенту. У 2018 році ЄС підписав Кодекс поведінки щодо дезінформації, до якого приєдналися провідні компанії з США. Цей документ передбачає обов'язковість прозорої звітності, зменшення видимості дезінформації та інвестування в інструменти перевірки фактів. Спільні зусилля також охоплюють законодавчу співпрацю. У США була прийнята низка законів, спрямованих на боротьбу з дезінформацією, зокрема закон про прозорість політичної реклами. Аналогічно, у ЄС введено загальний регламент із захисту даних (GDPR), який обмежує можливості маніпуляції персональною інформацією громадян. Координація цих зусиль дозволяє уникнути суперечностей у регулюванні і створює єдиний фронт протидії загрозам [63, p. 45-55].

Однак співпраця між США та ЄС у цій сфері стикається з викликами. Серед них – розбіжності у підходах до регулювання технологічного сектору, різні правові системи та інтереси національної безпеки. Наприклад, американські компанії часто висловлюють занепокоєння через жорсткі європейські регуляції, які можуть впливати на їхню комерційну діяльність. Водночас, європейські країни вимагають більшого контролю над діяльністю технологічних платформ, що може створювати напруженість у відносинах. Іншою проблемою є питання конфіденційності та захисту даних. США та ЄС

мають різні підходи до цієї теми, що ускладнює обмін інформацією між правоохоронними органами. Рішенням стало створення механізмів, таких як Угода про захист даних між ЄС і США, яка забезпечує прозорість і безпеку обміну інформацією. Проте впровадження цих угод вимагає часу та узгодження багатьох аспектів. На завершення, співпраця між США та ЄС у протидії інформаційному тероризму є важливим інструментом у забезпеченні глобальної безпеки. Незважаючи на виклики, їхні спільні зусилля сприяють підвищенню стійкості демократичних суспільств до дезінформації та кіберзагроз. За рахунок обміну знаннями, технологіями та ресурсами партнери можуть ефективніше протидіяти сучасним викликам. Подальше розширення співпраці у цій сфері є критично важливим для зміцнення трансатлантичного альянсу і забезпечення стабільності в умовах глобальної цифровізації [66].

У цьому контексті міжнародна співпраця стає вкрай важливою, а центральне місце займає співпраця США та ООН. США як одна з провідних держав у сфері інформаційних технологій та безпеки відіграє значну роль у формуванні та реалізації глобальних стратегій боротьби з інформаційним тероризмом. Приклади успішної співпраці США та ООН у протидії інформаційному тероризму демонструють досягнення у сфері кібербезпеки та боротьби з дезінформацією. Наприклад, операція «Глобальний щит», організована за підтримки ООН та США, допомогла виявити й знешкодити міжнародну мережу, що поширювала пропаганду терористичних організацій через соціальні медіа. Також США активно співпрацювали з ООН під час реалізації ініціативи «Цифровий світ без тероризму», яка спрямована на обмін найкращими практиками серед держав у боротьбі з інформаційними загрозами.

ООН є головною платформою для координації міжнародних зусиль у протидії тероризму, зокрема його інформаційним аспектам. Проблематика інформаційного тероризму була вперше офіційно визнана на міжнародному рівні наприкінці 1990-х років, коли розпочалися дискусії про небезпеки, які створюють нові технології для глобальної безпеки. Після терористичних атак 11 вересня 2001 року в США питання інформаційної безпеки стало ще

актуальнішим, і саме Сполучені Штати виступили ініціаторами багатьох резолюцій у рамках ООН, спрямованих на посилення міжнародної співпраці у цій сфері. Одним із найважливіших елементів співпраці США з ООН у протидії інформаційному тероризму є робота в рамках Контртерористичного комітету Ради Безпеки ООН (КТК РБ ООН). Цей комітет, створений у 2001 році на основі резолюції 1373, займається координацією глобальних зусиль у боротьбі з тероризмом, зокрема й інформаційним. США активно підтримують діяльність цього комітету, надаючи експертні оцінки, фінансову допомогу та технологічні ресурси. Зокрема, Сполучені Штати сприяли розробці КТК рекомендацій щодо боротьби з використанням інтернету для терористичних цілей, таких як пропаганда, рекрутування та фінансування [57, p. 115-125].

Іншим важливим механізмом є Управління ООН з боротьби з тероризмом (УБТ ООН), яке було створене у 2017 році. США беруть активну участь у фінансуванні та програмній діяльності цього органу, зокрема через ініціативи щодо підвищення кібербезпеки в країнах, що розвиваються, та створення механізмів моніторингу інформаційного простору. Наприклад, у 2019 році було запущено спільний проєкт між УБТ ООН та американськими партнерами для розробки систем раннього виявлення терористичного контенту в соціальних мережах. США разом із союзниками виступають активними учасниками процесу формування міжнародних стандартів у сфері інформаційної безпеки. В рамках ООН Сполучені Штати ініціювали кілька резолюцій, що закликають до посилення боротьби з інформаційним тероризмом. Наприклад, у 2016 році Рада Безпеки ухвалила резолюцію 2341, яка спрямована на захист критичної інфраструктури від кібератак, включаючи ті, що мають терористичну природу. Ця резолюція була ініційована США та підтримана більшістю країн-членів ООН [43, p. 106-119].

Важливою складовою є також співпраця в рамках Глобальної контртерористичної стратегії ООН, ухваленої у 2006 році. США активно сприяли включенню до цієї стратегії пунктів, пов’язаних із боротьбою з терористичною пропагандою та використанням інтернету для радикалізації. У

2020 році США запропонували оновлення цієї стратегії, акцентуючи увагу на нових загрозах, пов’язаних із розвитком штучного інтелекту та алгоритмів, які використовуються для автоматизованого поширення дезінформації. Одним із найпомітніших прикладів співпраці США з ООН у боротьбі з інформаційним тероризмом є програма Tech Against Terrorism, запущена в 2017 році під егідою ООН за підтримки американських технологічних гігантів, таких як Google, Microsoft і Facebook. Ця ініціатива спрямована на створення спільних платформ для обміну інформацією між державами, приватними компаніями та громадськими організаціями з метою ідентифікації та блокування терористичного контенту в інтернеті. У рамках програми були розроблені інструменти для автоматизованого виявлення пропагандистських матеріалів, які використовуються терористичними групами [45].

Ще одним важливим напрямом є програма Global Internet Forum to Counter Terrorism (GIFCT), яка була ініційована американськими корпораціями за підтримки уряду США та міжнародних організацій, включаючи ООН. Основною метою цієї програми є створення бази даних для ідентифікації та видалення терористичного контенту, а також розробка стандартів для реагування на загрози в інформаційному просторі. Окремо слід відзначити ініціативу щодо протидії радикалізації в мережі, запущену США спільно з УБТ ООН у 2018 році. У рамках цього проєкту проводяться тренінги для державних службовців та представників громадянського суспільства у країнах, які найбільше постраждали від тероризму, щодо виявлення та протидії терористичній пропаганді. Наприклад, в Іраку та Сирії програма спрямована на створення локальних інформаційних кампаній, які спростовують наративи, що використовуються терористичними угрупованнями для вербування молоді [76].

