МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

УКРАЇНСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІМЕНІ МИХАЙЛА ДРАГОМАНОВА

Історичний факультет

Кафедра історії міжнародних відносин та гуманітарних дисциплін

МАГІСТЕРСЬКА РОБОТА

На тему:

«Інформаційний тероризм як загроза міжнародній безпеці»

Кваліфікаційна робота на здобуття освітнього рівня «магістр» за спеціальністю 291 – міжнародні відносини, суспільні комунікації та регіональні студії

Студента 2 курсу, групи 2МІМВЗ, заочної форми навчання, напряму підготовки «магістр» спеціальності Міжнародні відносини, суспільні комунікації та регіональні студії.

Наволовського Захара Р.

Керівник: кандидат філософських наук, доцент, професор кафедри міжнародних та регіональних студій **Цибух Валерій Іванович**

Національна шкала: _____

Кількість балів: _____ Оцінка: ECTS _____

Голова комісії

_____ _____

(підпис) (прізвище та ініціали)

Члени комісії:

_____ _____

(підпис) (прізвище та ініціали)

_____ _____

(підпис) (прізвище та ініціали)

_____ _____

(підпис) (прізвище та ініціали)

Київ – 2025

ЗМІСТ

ВСТУП

У сучасному світі, де інформаційні технології стали невід'ємною частиною повсякденного життя, питання безпеки набуває нових вимірів, а загроза інформаційного тероризму виходить далеко за межі традиційних понять військового або політичного конфлікту. Інформаційний тероризм — це явище, що полягає у свідомому використанні цифрових засобів масової інформації для впливу на свідомість людей, залякування населення, створення атмосфери хаосу та дестабілізації державних інституцій. Особливості цього явища полягають у високій швидкості поширення інформації, можливості масштабного впливу через глобальні мережі та використанні сучасних технологій, таких як штучний інтелект, deepfake, алгоритми аналізу даних та бот-мережі. Проблема інформаційного тероризму є надзвичайно актуальною для міжнародної безпеки, оскільки вона безпосередньо впливає на політичну стабільність, економічний розвиток і соціальну згуртованість суспільств у багатьох країнах.

Актуальність теми. Актуальність дослідження зумовлене тим, що інформаційний тероризм став невід’ємною складовою міжнародних конфліктів і гібридних стратегій. Його масштаби зростають разом із розвитком соціальних мереж, штучного інтелекту та цифрових платформ. Інформаційні атаки здатні впливати на виборчі процеси, стратегічні рішення, міжнародну підтримку, економічну стабільність та соціальну згуртованість. Україна переживає ці процеси у найбільш концентрованій формі, що робить аналіз інформаційного тероризму критично важливим для формування національної та міжнародної політики безпеки. У сучасних умовах, коли цифровий простір стає основною ареною для проведення конфліктів, країни змушені пристосовувати свої стратегії безпеки до нових викликів, що породжуються інформаційними атаками. Глобальний характер таких загроз вимагає не лише національних заходів, але й активної міжнародної співпраці, створення спільних стандартів, нормативних актів та технологічних рішень, здатних запобігти поширенню дезінформації та

маніпулятивних наративів. Дослідження теми "Інформаційний тероризм як загроза міжнародній безпеці" є надзвичайно важливим з огляду на стрімкий розвиток цифрових технологій, збільшення кількості транскордонних кібернападів та дестабілізуючого впливу дезінформаційних кампаній.

Мета магістерської роботи полягає у всебічному аналізі сучасних методів інформаційного тероризму, оцінці його впливу на глобальну стабільність та розробці рекомендацій щодо вдосконалення національних і міжнародних механізмів протидії. Мета роботи передбачає розв'язання таких ***дослідницьких завдань***:

- Вивчити технологічні, психологічні та організаційні інструменти, що використовуються для здійснення інформаційного тероризму.
- Проаналізувати, як інформаційний тероризм впливає на політичну стабільність, економіку та соціальну згуртованість держав.
- Визначити, яким чином маніпулятивні інформаційні кампанії можуть спричиняти дестабілізацію та створювати передумови для конфліктів.
- Дослідити підходи різних країн і міжнародних організацій до протидії інформаційним загрозам.
- Запропонувати практичні рекомендації щодо удосконалення систем кібербезпеки та протидії дезінформації на національному та міжнародному рівнях.
- Проаналізувати, як інформаційні технології впливають на формування суспільної думки та змінюють політичний ландшафт.

Об'єктом дослідження виступає явище інформаційного тероризму в цілому, тобто його як комплексну форму загроз, що виникає в цифровій епосі та має значний вплив на міжнародну безпеку, політичну стабільність, економіку та соціальну згуртованість. Це явище охоплює використання сучасних технологій, засобів масової інформації, кіберзасобів, психологічних методів впливу, а також організаційних структур, що здійснюють дезінформаційні кампанії, маніпуляції та інші форми інформаційних атак.

Предметом дослідження є конкретні механізми, методи та засоби, які застосовуються для здійснення інформаційного тероризму, а також правові, технічні та організаційні підходи до його протидії. Тут розглядаються, зокрема, такі аспекти: як інформаційні терористи формують та поширюють маніпулятивні наративи; як державні та недержавні інститути виявляють і нейтралізують ці загрози; які міжнародні правові інструменти та технологічні рішення впроваджуються для забезпечення інформаційної безпеки; і як вплив інформаційного тероризму відображається на глобальній безпеці.

Теоретичне значення роботи. Дослідження інформаційного тероризму як загрози міжнародній безпеці має значний теоретичний внесок. По-перше, робота сприяє розвитку сучасної концепції безпеки в умовах цифрової епохи, розширюючи традиційні підходи до розуміння загроз за рахунок інтеграції елементів кібербезпеки, психології та інформаційних технологій. По-друге, вона дозволяє сформувати міждисциплінарну методологію аналізу інформаційних атак, що об'єднує дані з різних галузей знань та надає можливість точніше визначати механізми поширення дезінформації і маніпуляції суспільною думкою. По-третє, дослідження ідентифікує ключові чинники, які впливають на ефективність інформаційного тероризму, та описує їх взаємодію, що допомагає сформувати базу для подальших теоретичних розробок у галузі міжнародної безпеки та протидії цифровим загрозам. Таким чином, робота збагачує наукову літературу, пропонуючи нові концептуальні підходи до вивчення інформаційних загроз і дає змогу розробляти більш гнучкі та адаптивні моделі реагування на сучасні виклики.

Практичне значення роботи. Завдяки детальному розгляду механізмів поширення дезінформації та інформаційних атак, пропонуються інноваційні підходи до моніторингу цифрового простору, що сприятиме швидкому реагуванню на кіберзагрози. Практичні висновки можуть бути використані законодавцями для формування нормативно-правових актів, спрямованих на регулювання інформаційного простору і протидію маніпуляціям.