Попри значні успіхи, співпраця США та ООН у протидії інформаційному тероризму стикається з низкою викликів. Одним із них є розбіжності у підходах до регулювання інформаційного простору. Наприклад, деякі країни, зокрема Китай і РФ, наполягають на більш жорсткому контролі

над інтернетом на національному рівні, тоді як США та їхні союзники відстоюють принципи свободи слова та саморегуляції. Ці розбіжності ускладнюють досягнення консенсусу щодо розробки універсальних стандартів у сфері кібербезпеки. Ще однією проблемою є недостатня залученість деяких країн до міжнародних ініціатив. Наприклад, багато держав Африки та Близького Сходу через обмежені ресурси не можуть ефективно впроваджувати рекомендації ООН. У відповідь на це США ініціювали програми технічної допомоги, однак їхня реалізація вимагає тривалого часу та значних інвестицій [64, p. 169-185].

У майбутньому співпраця США з ООН у протидії інформаційному тероризму матиме вирішальне значення для глобальної безпеки. Розвиток технологій, таких як штучний інтелект, блокчейн та квантові обчислення, створює як нові можливості, так і нові загрози. У цьому контексті важливо забезпечити ефективну координацію між країнами, міжнародними організаціями та приватним сектором. США, як одна з провідних держав у сфері технологій, мають унікальні можливості для формування глобальної політики у цій сфері. Співпраця з ООН дозволяє об’єднати зусилля різних країн і забезпечити інтегрований підхід до вирішення проблеми інформаційного тероризму. З огляду на це, подальша інтеграція США та ООН у боротьбі з цією загрозою є не лише бажаною, але й необхідною умовою для досягнення стабільності та безпеки у сучасному світі [67, p. 212-232].

Отже, співпраця США з ООН у протидії інформаційному тероризму є комплексним і багатогранним процесом, який включає створення міжнародних норм, розвиток технологій, підтримку освітніх програм і партнерство з приватним сектором. Незважаючи на наявні виклики, ця співпраця демонструє значний потенціал для зміцнення глобальної безпеки у цифрову епоху. Завдяки поєднанню зусиль держав, міжнародних організацій та приватного сектору, можна досягти більш ефективного захисту суспільств від загроз, пов’язаних з інформаційним тероризмом, і сприяти сталому розвитку міжнародної системи безпеки.

Окрім міжнародних організацій, США розвивають двосторонні партнерства з багатьма державами для спільного протистояння інформаційним загрозам. Одним із найбільш успішних прикладів є співпраця з Великою Британією, яка має великий досвід у сфері кібербезпеки та боротьби з дезінформацією. Партнерство між Національним агентством з кібербезпеки США (CISA) та його британським аналогом сприяло обміну інформацією про кіберзагрози та координованій відповіді на атаки. Іншим прикладом є співпраця США з країнами Балтії, які через свою історію мають високий рівень обізнаності про загрози, пов’язані з пропагандою та інформаційними атаками. Спільні навчання та проєкти, спрямовані на зміцнення медіаграмотності серед населення, є ключовими напрямками цієї співпраці.

Особливе значення США надають залученню приватного сектору та технологічних компаній до боротьби з інформаційними загрозами. У рамках Глобального альянсу за боротьбу з дезінформацією США ініціювали тісну співпрацю між урядами, громадянським суспільством і провідними технологічними компаніями, такими як Google, Facebook і Twitter. Ці платформи є основними каналами поширення дезінформації, тому їхня участь у створенні ефективних механізмів протидії є критично важливою. Наприклад, у рамках цієї співпраці було запроваджено алгоритми виявлення та блокування фейкових новин, а також підвищено прозорість політичної реклами в соціальних мережах [66].

Ще одним важливим аспектом є інформаційна дипломатія. США активно просувають ідеї свободи слова та доступу до інформації як основоположні принципи міжнародного співробітництва у боротьбі з інформаційними загрозами. Наприклад, у рамках Саміту за демократію, ініційованого президентом Дж. Байденом, США закликали країни до створення міжнародної коаліції для боротьби з дезінформацією та підтримки незалежної журналістики. Ця ініціатива має на меті посилити роль незалежних медіа у протидії маніпулятивному впливу недемократичних режимів.

США також активно співпрацюють із міжнародними організаціями у

сфері кібербезпеки. Наприклад, вони є членом Глобального форуму з кіберекспертизи (GFCE), який сприяє обміну досвідом у сфері кібербезпеки та розробці міжнародних стандартів протидії кіберзагрозам. У рамках цієї організації США фінансують програми технічної допомоги для країн, що розвиваються, з метою посилення їхньої стійкості до інформаційних загроз. На практичному рівні США проводять багато спільних навчань і симуляцій для підготовки до можливих інформаційних атак. Наприклад, щорічні навчання Cyber Flag, організовані Агентством з національної безпеки (NSA), об'єднують кіберфахівців із різних країн для моделювання сценаріїв кіберзагроз і розробки спільних стратегій реагування. Такі навчання не лише підвищують професійний рівень учасників, але й сприяють зміцненню довіри між партнерами [63, p. 125-130].

Важливою складовою міжнародного співробітництва у протидії інформаційним загрозам є підтримка демократичних інститутів і виборчих процесів. США активно співпрацюють з міжнародними організаціями, такими як Організація з безпеки і співробітництва в Європі (ОБСЄ), щоб моніторити вибори в країнах, де є ризик зовнішнього втручання. У рамках цієї співпраці США надають технічну підтримку, включаючи навчання спостерігачів і впровадження новітніх технологій для захисту виборчої інфраструктури. Наприклад, у 2019 році США співпрацювали з Україною, щоб запобігти кібератакам на сервери Центральної виборчої комісії, успішно відбивши кілька спроб втручання [72].

Особливу увагу США приділяють співпраці в Азіатсько-Тихоокеанському регіоні, де інформаційні загрози часто мають форму кібершпигунства та втручання в діяльність урядів і приватних компаній. У 2021 році було укладено угоду між США, Австралією, Японією та Індією в рамках ініціативи «Quad» про створення спільної платформи для обміну даними про кіберзагрози. Це дозволило оперативно реагувати на атаки, спрямовані на критичну інфраструктуру, зокрема, енергетичний сектор і фінансові установи. Співпраця в рамках «Quad» також включає проведення

спільних кібернавчань і розробку стандартів для захисту об’єктів критичної інфраструктури.

У боротьбі з інформаційними загрозами важливим інструментом є міжнародні угоди та нормативні документи, які регулюють поведінку держав в інформаційному просторі. США активно просувають ідею створення «Цифрової Хартії», яка має стати глобальним документом, що визначатиме правила для країн щодо використання цифрових технологій і забезпечення прозорості в інформаційній політиці. Підтримка цієї ініціативи з боку таких партнерів, як ЄС, Канада і Південна Корея, свідчить про потенціал для формування єдиних стандартів у цій сфері. Прикладом успішної регіональної ініціативи є співпраця США з країнами Балтії, які є одним із головних об’єктів дезінформаційних кампаній. У рамках «Ініціативи трьох морів» було створено програми для обміну досвідом у сфері медіаграмотності та підвищення стійкості суспільства до інформаційних маніпуляцій. США фінансують тренінги для журналістів, освітні програми для молоді та розробку програмного забезпечення для виявлення фейкових новин [60, p. 206-217].

Значну роль у міжнародній співпраці відіграють приватні компанії, зокрема технологічні гіганти, такі як Microsoft, Google і Meta. Вони працюють у тісному контакті з урядом США для розробки інструментів, що дозволяють протидіяти дезінформації та кібератакам. У 2020 році Microsoft у співпраці з Європейським Союзом запустила програму «Defending Democracy», яка спрямована на захист виборчих процесів від кібератак. Програма отримала підтримку з боку кількох держав, зокрема Німеччини та Франції, і стала важливим елементом глобальної стратегії кіберзахисту.

Підсумовуючи, можна сказати, що співпраця США з міжнародними організаціями, союзниками та іншими державами у протидії інформаційним загрозам є багатовекторною та комплексною. Вона охоплює такі аспекти, як участь у роботі міжнародних структур, фінансова та технічна допомога, спільні навчання, інформаційна дипломатія та залучення приватного сектору. Успішність цих зусиль значною мірою залежить від рівня координації між

учасниками, а також від здатності адаптуватися до нових викликів, які постійно виникають у сфері інформаційної безпеки. США продовжують активно розвивати цей напрямок, усвідомлюючи, що ефективна боротьба з інформаційними загрозами можлива лише у тісній співпраці з міжнародною спільнотою.

3.3. Досвід США для України у міжнародній співпраці щодо протидії інформаційному тероризму

Протидія інформаційному тероризму є одним із ключових викликів сучасного світу, особливо в умовах розвитку цифрових технологій, які кардинально змінили динаміку міжнародної співпраці. Інтеграція досвіду США повинна ґрунтуватися на глибокому аналізі потреб українського суспільства, ресурсів держави та геополітичного контексту. Однак, важливо також враховувати потенційні виклики, які можуть виникнути у процесі імплементації подібних стратегій. Досвід США у цій сфері може стати важливим орієнтиром для України, яка стикається з постійною інформаційною агресією. США, як одна з провідних держав у забезпеченні глобальної кібербезпеки та боротьбі з інформаційними загрозами, накопичили значний досвід, що включає законодавчі ініціативи, міжвідомчу співпрацю, розбудову партнерств із приватним сектором, а також взаємодію з міжнародними організаціями. Аналіз цього досвіду може надати Україні практичні інструменти для посилення власного потенціалу у сфері протидії інформаційному тероризму [72].

Інформаційний тероризм охоплює дії, спрямовані на маніпулювання інформацією, дестабілізацію суспільства, втручання у внутрішні справи держави або створення хаосу в міжнародній системі. Це явище стало особливо актуальним через поширення соціальних мереж, доступність дезінформаційних кампаній та технологічну еволюцію кіберзлочинності. Для України ця проблема набуває особливого значення через гібридну війну, яку

веде РФ паралельно з військовою агресією. Систематичні інформаційні атаки, пропаганда, маніпулювання громадською думкою та поширення фейків є ключовими елементами російської агресії. З огляду на це, досвід США може стати фундаментом для розробки ефективних стратегій протидії.

Для України важливим аспектом є використання досвіду США у побудові регіональних альянсів. У 2019 році США ініціювали створення Триморського партнерства, яке включає країни Центральної та Східної Європи, з метою посилення кібербезпеки та протидії гібридним загрозам. Участь України у подібних ініціативах могла б стати важливим кроком для посилення власного інформаційного потенціалу. Україна вже зробила певні кроки у напрямку протидії інформаційному тероризму. Прийняття закону про медіа, створення Центру протидії дезінформації та тісна співпраця з міжнародними партнерами свідчать про серйозність намірів держави. Однак існують значні виклики, зокрема обмеженість ресурсів, недостатня координація між відомствами та низький рівень технологічної інтеграції. Одним із ключових викликів є різниця у ресурсній базі та інституційному потенціалі між США та Україною. Американська система протидії інформаційному тероризму базується на значних фінансових вкладеннях, розвинутій технологічній інфраструктурі та доступі до передових досліджень. Для України адаптація цих підходів потребує не лише фінансування, але й перегляду пріоритетів державної політики, спрямованої на підтримку інформаційної безпеки [23, с. 119-124].

Іншим викликом є брак координації між різними органами влади. У США існує налагоджена система міжвідомчої співпраці, яка дозволяє ефективно реагувати на інформаційні загрози. Для України це залишається слабкою ланкою, оскільки різні відомства часто дублюють функції або діють у відриві одне від одного. Впровадження системи чіткої координації, яка включатиме урядові, неурядові та міжнародні організації, є важливим завданням.

Ще один аспект, який потребує уваги, – це рівень довіри громадян до

державних інституцій. У США урядова політика протидії інформаційному тероризму спирається на підтримку суспільства. В Україні ж довіра до інституцій часто є низькою через корупцію, політичну нестабільність та відсутність прозорості. Це може стати бар'єром для ефективної реалізації ініціатив у сфері інформаційної безпеки. США значну увагу приділяють залученню громадянського суспільства до боротьби з інформаційними загрозами. Медіаграмотність, критичне мислення та активна позиція громадян є важливими елементами стійкості до дезінформації. Для України ця сфера також потребує значного розвитку. Підвищення обізнаності серед населення про методи маніпуляції інформацією дозволить зменшити вплив пропаганди та фейків. Зокрема, важливим є впровадження освітніх програм, спрямованих на розвиток критичного мислення у школах та університетах. Американські ініціативи, як-от програми Digital Literacy Now, які фінансуються як урядом, так і приватними донорами, можуть стати прикладом для України. Вони охоплюють не лише молодь, але й ширші верстви населення, включаючи літніх людей, які є особливо вразливими до інформаційних маніпуляцій [17].