Розділ І

Теоретичні засади інформаційного тероризму

1.1 Поняття інформаційного тероризму: визначення та основні характеристики

Інформаційний тероризм — це форма тероризму, яка використовує інформаційні технології та засоби масової інформації для досягнення політичних, релігійних або ідеологічних цілей шляхом залякування, дезінформації або маніпуляції свідомістю мас. Це явище стало особливо актуальним у сучасному світі, де інформація поширюється миттєво, а цифрові платформи стали невід'ємною частиною повсякденного життя. Технології, що застосовуються для інформаційного тероризму, постійно розвиваються, адаптуючись до нових умов та цифрових реалій. Одним із найефективніших інструментів інформаційного тероризму є соціальні мережі (Facebook, Twitter, Telegram, TikTok). Через них поширюється пропаганда, дезінформація та маніпулятивний контент. Аавтоматизовані акаунти, що масово поширюють певні наративи, штучно створюючи "популярність" інформації. Вони можуть лайкати, коментувати та поширювати фейковий контент, створюючи ілюзію підтримки чи паніки, спеціально навчені люди, які маніпулюють громадською думкою, вкидають провокаційні теми, ображають опонентів і провокують соціальні конфлікти. Використання механізмів платформи для того, щоб фейкова інформація ставала вірусною, наприклад, через багаторазове поширення в групах або за допомогою накрутки взаємодій. Використовуючи штучний інтелект, можна створювати реалістичні відео чи аудіо, де відомі особи говорять або роблять те, чого ніколи не було. Ще можна створити відео, де президент країни закликає до капітуляції або розпалює міжнаціональну ворожнечу. За допомогою ШІ можна підробити голос будь-якої людини, створивши фейкові телефонні дзвінки чи звернення. Редагування відео або фотографій для створення альтернативної реальності (наприклад, показати протест, якого не було, або приписати злочин конкретній групі людей). Хакерські атаки є ключовою

частиною інформаційного тероризму. Вони дозволяють знищувати або змінювати важливу інформацію, перехоплювати дані та порушувати роботу інфраструктури. «DDoS-атаки» – масова атака на сервери, яка може "покласти" державні сайти, новинні портали або соціальні платформи, що використовуються для правдивої інформації. Хакери можуть отримати контроль над урядовими ресурсами та публікувати фейкові заяви від імені уряду або силових структур. Шпигунські програми можуть використовуватися для викрадення персональних даних, компрометації чиновників або отримання доступу до критичної інформації.

Окремий інструмент інформаційного тероризму – це створення псевдо-ЗМІ, які видають фейкові новини за правду. Сайти-клони – сторінки, які імітують відомі медіа, але поширюють викривлену або вигадану інформацію. Telegram-канали та закриті платформи. Telegram став однією з основних платформ для поширення інформаційного тероризму. Він забезпечує анонімність, дозволяє швидко поширювати контент та важко контролюється державами. Анонімні канали – пропагандистські канали можуть поширювати дезінформацію, створювати паніку та організовувати інформаційні спецоперації. створення чатів для координації протестів, диверсій або кампаній тиску на суспільство. Зловмисники можуть маніпулювати алгоритмами Google, щоб поширювати потрібні їм наративи у топ-результатах пошуку, масове поширення посилань на фейкові ресурси, щоб вони виходили в топ, створення ілюзії, що певна тема є дуже популярною, атаки на сайти опонентів, щоб вони випадали з результатів пошуку.

Деякі інформаційні атаки будуються на складних психологічних механізмах, залучаючи гейміфікацію для маніпуляції людьми, навмисне поширення напівправди або брехні, щоб змусити суспільство повірити у змову або зраду, створення вірусних трендів, які поширюють певні ідеї або викликають емоційний відгук, посилення розколу всередині країни через створення інформаційного конфлікту між різними групами. Інформаційний тероризм є комплексним явищем, яке поєднує в собі технологічні та психологічні методи

впливу. Зловмисники використовують соціальні мережі, ШІ, deepfake, кібератаки, Telegram-канали та маніпуляцію пошуковими системами, щоб дестабілізувати суспільство, підірвати довіру до державних інституцій і викликати паніку.

Засоби масової інформації є одним із найпотужніших інструментів інформаційного тероризму. Завдяки своїй здатності формувати громадську думку, поширювати наративи та контролювати потік інформації, вони можуть стати зброєю в руках тих, хто прагне маніпулювати масами, розпалювати страх, підривати довіру до інституцій або провокувати конфлікти. Один із ключових способів використання ЗМІ для інформаційного тероризму – це розповсюдження дезінформації. Це може бути повне вигадування подій, викривлення фактів або подача інформації в маніпулятивному контексті. терористи інформаційної війни часто використовують "екстрені" новини для дестабілізації суспільства. Це може бути, наприклад, фейкова заява про атаку, введення воєнного стану або катастрофу. У багатьох випадках створюються псевдо-медіа, які зовні виглядають як реальні інформаційні ресурси, але насправді працюють заради пропаганди або дискредитації. Підконтрольні державним або терористичним групам канали, що працюють під виглядом незалежних журналістів. Вони активно просувають певні політичні чи воєнні наративи. Альтернативні "незалежні" медіа – ще один спосіб введення аудиторії в оману. Такі ресурси зазвичай позиціонують себе як "єдиний чесний голос", що розкриває "правду", якої нібито не дають побачити великі ЗМІ. Один із найефективніших способів впливу – це організація інформаційних спецоперацій, які розгортаються у кілька етапів:

1) Запуск вкидової інформації – наприклад, на маловідомому ресурсі публікується вигадана історія.

2) ідхоплення "сумнівними" ЗМІ – кілька інших, трохи впливовіших ресурсів поширюють цю історію без перевірки.

3) Переклад і поширення в міжнародних медіа – якщо наратив працює добре, його підхоплюють вже більш впливові міжнародні ресурси.

4) Використання соцмереж для тиражування – одночасно йде масштабна інформаційна атака через соцмережі, де боти та тролі розганяють тему.

5) Дискусія серед авторитетних експертів – після резонансу залучаються "експерти", які коментують ситуацію, часто посилюючись на першоджерело-фейк.

Таким чином, навіть повністю вигадана інформація може перетворитися на "факт", якщо достатня кількість людей у неї повірить.

Нагнітання страху через ЗМІ. Страх – це один із найсильніших психологічних інструментів, і його часто використовують через ЗМІ для залякування населення. Наприклад, замість реальної оцінки терористичних загроз ЗМІ можуть нагнітати паніку, повідомляючи, що "атака може статися в будь-який момент". Терористичні акти, природні катастрофи, соціальні протести можуть подаватися так, ніби вони є набагато масштабнішими, ніж насправді. Використання емоційних кадрів – показування трагічних зображень та відео для максимального емоційного впливу, навіть якщо вони не мають прямого стосунку до подій. Телебачення залишається ключовим інструментом формування думки серед широкої аудиторії.

Політичні ток-шоу часто використовуються як інструмент маніпуляції:

1) Запрошення провокативних гостей – у дискусіях можуть брати участь "експерти", які навмисно просувають маніпулятивні або неправдиві тези.

2) Контрольована модерація – ведучі можуть спрямовувати дискусію у потрібне русло, підтримуючи одних спікерів та перебиваючи інших.

3) Маніпуляція аудиторією в студії – глядачі можуть бути підібрані так, щоб аплодувати або негативно реагувати на певні висловлювання, створюючи ефект масової підтримки чи засудження.