Інформаційний тероризм постійно еволюціонує, і технології стають як інструментом загроз, так і засобом їх нейтралізації. У США активно використовуються штучний інтелект, машинне навчання та аналіз великих даних для ідентифікації шкідливого контенту, виявлення дезінформаційних кампаній і прогнозування потенційних атак. Наприклад, аналітичні системи, які розробляються у співпраці з такими компаніями, як Palantir Technologies, дозволяють швидко ідентифікувати патерни дій зловмисників. Україна могла б використати ці технології, створюючи власні системи моніторингу інформаційного простору. Це особливо важливо в контексті російської агресії, яка включає багаторівневі інформаційні атаки. Однак важливо враховувати, що такі системи потребують значних ресурсів і високого рівня технічної експертизи. Для цього необхідно посилювати співпрацю з міжнародними донорами, які можуть надати як фінансову підтримку, так і експертну допомогу [1, с. 110-116].

Україна вже отримує значну підтримку від міжнародної спільноти у сфері протидії інформаційним загрозам. Зокрема, США активно фінансують проєкти, спрямовані на зміцнення інформаційної стійкості. Наприклад, у рамках програми USAID «Медійна програма в Україні» виділено десятки мільйонів доларів на підтримку незалежних медіа, боротьбу з дезінформацією та розвиток цифрової безпеки. Іншим важливим прикладом є програми ЄС, які також спрямовані на підвищення медіаграмотності та підтримку журналістів-розслідувачів. Україна може виступати як пілотний майданчик для впровадження нових підходів до боротьби з інформаційним тероризмом, оскільки її досвід має стратегічне значення для всієї Європи. З досвіду США можна виділити кілька ключових напрямів для адаптації [23, с. 119-124]:

1. Розбудова інституційного потенціалу, центр протидії дезінформації міг би стати аналогом американського Global Engagement Center, виконуючи роль координатора між різними урядовими структурами та міжнародними партнерами.

2. Залучення приватного сектору, українські технологічні компанії можуть відігравати важливу роль у розробці програмного забезпечення для моніторингу інформаційного простору та виявлення шкідливого контенту.

3. Посилення кібербезпеки, створення національного агентства, подібного до CISA, зосередженого на захисті критичної інфраструктури, могло б значно посилити здатність України протидіяти інформаційним атакам.

4. Фокус на медіаграмотності, масштабні програми освіти та інформування населення.

5. Міжнародна співпраця, участь у глобальних ініціативах, таких як Триморське партнерство чи програми НАТО, допоможе Україні отримати доступ до передових технологій та практик.

Співпраця України та США у сфері кібербезпеки вже має позитивні результати. У 2021 році відбулися спільні навчання із захисту критичної інфраструктури від кібератак, організовані за підтримки Агентства міжнародного розвитку США (USAID). Ці навчання допомогли українським

фахівцям вдосконалити навички реагування на інформаційні загрози. Іншим прикладом є програма з підвищення медіаграмотності, реалізована за підтримки американських партнерів. Ця ініціатива спрямована на підвищення обізнаності громадян щодо дезінформації та маніпуляцій у ЗМІ. Такі програми сприяють формуванню стійкості суспільства до інформаційного тероризму.

Досвід США у протидії інформаційному тероризму має ключове значення для України. Інтеграція американських практик, адаптованих до українських реалій, дозволить посилити національну безпеку та сприяти ефективнішій міжнародній співпраці. Ключовими елементами цього процесу є інтеграція інноваційних технологій, залучення громадськості та побудова міжнародних партнерств. Інформаційний тероризм є глобальною загрозою, і лише через консолідацію зусиль на національному та міжнародному рівнях Україна може забезпечити власну стійкість у цій сфері, ставши прикладом для інших країн. Таким чином, інтеграція досвіду США у стратегію України дозволить створити ефективну систему протидії інформаційному тероризму, що сприятиме як національній, так і глобальній безпеці.

Висновки до розділу 3

Інформаційний тероризм є однією з найбільших загроз сучасного світу, що змушує держави та міжнародні організації активно співпрацювати для протидії цьому явищу. Сполучені Штати Америки, як одна з провідних держав світу, відіграють ключову роль у створенні та впровадженні інституційних рамок міжнародної співпраці в боротьбі з інформаційним тероризмом. США мають розвинену нормативно-правову базу, яка включає закони, спрямовані на захист інформаційного простору, та спеціалізовані установи, такі як Агентство національної безпеки (АНБ) та Департамент внутрішньої безпеки (ДВБ). Важливим інструментом є й багатосторонні угоди та ініціативи, які створюють умови для співпраці з іншими державами та міжнародними організаціями.

У сфері міжнародної співпраці США активно взаємодіють із такими організаціями, як ООН, НАТО, Європейський Союз та ОБСЄ. Сполучені Штати беруть участь у розробці міжнародних стандартів кібербезпеки та ініціативах, спрямованих на обмін інформацією щодо кіберзагроз. Особливо важливим є партнерство США з Європейським Союзом, в рамках якого реалізуються програми посилення кіберстійкості та боротьби з дезінформацією. НАТО також є важливим партнером США у протидії інформаційному тероризму, зокрема через Центр кіберзахисту в Естонії. Крім того, США активно співпрацюють із такими країнами, як Великобританія, Канада, Австралія та Нова Зеландія у рамках альянсу "П’ять очей", що дозволяє обмінюватися розвідувальною інформацією та спільно протидіяти загрозам в інформаційному просторі.

Для України досвід США у боротьбі з інформаційним тероризмом та міжнародній співпраці є надзвичайно цінним. Зважаючи на гібридні загрози, які постійно виникають через дії РФ, Україні необхідно посилити інституційні механізми захисту інформаційного простору. Досвід США може бути корисним у формуванні національної стратегії кібербезпеки, розвитку спеціалізованих державних установ та створенні правової бази для боротьби з дезінформацією. Окрім цього, важливою є адаптація американського досвіду міжнародної співпраці, зокрема, у контексті партнерства з ЄС, НАТО та іншими міжнародними організаціями. Україні варто брати приклад з США у питаннях розробки двосторонніх угод із ключовими партнерами та участі у міжнародних програмах кіберзахисту.

ВИСНОВКИ

У результаті дослідження протидії інформаційному тероризму в США, зроблено наступні висновки:

1. Визначивши сутність поняття інформаційного тероризму, зроблено висновок, що інформаційний тероризм є специфічною формою тероризму, яка передбачає використання інформаційних технологій і засобів комунікації з метою досягнення політичних, соціальних, економічних або інших цілей шляхом маніпулювання інформацією, поширення фальшивих новин, пропаганди насильства та створення паніки серед населення. У сучасному світі інформаційний тероризм набув значної популярності через швидкий розвиток цифрових технологій, зокрема Інтернету, що дозволяє терористам здійснювати анонімні атаки на інформаційні системи та маніпулювати громадською думкою. Технології, які використовуються для реалізації інформаційного тероризму, включають хакерські атаки, фішинг, спам, поширення вірусів та інших шкідливих програм, а також операції з дезінформацією, що проводяться через соціальні мережі та медіаплатформи. Інформаційний тероризм може бути спрямований як на державні органи влади, так і на приватні компанії, громадські організації та окремих осіб. Однією з основних особливостей цього явища є його здатність швидко поширюватися по всьому світу завдяки глобальній мережі Інтернет, що ускладнює виявлення і припинення таких актів тероризму.