ЗМІ можуть цілеспрямовано працювати над переписуванням історії, щоб сформувати вигідний політичний чи ідеологічний порядок денний. створення документальних фільмів або публікацій, що представляють тиранів у позитивному світлі. цілеспрямована інформаційна кампанія проти історичних діячів, щоб підірвати національну ідентичність. Публікації, що представляють різні групи населення як ворогів, намагаючись розколоти суспільство. Популярні інфлюенсери можуть отримувати фінансову підтримку для просування потрібних наративів. Засоби масової інформації можуть бути як інструментом правди, так і зброєю в руках інформаційних терористів. Через фейки, маніпуляції, страх, викривлення фактів, контрольовані дебати та переписування історії можна не лише впливати на громадську думку, а й змінювати хід подій у світі.

1.2 Відмінності між інформаційним тероризмом, кібератаками та інформаційною війною

Інформаційний тероризм, кібератаки та інформаційна війна – це три явища, що використовують інформаційні технології, але вони мають різний характер, цілі та методи реалізації. Інформаційний тероризм передбачає свідоме використання засобів масової інформації та цифрових платформ для залякування населення, створення паніки та дестабілізації суспільства. Це явище орієнтоване переважно на психологічний вплив: за допомогою дезінформації, маніпуляцій фактами, поширення фейкових новин чи емоційно зарядженого контенту терористи створюють атмосферу страху і невизначеності. Метою є не стільки прямий фізичний збиток, скільки руйнування довіри до державних інститутів, викликання хаосу та розколу у суспільстві. Кібератаки – це технічно спрямовані операції, що використовують комп'ютерні мережі та інформаційні системи для завдання шкоди, викрадення даних, зупинки роботи критично важливих інфраструктур або шпигунства. Основний акцент тут робиться на технологічних засобах: злом серверів, DDoS-атаки, використання шкідливого програмного забезпечення (вірусів, троянів) для порушення нормального функціонування систем. Хоча кібератаки можуть бути частиною інформаційної війни чи навіть інформаційного тероризму, їх первинна мета – це руйнування або тимчасове припинення роботи інформаційних систем, а не обов'язково створення психологічного терору. Інформаційна війна є більш широкою концепцією, яка об'єднує як елементи дезінформації та пропаганди, так і кібератаки. Це комплекс заходів, спрямованих на формування або зміну громадської думки, підрив опонентської здатності приймати рішення та ослаблення суспільної стабільності. Вона може включати як пряму маніпуляцію медіа, так і технічні атаки на комунікаційні мережі. Інформаційна війна ведеться, як правило, на державному або напівдержавному рівні і є невід'ємною частиною сучасного гібридного конфлікту, де інформація використовується як стратегічна зброя. Інформаційний тероризм орієнтований на створення страху і паніки через маніпуляцію інформацією та дезінформацію з метою психологічного впливу на населення.

Кібератаки використовують технологічні засоби для прямого руйнування або порушення роботи комп'ютерних систем і мереж, що можуть бути спрямовані як на державні, так і на приватні структури. Інформаційна війна охоплює комплекс дій, які поєднують в собі елементи дезінформації, пропаганди та кібератак, і спрямовані на досягнення стратегічних політичних чи військових цілей на макрорівні.

Уявімо собі вигадану країну Новорію, яка стикається із загрозою з боку ворожої держави Рімланд. Ворог використовує різні інформаційні технології для дестабілізації Новорії, застосовуючи інформаційний тероризм, кібератаки та інформаційну війну. На цьому прикладі ми розглянемо основні відмінності між цими поняттями.

Інформаційний тероризм. Рімланд запускає масовану дезінформаційну кампанію у соціальних мережах, поширюючи сфальсифіковані новини про те, що найближчими днями у Новорії станеться серія руйнівних вибухів. Боти, фейкові акаунти та контрольовані «експерти» поширюють панічні повідомлення, підроблені фото з нібито жертвами атак, створюючи ілюзію справжньої загрози. У результаті серед населення зростає паніка: люди починають масово покидати міста, магазини спорожнюються, транспортні системи перевантажені. Основна мета такої атаки — не завдати фізичної шкоди, а підірвати довіру громадян до уряду, створити хаос і дестабілізувати суспільство через страх та невизначеність.

Кібератаки. Паралельно хакери Рімланду атакують державну інфраструктуру Новорії. Вони запускають масштабну DDoS-атаку на урядові вебсайти, роблячи їх недоступними для громадян, зламують системи банків та вимикають сервери лікарень, через що електронні медичні картки стають недоступними, а пацієнти не можуть отримати необхідне лікування. Також хакери отримують доступ до мережі електропостачання та тимчасово знеструмлюють декілька великих міст. Основна мета такої атаки — завдати реальної шкоди інфраструктурі, послабити обороноздатність країни та порушити нормальне функціонування держави. На

відміну від інформаційного тероризму, що впливає на психологічний стан людей, кібератаки завдають прямої шкоди об’єктам критичної інфраструктури.

Інформаційна війна. Рімланд веде комплексну кампанію, що поєднує елементи інформаційного тероризму та кібератак, використовуючи довгострокові стратегічні методи. Вони зламують національні телеканали та запускають фальшиві новини про те, що уряд Новорії начебто уклав секретну угоду з іншими країнами про продаж природних ресурсів за безцінь. Одночасно в соціальних мережах поширюються маніпулятивні відео з підробленими заявами політичних лідерів, що викликає обурення серед громадян. Також хакери зливають у відкритий доступ фальшиві «секретні документи», нібито підтверджуючи ці звинувачення. Головна мета інформаційної війни — підрив довіри до державних інституцій, розкол суспільства та створення сприятливих умов для політичної та військової дестабілізації. Якщо інформаційний тероризм спрямований на поширення страху серед населення шляхом дезінформації, а кібератаки зосереджені на руйнуванні інфраструктури, то інформаційна війна — це довгострокова стратегія, яка поєднує обидва методи з метою повного підриву стабільності країни. Уявімо, що Новорія зможе швидко відновити доступ до своїх серверів після кібератаки, але якщо громадяни вже втратили довіру до уряду через інформаційну війну, то наслідки будуть значно серйознішими та довготривалими.

Таким чином, хоча ці три методи часто використовуються разом, їхній вплив та кінцева мета різняться. Інформаційний тероризм діє через страх, кібератаки — через технічний збій, а інформаційна війна — через зміну суспільних наративів та довготривалу дестабілізацію.

1.3 Основні методи та засоби здійснення інформаційного тероризму

Інформаційний тероризм використовує сучасні інформаційні технології для того, щоб впливати на психологічний стан людей, створюючи атмосферу страху, паніки та невизначеності, що веде до дестабілізації суспільства. Щоб зрозуміти, як це відбувається, уявімо умовний сценарій. Спочатку інформаційні терористи проводять ґрунтовний аналіз цільової аудиторії та інформаційного простору, де вони визначають слабкі місця – канали, через які маса громадськості отримує новини. Потім за допомогою технологій штучного інтелекту та машинного навчання створюють або підробляють відеоматеріали та аудіозаписи. Наприклад, використовуючи технологію deepfake, вони генерують відео, на якому виглядає, ніби високопосадовець оголошує надзвичайну кризу чи приймає рішення, яке може кардинально змінити життя країни. Для підвищення достовірності такі відео ретельно монтуються, використовуються реальні кадри та голосові моделі, що імітують справжніх осіб. Далі, матеріал запускається у цифровий простір. Інформаційні терористи використовують бот-мережі для масового розповсюдження цього контенту в соціальних мережах, таких як Facebook, Twitter, Telegram чи TikTok. Автоматизовані акаунти, часто підробленої природи, миттєво розповсюджують новину, створюючи ілюзію, ніби інформація підтверджується численними джерелами. Паралельно створюються псевдо-новинні ресурси – сайти та блоги, які копіюють вигляд авторитетних медіа, але публікують викривлені факти і доповнюють первинну інформацію новими деталями, які лише посилюють паніку. Уявімо, що в умовній країні, "Новорія"-ї, інформаційні терористи запускають кампанію, спрямовану на підрив довіри до уряду під час політичної кризи. Вони створюють відео, в якому, за допомогою deepfake, показано, що один з високопосадовців оголошує про запровадження воєнного стану та примусовий виїзд з міста через загрозу масових повстань. Цей матеріал швидко поширюється ботами, а потім підкріплюється кількома "незалежними" статтями на фейкових новинних сайтах. Громадськість, не маючи можливості оперативно перевірити достовірність інформації, починає панікувати – люди масово залишають свої домівки, вулиці порожніють, а критика уряду досягає нових висот. Зрештою, цей комплексний

ланцюжок – від аналізу аудиторії до створення фейкового контенту та його масового поширення – має на меті не завдати прямої фізичної шкоди, а підірвати суспільну довіру, створити хаос та посіяти розкол у суспільстві. Цей умовний приклад добре ілюструє, як інформаційний тероризм відрізняється від кібератак та інформаційної війни. У той час як інформаційний тероризм спрямований насамперед на психологічний вплив, використовуючи дезінформацію та маніпулятивний контент для створення паніки, кібератаки зосереджені на технічному руйнуванні інфраструктури (наприклад, злам урядових сайтів або DDoS-атаки), а інформаційна війна являє собою комплексну стратегію, що поєднує і той, і інший підходи для досягнення ширших стратегічних цілей, таких як підрив довіри до державних інституцій та ослаблення державної влади.

Інформаційні терористи постійно вдосконалюють свої методи, експериментуючи з новими технологіями та підходами. Вони аналізують сучасні тренди у розвитку штучного інтелекту, соціальних мереж та мобільних платформ, що дозволяє їм знаходити нові шляхи впливу та адаптувати свої кампанії до змін у цифровому середовищі. Таким чином, боротьба з інформаційним тероризмом вимагає постійного оновлення знань і технологій для своєчасного виявлення та нейтралізації загроз. Інформаційний тероризм постійно еволюціонує, пристосовуючись до нових технологій і змін у цифровому просторі. Окрім описаних раніше методів, варто звернути увагу на кілька додаткових і цікавих аспектів цього явища. Однією з новітніх тенденцій є мікротаргетинг, який використовує великі дані (big data) та алгоритми штучного інтелекту для створення дуже точних психологічних профілів окремих груп населення. Завдяки цьому зловмисники можуть формувати персоналізовані повідомлення, які максимально резонують із страхами, переконаннями та слабкостями конкретних аудиторій. Наприклад, окремі користувачі можуть отримувати інформаційні блоки, адаптовані до їхніх інтересів та поведінкових патернів, що ще більше посилює ефект маніпуляції.Ще один цікавий метод – інформаційне пральництво (information laundering). Це процес, коли неправдива або маніпулятивна інформація спочатку поширюється через низку маловідомих

ресурсів, а потім – через офіційні канали, що призводить до її "легітимізації". Такі техніки дозволяють створити ілюзію достовірності інформації, коли вона доходить до широкої аудиторії, і звичайно ускладнюють процес її перевірки.

Не менш важливим є використання ефемерного контенту – наприклад, короткочасних відео або постів у соціальних мережах, які швидко зникають після публікації (як у Snapchat чи TikTok). Такий контент важко відслідковувати, а його стрімке поширення дозволяє миттєво впливати на громадську думку без можливості детального аналізу з боку незалежних експертів. Також інформаційні терористи активно використовують мемети та елементи поп-культури. Мемети здатні миттєво охопити величезну аудиторію, і навіть якщо їх сприймають з гумором, вони можуть використовуватись для підриву довіри до офіційних структур або для розпалювання соціальних конфліктів. Це, по суті, невелика, але дуже ефективна форма інформаційного впливу, яка може бути частиною ширшої стратегії. До того ж, терористи застосовують координовані кампанії в онлайн-спільнотах та форумах, де за допомогою групових дій (так званий "астротерфінг") створюють видимість широкої підтримки певного наративу. Це включає в себе використання груп тролів, ботів, а також "посадку" дописів у популярних коментарях, що робить інформацію більш помітною та впливовою.

Усе це свідчить про те, що сучасні засоби інформаційного тероризму – це не лише технологічні інструменти, а й глибоко психологічні методи впливу. Терористи активно експериментують з новими технологіями, постійно аналізують тренди в цифровій сфері, щоб знаходити ще більш ефективні способи маніпулювання суспільною свідомістю. Боротьба з такими загрозами вимагає комплексного підходу, що включає як розвиток технологій кібербезпеки, так і підвищення медіаграмотності населення, здатного критично оцінювати отриману інформацію. Сучасні загрози інформаційного тероризму не обмежуються лише технологічними аспектами – вони глибоко впливають на

соціальну тканину суспільства, формуючи нові форми колективної поведінки та сприйняття. Наприклад, соціологічні дослідження показують, що інформаційні кампанії можуть створювати так звані «ефект бульбашки» — коли люди отримують інформацію, що підтверджує їхні вже існуючі переконання, і таким чином стають вразливими до маніпуляцій. Це явище сприяє поляризації суспільства, адже люди все рідше виходять за межі своєї інформаційної комфортної зони, що ускладнює об’єктивну оцінку подій.

Ще один цікавий аспект полягає в тому, як інформаційний тероризм використовує принципи емоційного зараження, що широко досліджуються в соціальній психології. Емоції можуть передаватися від однієї людини до іншої через мережеві платформи, що створює умови для швидкого розповсюдження страху або тривоги. У таких умовах навіть невелика порція неправдивої інформації, наповненої сильними емоційними візуалами або словами, може стати каталізатором масової паніки або навіть соціальних заворушень.

Водночас, сучасні технології дозволяють терористам експериментувати з форматами комунікації. Наприклад, інтеграція елементів віртуальної та доповненої реальності стає новим майданчиком для створення симуляцій кризових ситуацій, що можуть імітувати реальні загрози. Такі симуляції не лише дезінформують, але й створюють нову реальність у свідомості людей, де межа між вигадкою та реальністю стає все більш розмитою.

Цікаво, що в соціологічних колах обговорюють феномен «інформаційного дежавю», коли повторюваність певних наративів у медіапросторі приводить до того, що люди починають сприймати їх як щось природне, невідворотне. Цей ефект, у поєднанні з ретельно продуманими алгоритмами поширення контенту в соціальних мережах, може стати потужним інструментом впливу, адже аудиторія стає менш критичною до повторюваної інформації.