2. Розглянувши форми та методи протидії інформаційному тероризму, зроблено висновок, що ефективна боротьба з цим явищем вимагає комплексного підходу, який поєднує правові, технологічні та соціальні заходи. Зокрема, важливим елементом є розвиток законодавства, що регулює питання інформаційної безпеки та забезпечує правову відповідальність за злочини в інформаційній сфері. Однак цього недостатньо без належної технічної підтримки, що передбачає впровадження новітніх технологій для виявлення та нейтралізації загроз. Також необхідно забезпечити підготовку фахівців у галузі кібербезпеки, здатних оперативно реагувати на можливі інформаційні

атаки. Соціальні методи протидії включають підвищення рівня інформаційної свідомості громадян та сприяння їхньому вмінню критично оцінювати джерела інформації. Особливу увагу слід приділяти міжнародній співпраці в боротьбі з інформаційним тероризмом, оскільки сучасні загрози мають транснаціональний характер і потребують координації зусиль різних держав і міжнародних організацій. Лише за умови комплексного підходу, що включає технічні, правові, освітні та міжнародні аспекти, можна ефективно протистояти інформаційному тероризму та зменшити його негативний вплив на безпеку суспільства.

3. Визначивши вплив інформаційного тероризму на міжнародну безпеку, зроблено висновок, що цей феномен є одним із найбільш серйозних викликів сучасному світу. Інформаційний тероризм, як новітня форма терористичної діяльності, використовує інформаційні технології та кіберпростір для досягнення політичних, економічних та соціальних цілей. Він включає в себе акти дезінформації, кібератаки, маніпуляції інформацією і створення психологічного стресу серед населення та державних інститутів. Такі дії можуть дестабілізувати політичну ситуацію, знижувати рівень довіри до державних установ, а також підривати соціальний порядок у країнах. Вплив інформаційного тероризму на міжнародну безпеку проявляється в ряді аспектів. По-перше, через кібератаки на критичну інфраструктуру, що може привести до серйозних економічних та соціальних наслідків, порушення зв’язку та національної безпеки. По-друге, завдяки широкому поширенню дезінформації, що може призвести до політичних і соціальних конфліктів. Інформаційний тероризм також сприяє розпалюванню міжнародних криз, створюючи конфлікти між державами, зокрема у зв’язку з маніпулюванням громадською думкою та впливом на виборчі процеси.

4. Розглянувши законодавчі основи протидії інформаційному тероризму у США, зроблено висновок, що Сполучені Штати Америки мають розвинену правову базу для боротьби з інформаційним тероризмом, яка включає комплекс заходів, спрямованих на забезпечення національної безпеки

в умовах швидкого розвитку інформаційних технологій. Одним із основних інструментів є Закон про захист національної безпеки, що дозволяє уряду здійснювати моніторинг та контроль над інформаційними потоками, особливо в частині боротьби з терористичними організаціями, що використовують сучасні технології для пропаганди насильства та залякування населення. Важливу роль у протидії інформаційному тероризму відіграють також федеральні закони, які регулюють питання кібербезпеки, а також спеціальні органи, як-от ФБР та Департамент внутрішньої безпеки, що активно взаємодіють з приватними компаніями та міжнародними партнерами. Однак є й певні виклики, пов'язані з балансом між безпекою та захистом прав людини, що викликає певні юридичні та етичні дискусії. Загалом, законодавство США продовжує вдосконалюватися для ефективної боротьби з інформаційним тероризмом в умовах глобалізації та швидких змін у технологічному середовищі.

5. Розглянувши політику США у сфері кібербезпеки та протидії інформаційному тероризму, зроблено висновок, що Сполучені Штати приділяють значну увагу забезпеченню національної безпеки в кіберпросторі. Основними аспектами цієї політики є запобігання кіберзагрозам, виявлення та нейтралізація атак, а також зміцнення партнерства між урядом, приватним сектором та міжнародними організаціями. США активно розвивають нормативно-правову базу, створюючи стратегії, які включають інтеграцію новітніх технологій, покращення взаємодії між державними і приватними структурами, а також формування інститутів для боротьби з інформаційним тероризмом. У політиці США наголошується на превентивних заходах, таких як підвищення рівня обізнаності громадськості та удосконалення розвідувальних структур для виявлення потенційних загроз. Водночас проблема глобальних кіберзагроз вимагає міжнародної координації, зокрема у рамках ООН та інших безпекових організацій. Враховуючи швидкий розвиток технологій, важливим є постійне оновлення політик і заходів протидії, що дозволить ефективно реагувати на нові виклики у сфері кібербезпеки та

інформаційного тероризму.

6. Визначивши роль недержавних інституцій та організацій у протидії інформаційному тероризму, зроблено висновок, що ці структури мають важливе значення для забезпечення національної безпеки та стабільності. Недержавні організації можуть ефективно сприяти виявленню та нейтралізації загроз, оскільки вони мають можливість оперативно реагувати на нові виклики та загрози, що виникають у глобальному інформаційному просторі. Вони активно використовують сучасні технології для моніторингу інформаційних потоків, аналізу загроз та проведення освітніх кампаній для підвищення обізнаності громадян про методи протидії інформаційним атакам. Окрім цього, важливою є їх роль у формуванні громадської думки, боротьбі з дезінформацією та маніпуляціями в медіапросторі. Недержавні організації сприяють створенню механізмів взаємодії між державними і приватними структурами, надаючи незалежну платформу для оцінки ситуації та розробки стратегій щодо протидії інформаційному тероризму. Таким чином, їх діяльність має значний вплив на зміцнення національної безпеки, забезпечення стабільності та захисту демократичних цінностей в умовах інформаційних загроз.