Інший соціологічний аспект стосується «ефекту групової думки», коли в умовах нестачі альтернативних джерел інформації групи людей схильні приймати рішення, що відповідають домінуючим наративам, навіть якщо вони суперечать раціональним висновкам. Це особливо небезпечно під час інформаційних кампаній, спрямованих на дискредитацію урядових інститутів чи посів розколу всередині суспільства.

Таким чином, інформаційний тероризм у сучасному світі – це не лише технічне питання, але й комплексний соціально-психологічний феномен. Він використовує можливості сучасних цифрових технологій для створення штучних емоційних станів, маніпулювання груповою свідомістю та формування спотвореної реальності, що в кінцевому рахунку впливає на стабільність і єдність суспільства. Боротьба з такими загрозами вимагає не лише інвестицій у технології кібербезпеки, але й активної роботи з підвищення критичного мислення та медіаграмотності населення, щоб кожна людина могла стати першою лінією оборони проти маніпулятивних наративів.

1.4 Психологічні механізми впливу та роль соціальних мереж

Психологічні механізми лежать у центрі інформаційного тероризму. Без розуміння людської поведінки, когнітивних спотворень і динаміки масової свідомості неможливо пояснити ефективність сучасних інформаційних атак. Оператори інформаційного впливу діють не лише через технології, а насамперед через психіку людини. Їхня мета — викликати передбачувані реакції, знизити критичність мислення, посилити тривогу, спровокувати розкол у суспільстві. У своїй основі інформаційний тероризм відрізняється від звичайної пропаганди тим, що він не прагне переконати. Його ціль — деморалізувати, виснажити і викликати відчуття безвиході. Саме психологічний вплив стає головним інструментом. Його структура спирається на закономірності сприйняття, соціального навчання, когнітивного дисонансу, групового тиску і колективної емоційної реакції. Одна з базових теорій, що пояснює цей феномен, — соціальне навчання Альберта Бандури [21]. Згідно з нею, люди вчаться через спостереження. Якщо індивід бачить, що певна модель поведінки отримує винагороду, він її повторює. У цифровому середовищі це означає, що емоційні реакції, демонстративна агресія або панічні пости стають моделями поведінки, які масово копіюються. Алгоритми соціальних мереж підсилюють цей процес, адже винагороджують саме контент, що викликає реакцію. Коли користувач бачить, що страх або обурення приносять увагу, він несвідомо продовжує продукувати подібний контент. Інша важлива теорія — когнітивний дисонанс Леона Фестінгера [22]. Люди прагнуть уникати внутрішнього конфлікту між переконаннями і реальністю. Коли інформація суперечить їхнім переконанням, вони відкидають її або шукають пояснення, яке зберігає внутрішню узгодженість. Інформаційний тероризм експлуатує цей механізм. Атакуюча сторона створює наратив, що підкріплює існуючі страхи або упередження, і одночасно виставляє протилежну точку зору як брехню або загрозу. Людина, опинившись у когнітивному дисонансі, обирає емоційно комфортну позицію — і таким чином поглиблює свою інформаційну залежність. Психологічний тиск базується і на ефекті “спіралі мовчання”, який описала Елізабет Ноель-Нойман [23]. Люди схильні мовчати, якщо їхня думка не збігається з домінуючою. У соціальних мережах цей ефект підсилюється кількістю лайків і репостів.

Інформаційні кампанії створюють ілюзію консенсусу: певна позиція здається більш поширеною, ніж вона є насправді. Ті, хто думають інакше, відчувають ізоляцію і перестають висловлюватися. У підсумку формується фальшива одностайність, що підживлює страх і конформізм. Когнітивні спотворення — ще одна ключова площина психологічного впливу. Даніель Канеман і Амос Тверскі довели, що люди не завжди мислять раціонально [24]. Вони приймають рішення, спираючись на евристики — ментальні скорочення, які дозволяють швидко оцінювати ситуації, але часто ведуть до помилок. Наприклад, ефект доступності змушує нас переоцінювати значення подій, про які ми чуємо частіше. Інформаційні кампанії використовують це, повторюючи певні меседжі, щоб створити ілюзію масовості проблеми. Так само ефект фреймінгу впливає на те, як ми оцінюємо факти: одна й та сама подія може сприйматися позитивно або катастрофічно залежно від того, як вона представлена. Емоційний вплив має вирішальне значення. Страх і гнів активують симпатичну нервову систему, що знижує здатність до аналітичного мислення. Люди в стані тривоги шукають прості пояснення і винних. Інформаційні атаки спеціально викликають такий стан — через фейкові новини, шокуючі візуальні зображення або повторювані повідомлення про небезпеку. Коли людина живе у середовищі постійної тривоги, її когнітивні ресурси виснажуються, і вона стає більш піддатливою до маніпуляцій. Соціальні мережі посилюють усі ці ефекти. Вони створені для утримання уваги, а не для пошуку істини. Алгоритми підбирають контент, який викликає емоційну реакцію. Так формується феномен “емоційного циклу підсилення” — чим більше користувач реагує, тим більше платформа показує схожий контент. Це створює замкнене коло, у якому страх і гнів підживлюють самі себе. Оператори інформаційного тероризму використовують це системно. У 2014–2025 роках інформаційні атаки проти України показали, що соціальні мережі можуть стати інструментом масової дестабілізації. Сотні тисяч ботів поширювали панічні повідомлення, маніпулювали темами мобілізації, економічної кризи і “зради” [25]. Емоційна хвиля таких кампаній була настільки потужною, що навіть офіційні спростування сприймались як підтвердження змови. Мікротаргетинг відкрив нову епоху персоналізованого впливу. Замість

масових меседжів оператори отримали змогу адресувати повідомлення конкретним людям на основі їхніх інтересів, політичних симпатій, стану здоров'я чи страхів. Скандал із Cambridge Analytica показав, як мільйони профілів Facebook були використані для створення психологічних портретів виборців [26]. На основі цих даних формувались повідомлення, які стимулювали страх або обурення, знижуючи участь опонентів у виборах або посилюючи емоційне згуртування прихильників. Психологічні механізми впливу діють також через ефект групової належності. Люди прагнуть бути частиною більшості. Коли вони бачать, що "всі так думають", вони змінюють свою думку. У цифровому середовищі цей ефект посилюється штучним "хором" ботів або підставних акаунтів. Навіть кілька сотень синхронних коментарів здатні створити ілюзію масової підтримки. Цей принцип активно використовувався під час інформаційних кампаній у Німеччині, Польщі та США, коли політичні дискусії у Twitter або Facebook заповнювались повторюваними фразами, що виглядали як народна реакція, але насправді були координованою дією [27]. Окреме місце займає ефект "страху пропустити" (FOMO), який експлуатує постійний потік інформації. Люди бояться залишитись осторонь подій, тому часто діляться неперевіреними повідомленнями. У кризові періоди — наприклад, під час пандемії COVID-19 або під час початку війни — цей ефект посилюється. Користувачі хочуть "бути в курсі", тому масово поширюють повідомлення, не перевіряючи їхнє джерело. Для операторів інформаційного терору це ідеальний інструмент — достатньо запустити кілька панічних тез, і натовп зробить усе інше. Психологічний аспект інформаційних кампаній пов'язаний і з поняттям соціального доказу. Люди оцінюють істинність інформації за поведінкою інших. Якщо певна новина має багато коментарів або реакцій, вона здається достовірною. Оператори створюють фальшивий соціальний доказ, використовуючи ботів, накручені перегляди або "фабрики лайків". Так формується інформаційне середовище, де кількість підмінює якість, а популярність — істину. Не менш важливим є психологічне зараження. У великих онлайн-спільнотах емоції передаються з дивовижною швидкістю. Один панічний допис може за хвилини перетворитися на хвилю страху. Експерименти

Facebook у 2014 році підтвердили, що зміна емоційного тону стрічки новин впливає на настрій користувачів [28]. Інформаційний тероризм використовує це як зброю, формуючи “вірусні емоції”. Розвиток візуальної культури посилив роль образів. Людина реагує на зображення швидше, ніж на текст. Фото руйнування, поранених, хаосу викликають негайний страх. Навіть якщо контент підроблений, емоційний ефект залишається. Deepfake-технології зробили це ще небезпечнішим. У 2022–2023 роках кілька deepfake-відео із “заявою” українського президента про капітуляцію поширювались мережею за лічені години [29]. Їх миттєво спростували, але психологічний шок уже відбувся — частина населення на короткий час відчула невпевненість і тривогу. Соціальні мережі також створили нову форму колективного страху — “цифрову паніку”. Коли тисячі людей одночасно реагують на неправдиве повідомлення, воно набуває вигляду правди. Алгоритми не здатні швидко відрізнити фейк від реальності. У таких випадках навіть короткий спалах паніки може призвести до економічних втрат або реальних криз — наприклад, коли масово знімають гроші з банкоматів через чутки про “колапс банківської системи”. Психологічна динаміка групової поведінки посилює ефект інформаційного терору. Люди мислять не лише індивідуально, а й колективно. У великих спільнотах формується те, що соціальні психологи називають “груповим мисленням”. Цей феномен описав Ірвінг Дженіс [30]. Коли група орієнтована на підтримання єдності, критичне мислення знижується. Незгода сприймається як загроза цілісності. В умовах інформаційної війни це призводить до того, що всередині поляризованих спільнот будь-який інакодумець швидко маркується як “ворог” або “зрадник”. У результаті група стає керованою зовнішніми сигналами, а її внутрішня логіка — передбачуваною. Такі механізми широко застосовуються у російських і китайських інформаційних операціях. Вони спрямовані на створення двох паралельних спільнот — лояльної та ворожої. Кожна з них отримує власний набір меседжів. Лояльним нав’язується наратив стабільності, порядку і “зовнішньої загрози”. Опонентам підкидають меседжі хаосу, зневіри, недовіри до лідерів. Обидві групи існують у дзеркальному протистоянні, але спільний результат — дестабілізація середовища та руйнування соціальної

єдності. У Польщі і Німеччині аналогічні кампанії фіксував Центр передового досвіду НАТО StratCom. Атаки спрямовувались на теми міграції, вакцинації, гендерної рівності, національної ідентичності. Мета була не переконати, а посварити. Психологічний ефект полягає у виснаженні: люди постійно перебувають у стані конфлікту, що знижує довіру до держави і медіа. Американський досвід також демонструє, що соціальні платформи можуть стати каталізатором колективної агресії. Події 6 січня 2021 року у Вашингтоні показали, як онлайн-дезінформація перетворюється на фізичну дію. Соціальні мережі протягом тижнів підживлювали відчуття обману і гніву серед певних груп. Механізм самопідсилення зробив радикалізацію лавиноподібною. Люди не лише вірили у фейкові повідомлення, вони відчували обов'язок діяти. Це класичний приклад того, як цифрова психологічна інженерія перетворює емоцію на поведінку. Український контекст має власні особливості. З 2014 року країна перебуває під постійним інформаційно-психологічним тиском. Атаки спрямовані на емоції — страх, провину, безнадію. Російські інформаційні операції активно використовують тему втрат, соціальної нерівності, внутрішньої корупції. Ціль — підірвати віру в державу та створити відчуття хаосу. Дослідження Інституту масової інформації показали, що 72% емоційно забарвлених фейків у 2022–2023 роках стосувалися саме питань безпеки і стабільності. Сучасні мережеві алгоритми створюють нову форму психологічної пастки. Вони підлаштовують контент під реакції користувача, формуючи ефект "підкріплення". Якщо людина читає новини про загрозу, система показує їй ще більше подібного контенту. Так формується хронічна тривога, яку користувач сприймає як об'єктивну реальність. Психологи називають це "цифровим резонансом страху". У довготривалій перспективі він призводить до зниження довіри до всіх джерел, навіть достовірних. Інформаційний тероризм використовує візуальне моделювання реальності. Замість логічних аргументів застосовуються образи, що вкорінюються у підсвідомості. Фотографії, символи, кольори, навіть шрифти створюють підсвідомі асоціації. Візуальні патерни повторюються у різних кампаніях, що формує стійкий емоційний зв'язок. Саме тому державні програми протидії дезінформації у Німеччині й Естонії

використовують психологічні лабораторії для тестування візуального впливу. Окремий пласт — моральна маніпуляція. Вона спирається на систему цінностей аудиторії. Наприклад, під час пандемії COVID-19 маніпулятори часто посилалися на ідеї “свободи” і “захисту дітей”. Такий фреймінг переводив дискусію у моральну площину. Люди, які відмовлялися від вакцинації, відчували себе героями, а не порушниками. Психологічна сила цього методу полягає у тому, що він створює позитивну ідентичність навколо антинаукових наративів [31]. Поведінкові реакції в інтернеті дедалі більше піддаються автоматизованому аналізу. Алгоритми машинного навчання прогнозують, які повідомлення викличуть страх або гнів. Це дозволяє будувати динамічні кампанії, які змінюються у режимі реального часу. Наприклад, якщо аудиторія не реагує на тему війни, їй подають тему економічної кризи. Якщо байдужість зростає, активізують шок-контент. У цьому сенсі інформаційний тероризм стає кіберпсихологічним конструктом — симбіозом технологій і маніпуляцій свідомістю. У Китаї та Росії ця модель отримала інституційне закріплення. Створені цілі центри психологічних операцій, де працюють фахівці з лінгвістики, соціології, IT та нейронаук. Їх завдання — розробляти методи формування довготривалих установок. У таких структурах тестують, як поєднання страху і гордості створює ефект “м’якої покори”. Люди не відчувають примусу, але діють у потрібному напрямі. Водночас у демократичних країнах почали формуватись протидієві стратегії. У Німеччині запроваджено програму “Digitaler Zivilgesellschaft”, що поєднує освіту, фактчекінг і психологічну підтримку медіаспоживачів. У Польщі діє “Centrum Przeciwdziałania Dezinformacji”, яке вивчає, як інформаційний тиск впливає на колективну довіру. В Україні після 2021 року створено Центр протидії дезінформації при РНБО, що координує дії державних і громадських структур у сфері інформаційної безпеки. Психологічні наслідки інформаційного терору вимагають міждисциплінарного підходу. Йдеться не лише про безпеку, а й про ментальне здоров’я населення. Постійний інформаційний стрес призводить до підвищеної тривожності, соціальної ізоляції, депресивних станів. Звіт ВООЗ за 2023 рік вказує, що 28% користувачів соцмереж у періоди кризових інформаційних кампаній відчували