7. Розглянувши інституційні рамки міжнародної співпраці США в боротьбі з інформаційним тероризмом, зроблено висновок, що Сполучені Штати мають розвинену та багатогранну систему організацій і механізмів, спрямованих на протидію загрозам в інформаційному просторі. Перш за все, це забезпечується через діяльність федеральних агентств, таких як Федеральне бюро розслідувань (FBI), Міністерство внутрішньої безпеки (DHS) та Агентство національної безпеки (NSA), які активно взаємодіють із міжнародними партнерами в межах багатосторонніх форумів, таких як ООН та НАТО. Крім того, важливим аспектом є співпраця США з союзниками в рамках двосторонніх угод та ініціатив, які дозволяють здійснювати обмін інформацією, розробляти спільні стратегії реагування та підвищувати ефективність контрзаходів. Роль приватного сектору також є суттєвою,

оскільки технологічні компанії виступають важливими партнерами в боротьбі з дезінформацією та кіберзагрозами. США активно сприяють розвитку глобальних стандартів і принципів у боротьбі з інформаційним тероризмом, підтримуючи ініціативи для покращення кібербезпеки, регулювання онлайн-контенту та протидії маніпуляціям з інформацією. Всі ці зусилля вказують на комплексний і багатосторонній підхід США до боротьби з інформаційним тероризмом на міжнародному рівні.

8. З'ясовано особливості співпраці США з міжнародними організаціями та іншими державами у протидії інформаційним загрозам, зазначено, що для ефективної боротьби з такими загрозами Сполучені Штати активно залучають різноманітні міжнародні структури, зокрема ООН, НАТО, ЄС та інші міжнародні альянси. Основними напрямками цієї співпраці є обмін розвідувальною інформацією, створення спільних стандартів у сфері кібербезпеки та здійснення колективних заходів для запобігання маніпуляціям з інформацією, кібератакам і дезінформаційним кампаніям. Зокрема, США здійснюють спільні операції з іншими країнами щодо боротьби з кіберзлочинністю, розробляють міжнародні правові норми для захисту інформаційної інфраструктури. Водночас зазначено, що в умовах геополітичної напруженості, така співпраця часто стикається з викликами через різницю в національних інтересах і стратегічних цілях. Проте, навіть у цих умовах, США залишаються активним учасником міжнародних ініціатив, прагнучи забезпечити глобальну безпеку та стабільність в інформаційній сфері. Окрему увагу приділено розвитку технологічних інновацій, які мають потенціал для зміцнення міжнародної координації та оперативного реагування на новітні загрози.

9. Розглянувши досвід США для України у міжнародній співпраці щодо протидії інформаційному тероризму, зроблено висновок, що активна участь України в міжнародних ініціативах та обміні досвідом з іншими державами є необхідною для ефективної протидії цим загрозам. США мають значний досвід у боротьбі з інформаційним тероризмом, який включає

створення спеціалізованих структур, впровадження інноваційних технологій для моніторингу та аналізу інформаційних загроз, а також розробку законодавчих ініціатив для забезпечення безпеки в інформаційному просторі. Україна може запозичити ці практики для удосконалення своєї політики в цій сфері. Одним з основних аспектів є розширення співпраці з міжнародними організаціями, зокрема НАТО та ЄС, що дозволить Україні інтегрувати новітні технології та стратегії боротьби з інформаційним тероризмом. Також важливою є розробка національних стандартів і заходів для захисту від кіберзагроз, які можуть бути використані терористами для маніпулювання громадською думкою. В цілому, використання досвіду США у боротьбі з інформаційним тероризмом є важливим кроком для зміцнення національної безпеки України та забезпечення стабільності в інформаційному просторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Банк Р.О. Інформаційний тероризм як загроза національній безпеці України: теоретико-правовий аспект. *Інформація і право.* № 1(16)/2016. С. 110-116.

2. Білан І.А. Кібертероризм: інформаційно-правовий аспект. *Інформація і право.* 2023. №4(47). С. 64-71.

3. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / за заг. ред. В. Б. Толубка. Київ: ДУТ, 2015. 288 с.

4. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Ukrainian Scientific Journal of Information Security.* 2013. Vol. 19. Issue 2. С. 118–129.

5. Гриник Р.О., Пилипенко В.М. Кібертероризм як нова форма міжнародного тероризму. *Актуальні задачі та досягнення у галузі кібербезпеки. Матеріали Всеукраїнської науково-практичної конференції 34-35 листопада 2016 року м. Кропивницький*. 2016. С. 61-64.

6. Грицун О. О. Питання міжнародно-правового регулювання інформаційного тероризму. *Часопис Київського університету права*. 2014. № 4. С. 312–317.

7. Гуцалюк М. Кібертероризм та заходи протидії. *Протидія терористичній діяльності: міжнародний досвід і його актуальність для України: матеріали міжнародної науково-практичної конференції. (30 вересня 2016 року, м. Київ).* Київ: Національна академія прокуратури України, 2016. С. 86–88.

8. Дзьобань О.П. Насильство інформаційне. Енциклопедія соціогуманітарної інформології. Київ: Видавничий дім «Гельветика», 2020. Т. 1. С. 151-155.

9. Законодавство та стратегії у сфері кібербезпеки країн європейського союзу, США, Канади та інших. *Інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром.* 2023.

URL: https://infocenter.rada.gov.ua/uploads/documents/28982.pdf (дата звернення: 21.10.2024).

10. Зінченко О. Політичні проблеми розвитку кібертероризму в міжнародному просторі. *Політикус*. 2024. №4. С. 154-160.

11. Іран звинуватив США у кібератаці на ядерні об'єкти. URL: https://ua.korrespondent.net/world/1174673-iran-zvinuvativ-ssha-u-kiberataci-nayaderni-obekti (дата звернення: 25.10.2024).

12. Когут Ю. Кібервійни, кібертероризм, кіберзлочинність. Київ: Консалтингова компанія Сідкон, 2022. 284 с.

13. Когут Ю. Кібертероризм (історія, цілі, об'єкти). Київ, 2023. 304 с.

14. Колосов О.О. Особливості протидії кіберзлочинам у Сполучених Штатах Америки. *Ірпінський юридичний часопис. Серія: право*. 2023. Вип. 1(10). С. 151–160.

15. Корченко О.Г. Кібернетична безпека держави: характерні ознаки та проблемні аспекти. *Безпека інформації*. 2013. №1. С. 10-17.

16. Корченко О.Г. Ознаковий принцип формування класифікацій кібератак. *Вісник Східноукраїнського національного університету імені Володимира Даля*. 2010. №1. С. 32-38.

17. Котляров В. Кібертероризм як загроза міжнародній безпеці. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2023. №5(71). С. 46-54.

18. Литвиненко Н.П., Погоріла Н.О. Концептуальне забезпечення політики глобального лідерства США постбіполярної доби. *Актуальні проблеми міжнародних відносин.* 2017. Вип. 132. С. 44-51.

19. Мокляк В.В. Сучасний досвід США у сфері запобігання тероризму. *Питання боротьби зі злочинністю*. 2017. № 34. С. 219-229.

20. Паламарчук С.А. Забезпечення захисту кіберпростору в провідних країнах світу. *Збірник наукових праць ВІТІ*. 2020. №1. С. 58-64.

21. Пилипчук В.Г., Дзьобань О.П. Теоретичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації.