симптоми постійного стресу [32]. Таким чином, інформаційний тероризм має не лише політичний, а й психосоматичний вимір. Важливим є аспект психологічного захисту. Люди, які мають навички критичного мислення, менше піддаються маніпуляціям. Тому медіаграмотність — не просто інструмент освіти, а стратегічна зброя оборони. У Фінляндії з 2015 року уроки з аналізу інформації введено до шкільної програми. Дослідження показують, що це знизило рівень довіри до фейків на 30% серед молоді. Україна також поступово впроваджує подібні курси, зокрема через ініціативу “Фільтр” Міністерства культури та інформаційної політики. Однак освіта має діяти не лише на рівні знань, а й емоцій. Люди часто вірять у дезінформацію не тому, що не знають фактів, а тому, що шукають психологічну підтримку. Тому стратегія протидії має включати емпатійні комунікації. Пояснення має бути людяним, спокійним, не осудливим. Психологи вважають, що довіра формується не через аргументи, а через стиль подачі. Алгоритмічний контроль і модерація контенту залишаються складними питаннями. Повне блокування може сприйматися як цензура, що підсилює антидержавні настрої. Ефективніша стратегія — прозоре пояснення рішень. Коли користувач розуміє, чому контент позначено як фейковий, він рідше сприймає це як акт контролю. Європейський Союз у 2022 році ухвалив Кодекс практик з протидії дезінформації, який зобов’язує платформи публікувати звіти про алгоритмічну модерацію. Водночас соціальні мережі мають значний потенціал для протидії інформаційному терору. Вони можуть стати інструментом швидкого оповіщення, платформою для координації допомоги, каналом достовірних новин. Все залежить від стратегії. Наприклад, у Польщі під час кризи з біженцями 2022 року волонтерські групи у Facebook стали основним джерелом допомоги. Це доводить, що психологічні механізми довіри і солідарності можуть бути використані у позитивному ключі. Етична проблема полягає у межах психологічного впливу з боку держави. Якщо держава починає застосовувати ті самі методи, що й терористи, вона ризикує втратити моральну перевагу. Тому сучасна стратегія інформаційної безпеки повинна ґрунтуватися на принципах відкритості, поваги до гідності і пропорційності дій . Психологічний захист має бути спрямований не на маніпуляцію, а на зміцнення

автономії громадян. Сучасні технології штучного інтелекту відкривають і нові можливості, і нові ризики. AI може автоматично виявляти маніпулятивні патерни, відстежувати дезінформаційні мережі, прогнозувати емоційні реакції. Але він може бути використаний і для створення суперреалістичних фейків або маніпулятивних наративів. Тому розвиток етичних стандартів AI стає частиною інформаційної безпеки. У контексті міжнародної політики зростає значення психологічної стійкості суспільства. НАТО у своїх доктринах 2023 року визнає інформаційний тероризм окремою загрозою, поряд із кібер- і біологічними ризиками. Альянс підкреслює, що колективна оборона має включати психологічний компонент — зміцнення довіри, комунікацію правди і розвиток критичного мислення. В Україні також формується нова культура інформаційної гігієни. Молодь активніше користується фактчекінговими ресурсами, а державні установи створюють відкриті сторінки для спростувань. Проте психологічна війна триває. Інформаційний тероризм адаптується до нових форматів — коротких відео, мемів, гейміфікованих кампаній. Тому протидія має бути постійною і динамічною. Підсумовуючи, можна сказати, що психологічні механізми інформаційного тероризму охоплюють широкий спектр — від емоцій і упереджень до групової ідентичності й алгоритмічних рекомендацій. Соціальні мережі виступають не лише інструментом, а середовищем, у якому ці процеси розгортаються. Протидія вимагає системності: освіта, комунікація, міжнародна координація, етичне регулювання і технологічні рішення мають працювати разом. Лише тоді можливо зменшити вплив інформаційного терору на свідомість суспільства.

РОЗДІЛ ІІ

Інформаційний тероризм у міжнародному контексті

2.1 Роль державних та недержавних акторів у здійсненні інформаційного тероризму

Роль державних та недержавних акторів у здійсненні інформаційного тероризму є багатогранною і комплексною, адже обидві групи використовують свої ресурси для досягнення подібних цілей, проте методи, масштаби та мотивації їхніх дій можуть істотно відрізнятися. З одного боку, державні актори, зазвичай, діють як частина офіційної політики зовнішньої чи внутрішньої безпеки. Держави, які прагнуть вплинути на політичний клімат або послабити суперечливих опонентів, можуть використовувати державні ресурси для організації інформаційних кампаній, що мають на меті дискредитацію опонентів, підрив довіри до інституцій чи розпалювання соціальних конфліктів. Наприклад, державні агентства або спеціально створені служби пропаганди можуть створювати офіційно схожий контент, який потім масово поширюється через державні канали, такі як телебачення, радіо, офіційні веб-сайти та профільні сторінки у соціальних мережах. Вони можуть організовувати координацію роботи із субпідрядниками – як внутрішніми експертами, так і агентами, працюючими за кордоном, для того щоб створити єдиний наратив, що відповідає державним інтересам. Також державні структури можуть використовувати свої дипломатичні та економічні важелі, щоб впливати на міжнародну публічну думку, проводячи інформаційні операції, які часто маскуються під аналітичні чи культурні ініціативи. У деяких випадках державні актори підтримують або навіть фінансують недержавні організації, які мають на меті поширення їхньої ідеології, тим самим забезпечуючи легітимність і більший охоплення аудиторії. З іншого боку, недержавні актори охоплюють різноманітні групи – від терористичних організацій і екстремістських угруповань до хактивістів і приватних медіа, що працюють за принципом відкритої інформаційної боротьби.

Ці актори часто мають більш гнучку і адаптивну структуру, що дозволяє їм швидко реагувати на події та експериментувати з новими технологічними засобами. Наприклад, терористичні групи можуть створювати вірусні кампанії в соціальних мережах, використовуючи бот-мережі та фейкові акаунти для поширення пропаганди, дезінформації і спотворених новин. Вони використовують технології deepfake для підробки відеозаписів, що виглядають переконливо, і таким чином намагаються вплинути на психологічний стан аудиторії, посіяти страх і хаос. Такі недержавні структури часто діють автономно або в рамках мережі партнерських організацій, які можуть бути пов'язані з іноземними державами, але при цьому офіційно не представляють жодну урядову структуру. Їх діяльність часто фокусується на локальних конфліктах або протистоянні з певними політичними групами, і вони можуть працювати за принципом "низового" впливу, де навіть невелика кількість активних осіб у соціальних мережах може призвести до масштабного ефекту через механізми "ефекту бульбашки" та "групової думки". Окрім цього, недержавні актори можуть використовувати так звані "інформаційні фабрики" — незалежні або приховані медіа-ресурси, які виглядають як традиційні новинні портали, але насправді розповсюджують пропаганду, спрямовану на дискредитацію певних політичних чи соціальних сил. Часто це супроводжується використанням сучасних технологій для маніпуляції пошуковими системами, що дозволяє створити ілюзію широкої підтримки певного наративу.