Стратегічні пріоритети. 2021. № 4. С. 12-17.

22. Стежко С.М. Сучасний досвід США у сфері забезпечення кібербезпеки. *Інформація і право*. 2021. № 2(37). С. 139-144.

23. Шемчук В. Національна стратегія кібербезпеки США: досвід для України. *Науковий вісник Національної академії внутрішніх справ*. 2020. № 4. С. 119-124.

24. Щодо обстановки в сфері кібер на 23-24 лютого 2024 року. URL: https://cert.gov.ua/article/6277822 (дата звернення: 25.10.2024).

25. Appeals regarding cybersecurity in 2015. *Barack Obama Administration*. URL: https://obamawhitehouse.archives.gov/issues/foreign-policy/cybersecurity (Last accessed: 11.10.2024).

26. Arora B. Exploring and analyzing Internet crimes and their behaviours. *Perspect Sci.* 2016. №8. P. 540-560.

27. Bakker R., Hill D. W. Jr, Moore W. H. «How Much Terror? Dissidents, Governments, Institutions, and the Cross-national Study of Terror Attacks». *Journal of Peace Research*. 2016. №53 (5). P. 711–726.

28. Biden-Harris Administration. National Cybersecurity Strategy. *The White House.* 2023. URL: whitehouse.gov (Last accessed: 22.10.2024)

29. Bill H. R. United States-Ukraine cybersecurity cooperation and require a report regarding such cooperation, and for other purposes: Congress of the United States of America, 2017. URL: https://docs.house.gov/billsthisweek/20180205/HR1997.pdf (Last accessed: 11.10.2024).

30. Bill H.R. 739–116th Congress: To support United States international cyber diplomacy, and for other purposes: Congress of the United States of America. 2019. URL: https://www.congress.gov/bill/116th-congress/house-bill/739/text#toc-HF69B2046ABEB4D71A8C145F6BFBADD92 (Last accessed: 11.10.2024).

31. Blinken A. United States International Cyberspace & Digital Policy Strategy. *U.S. Department of State.* URL: https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/ (Last accessed: 25.10.2024).

32. Brenner S. W. Cyber Threats: The Emerging Fault Lines of the Nation State. Oxford University Press, 2011. 296 p.

33. Cameron K. The Cyber Diplomacy Act of 2017: Giving Cyber the Importance It Needs at the State Department. *Hard National Security Choices*. 2017. URL: https://www.lawfareblog.com/cyber-diplomacy-act-2017-giving-cyber-importance-it-needs-state-department (Last accessed: 11.10.2024).

34. Center for Strategic and International Studies (CSIS). The Biden-Harris Administration's National Cybersecurity Strategy. 2023. URL: https://www.csis.org/ (Last accessed: 22.10.2024)

35. CISA's Role in Cybersecurity: Combating cyber crime. *Cybersecurity and infrastructure Security Agency USA*. URL: https://www.cisa.gov/combating-cyber-crime (Last accessed: 21.04.2021).

36. Counter-terrorism in cyberspace. *Unated Nation Security*. 2024. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/ctc_cted_factsheet_ct_in_cyberspace_oct_2021.pdf (Last accessed: 25.10.2024).

37. Cyber incident response. *Cybersecurity and infrastructure Security Agency USA*. 2023. URL: https://www.cisa.gov/cyber-incident-response (Last accessed: 11.10.2024).

38. Cybersecurity Adoption and Awareness. U.S. *National Institute of standards and technology (NIST)*. 2019. URL: https://csrc.nist.gov/Projects/usable-cybersecurity/research-areas/cybersecurity-adoption (Last accessed: 11.10.2024).

39. Cybersecurity Programs and Policy. *U.S. General Services Administration*. 2021. URL: https://www.gsa.gov/technology/government-it-initiatives/cybersecurity/cybersecurity-programs-policy (Last accessed: 11.10.2024).

40. Cybersecurity strategy. *U.S. Department of Foreign Security*. 2018. URL: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf (Last accessed: 11.10.2024).

41. Cybersecurity. *Office of the Coordinator For Cyber Issues*. 2015. URL: https://2009-2017.state.gov/documents/organization/255008.pdf (Last accessed: 11.10.2024).

42. Federal Information Security Modernization Act of 2014 (S. 2521 (113th): Congress of the United States of America. 2014. URL: https://www.govtrack.us/congress/bills/113/s2521/text (Last accessed: 11.10.2024).

43. Golase P.R. A comparative analysis of the factors predicting fears of terrorism and cyberterrorism in a developing nation context. *Journal of Ethnic and Cultural Studies.* 2022. №9(4). P. 106-119.

44. Iftikhar S. Cyberterrorism as a global threat: a review on repercussions and countermeasures. *PeerJ Computer Science*. 2024. №10.

45. International Cybersecurity Priorities: Fostering Cybersecurity Innovation Globally. *U.S. Department of Commerce*. 2017. URL: https://www.commerce.gov/sites/default/files/2018-06/International%20Cybersecurity%20Priorities%20Report.pdf (Last accessed: 11.10.2024).

46. Internet Users by Country 2024. World Population by Country 2024 (Live). https://worldpopulationreview.com/country-rankings/internetusers-by-country (Last accessed: 25.10.2024).

47. Judith H. G. Cybersecurity Partnerships: A New Era of Public-Private Collaboration. *Center on Law and Security*. 2014. URL: https://www.lawandsecurity.org/wp-content/uploads/2016/08/Cybersecurity.Partnerships-1.pdf (Last accessed: 11.10.2024).

48. Kaminska M. Risk Aversion Is at the Heart of the Cyber Response Dilemma. *Council on foreign relations*. 2021. URL: https://www.cfr.org/blog/risk-aversion-heart-cyber-response-dilemma (Last accessed: 11.10.2024).

49. Knake R. K. Most Tools Failed to Detect the SolarWinds Malware. Those That Did Failed Too. *Digital and Cyberspace Policy Program and Net*

Politics. 2021. URL: https://www.cfr.org/blog/most-tools-failed-detect-solarwinds-malware-those-did-failed-too (Last accessed: 11.10.2024).

50. Knake R.K. A Cyberattack on the U.S. Power Grid: Contingency Planning Memorandum. *Council on Foreign Relations*. № 31. 2017. URL: https://cfrd8-files.cfr.org/sites/default/files/pdf/2017/03/ContingencyPlanningMemo31_Knake.pdf (Last accessed: 25.10.2024).

51. Knake R.K. Cleaning Up U.S. Cyberspace. *Council on Foreign Relations*. 2015. URL: https://cfrd8-files.cfr.org/sites/default/files/pdf/2015/12/Cleaning_Up_CyberBrief.pdf[20.11.2021 (Last accessed: 25.10.2024).

52. Lee C.S., Choi K.S., Shandler R., Kayser C. Mapping global cyberterror networks: an empirical study of Al-Qaeda and ISIS cyberterrorism events. *J Contemp Crim Justice*. 2021. №37(3). P. 333–355.

53. Levin A. Securing Cyberspace: A Comparative Review of Strategies Worldwide. *Privacy and cybercrime institute*. 2012. URL: https://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_cyber_crime_final_report.pdf (Last accessed: 11.10.2024).

54. Macdonald S., Jarvis L., Chen T. Lavis, S. Cyberterrorism: A Survey of Researchers. *Cyberterrorism Project Research Report. Swansea University.* 2013. № 1. URL: www.cyberterrorism-project.org (Last accessed: 25.10.2024).

55. Mahmood R., Jetter M. Communications Technology and Terrorism. *Journal of Conflict Resolution.* 2019. Vol. 64. Iss.1. P. 89-109.

56. Montasari R. Countering Cyberterrorism. The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK National Cybersecurity. United Kingdom: Springer, 2023. 164 p.

57. Montasari R. Countering cyberterrorism: the confluence of artificial intelligence, cyber forensics and digital policing in US and UK national cybersecurity. *Intelligence and National Security.* 2024. Vol. 39. P. 115-125.

58. National cybersecurity strategy USA. 2023. URL:

https://peerj.com/articles/cs-1772.pdf (Last accessed: 25.10.2024).

59. National Security Agency USA. *Central Security Service.* URL: https://www.nsa.gov/ (Last accessed: 11.10.2024).

60. Nechyporuk M., Pavlikov V., Filipenko N. Cyberterrorism Attacks on Critical Infrastructure and Aviation: Criminal and Legal Policy of Countering. *Integrated Computer Technologies in Mechanical Engineering – 2020*. 2021. Vol. 188. P. 206–217.

61. Neuberger A. The Cybersecurity Threat From Russia. *Council on foreign relations*. 2021. URL: https://www.cfr.org/event/cybersecurity-threat-russia (Last accessed: 11.10.2024).

62. Painter C. Diplomacy in cyberspace: The rise of the internet and cyber technologies constitutes one of the central foreign policy issues of the 21st century. *The foreign service journal*. 2018. URL: https://www.afsa.org/diplomacy-cyberspace (Last accessed: 11.10.2024).

63. Pillar P.R. Counterterrorism. London: Routledge, 2023. 16 p.

64. Pitaksantayothin J. Cyber terrorism laws in the United States, the United Kingdom and Thailand: a comparative study. *Chulalongkorn Law Journal.* 2014. №32(2). P. 169–185.

65. Plotnek J.J., Slay J. Cyber terrorism: a homogenized taxonomy and definition. *Computer Security*. 2021. №10. P.1–9.

66. Reiber J., Glenn M. The U.S. Government Needs to Overhaul Cybersecurity. Here's How. *Cybersecurity*. 2021. URL: https://www.lawfareblog.com/us-government-needs-overhaul-cybersecurity-heres-how (Last accessed: 11.10.2024).

67. Robillard M. National counter-terrorism responses: United States of America. *Political Science and Public Policy.* 2021. P. 212–232. URL: https://www.elgaronline.com/downloadpdf/edcoll/9781800371293/9781800371293.00019.pdf (Last accessed: 25.10.2024).

68. Secure Cyberspace and Critical Infrastructure. *Department of Homeland Security, DHS*. 2024. URL: https://www.dhs.gov/secure-cyberspace-and-critical-infrastructure (Last accessed: 11.10.2024).

69. Scrivens R., Gill P., Conway M. The role of the internet in facilitating violent extremism and terrorism: suggestions for progressing research. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. Palgrave: Macmillan, Cham, 2020. P. 1417–1435.

70. Shakhbazian K. Cooperation of states in the field of combating cyber crime and approaches to solving the problem of cyber terrorism. *Actual problems of International Relations*. 2021. Vol. 1. №148. P. 35-48.

71. Shandler R., Gross M.L., Backhaus S. Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment. *British Journal of Political Science.* 2022. Vol. 52. Iss. 2. P. 850–868.

72. Shemchuk V. National Cyber Strategy of the United States of America: Experience for Ukraine. *Naukovij visnik Nacional'noi akademii vnutrisnih sprav*. 2019. URL: http://elar.naiau.kiev.ua/jspui/bitstream/123456789/17521/1/%D0%9D%D0%92%204%2819%29_p119-124.pdf (Last accessed: 11.10.2024).

73. Sherman J., Herr T. The U.S. Should Make «Leverage» the Foundation of Its Cyber Strategy. 2021. URL: https://www.cfr.org/blog/us-should-make-leverage-foundation-its-cyber-strategy (Last accessed: 11.10.2024).

74. Sico van der Meer. Foreign Policy Responses to International Cyber-attacks. *Netherlands institute of Foreign Relations*. 2015. URL: https://www.clingendael.org/sites/default/files/pdfs/Clingendael_Policy_Brief_Foreign%20Policy%20Responses_September2015.pdf (Last accessed: 11.10.2024).

75. Simran R. Maker. New frontier in defense: cyberspace and U.S. foreign policy. *Report of National Committee on American Foreign*. Policy. 2017. URL: https://www.ncafp.org/2016/wp-content/uploads/2017/05/Cyberspace-and-US-Foreign-Policy-Report-May-17.pdf (Last accessed: 11.10.2024).

76. Stigal D., Miller C. The 2018 U.S. National Strategy for

Counterterrorism: A Synoptic Overview. *Journals and Periodicals.* 2020. URL: https://heinonline.org/HOL/LandingPage?handle=hein.journals/natislaw10&div=3&id=&page= (Last accessed: 25.10.2024).

77. Strategic Goal 2: Keep Our Country Safe. *Objective 2.4: Enhance Cybersecurity and Fight Cybercrime.* URL: https://www.justice.gov/doj/doj-strategic-plan/objective-24-enhance-cybersecurity-and-fight-cybercrime (Last accessed: 25.10.2024).

78. Sutherland D. What Is a Cybersecurity Legal Practice? *Cybersecurity*. 2021. URL: https://www.lawfareblog.com/what-cybersecurity-legal-practice (Last accessed: 11.10.2024).

79. Taplin R. Cyber Risk, Intellectual Property Theft and Cyberwarfare: Asia, Europe and the USA. London: Routledge, 2020.

80. The DoD Cyber Strategy. *The Department of Defense.* 2015. URL: https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf (Last accessed: 11.10.2024).

81. The National Cyber Strategy 2017-2021. *Office of the Coordinator for Cyber Issues*. URL: https://2017-2021.state.gov/key-topics-office-of-the-coordinator-for-cyber-issues/index.html (Last accessed: 11.10.2024).

82. The USA Patriot Act. URL: https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf (Last accessed: 25.10.2024).