Умовний приклад: припустимо, що в країні А уряд вважає, що його опоненти намагаються підривати національну безпеку. Державні служби, використовуючи свої ресурси, створюють офіційний наратив, який висвітлюється через державне телебачення, радіо та інтернет-портали. Одночасно, недержавні групи, що підтримують уряд, запускають у соціальних мережах кампанію із створення фейкових відео та статей, які підтверджують офіційну версію подій, а також публікують документи, які, за їх словами, доводять небезпеку опонентів. При цьому незалежні ресурси, під впливом алгоритмів і маніпуляцій, починають поширювати ці наративи, створюючи ефект "самопідтримки" інформації. Внаслідок цього населення отримує єдиний інформаційний потік, який

маніпулює його сприйняттям, формує страх перед опонентами і закріплює владу уряду. Таким чином, державні та недержавні актори, хоча й діють за різними сценаріями та з різними мотиваціями, об'єднують свої зусилля для досягнення спільної мети – впливу на суспільну думку і створення стабільного, хоча й штучного, інформаційного середовища, що сприяє реалізації політичних або ідеологічних завдань. Цей приклад ілюструє, як у сучасному світі межі між офіційними та неофіційними каналами інформації стираються, а використання сучасних технологій дає змогу досягти високої ефективності як з державної, так і з недержавної сторони в реалізації інформаційного тероризму. Водночас це створює серйозні виклики для демократичних процесів, оскільки масова дезінформація та маніпуляції можуть кардинально змінити політичну картину і спричинити непередбачувані наслідки для суспільства. Окрім вже згаданих аспектів, варто звернути увагу на деякі менш очевидні, але надзвичайно цікаві деталі щодо ролі державних і недержавних акторів в інформаційному тероризмі, які все більше набувають значення в умовах стрімкого розвитку цифрових технологій. Однією з новітніх тенденцій є використання шифрованих месенджерів та закритих чатів як платформ для координації інформаційних кампаній. Державні структури можуть створювати власні спеціалізовані групи, які через зашифровані канали обмінюються даними, координують агресивні пропагандистські операції та взаємодіють із партнерами за кордоном. З іншого боку, недержавні організації, неодноразово зіштовхуючись із цензурою або спостереженням, використовують ті ж технології, що дозволяє їм залишатися поза зоною контролю урядових структур і розгортати більш гнучкі та адаптивні стратегії впливу. Ще один цікавий елемент – це інформаційні експерименти, які проводять як державні, так і недержавні актори, спрямовані на тестування реакції громадськості на певні наративи. За допомогою аналізу соціальних мереж, даних Big Data та алгоритмів штучного інтелекту вони створюють міні-кампанії, що мають на меті виміряти, як швидко і широко поширюється конкретний меседж, який потім або підсилюється, або корегується для досягнення максимального впливу. Такий підхід дозволяє "налаштовувати" наступні операції в режимі реального часу та оптимізувати інформаційні тактики, що робить інформаційний

тероризм дедалі більш адаптивним. Також важливо відзначити роль діаспори та іноземних громад. Державні структури, що прагнуть впливати на політичні процеси у певних регіонах, активно використовують свої дипломатичні та культурні відділи для залучення емігрантів. Ці групи, іноді навіть без прямого офіційного підкріплення, стають каналами для поширення альтернативних наративів через власні ЗМІ, форуми чи блогерські мережі, тим самим посилюючи загальний інформаційний вплив. Ще одна цікава риса – експерименти з новими форматами контенту, зокрема інтеграція елементів віртуальної та доповненої реальності. Деякі недержавні актори створюють VR-симуляції кризових ситуацій, які дозволяють користувачам відчути, ніби вони знаходяться у центрі подій. Це не тільки підсилює емоційний відгук, а й сприяє поширенню новин серед молодшої аудиторії, яка звикла до високотехнологічного контенту. Інший аспект, який варто згадати, – це співпраця з технологічними стартапами. Як державні, так і недержавні актори дедалі частіше залучають фахівців з галузі блокчейну для створення децентралізованих платформ поширення інформації, що ускладнює можливості контролю з боку традиційних силових структур. Такі платформи дозволяють зберігати дані у незмінному вигляді, що, з одного боку, може бути використано для документування подій, а з іншого – для того, щоб "завірити" певні наративи, навіть якщо вони є маніпулятивними. На завершення, цікаво відзначити, що процес створення та реалізації інформаційного тероризму часто супроводжується глибоким аналізом поведінки людської психології. Дослідники із соціології та психології постійно вивчають, як певні символи, кольори, мови та навіть звукові ефекти впливають на масову поведінку. Державні та недержавні актори активно застосовують ці знання для розробки стратегій, що спонукають до формування емоційних відповідей у аудиторії – від паніки до агресивної мобілізації. Таким чином, інформаційний тероризм перетворюється не лише на технологічний, але й на глибоко соціально-психологічний феномен, що змінює спосіб, яким суспільство сприймає реальність і приймає рішення.

2.2 Відомі випадки інформаційного тероризму у світовій практиці (приклади атак, пропагандистських кампаній, маніпуляцій громадською думкою)

Існує низка випадків, коли інформаційний тероризм використовувався для досягнення політичних, ідеологічних чи військових цілей, і ці приклади ілюструють, наскільки різноманітними можуть бути методи впливу та наслідки таких операцій. Одним із найбільш відомих прикладів є кампанії, які

проводилися протягом останніх років Росією проти України. Починаючи з анексії Криму в 2014 році, а згодом і під час війни на Донбасі, російські інформаційні операції активно використовували дезінформацію, маніпулятивні відео, фейкові новини та бот-мережі для того, щоб дискредитувати український уряд, підірвати довіру до його дій і створити враження, ніби українська влада є нестабільною. Наприклад, численні фальшиві новини та відеоматеріали поширювалися в соціальних мережах, які демонстрували нібито насильницьке придушення мирних протестів або "секретні" заяви українських політиків, що викликало паніку та розкол у суспільстві. Такі операції використовували сучасні технології deepfake, що дозволяли створювати відео, де відомі особи здавалися замішаними у злочинних діях, хоча насправді такі кадри були сфабриковані.

Ще одним яскравим прикладом є інформаційна діяльність Ісламської держави (ІД, ISIS). Ця організація, розуміючи силу цифрової пропаганди, активно використовувала соціальні мережі та спеціалізовані платформи для поширення своїх наративів. За допомогою професійно зрежисованих відеороликів, які поєднували жорстокі сцени з кришталево чистими зображеннями релігійних символів, ІД створювала образи безжального й могутнього ворога, що надихало нових рекрутерів у всьому світі. Ці відео не тільки залякували потенційних супротивників, а й розпалювали емоції вірних, сприяючи поширенню радикальної ідеології. Вони використовували сучасні засоби монтажу, спецефекти та навіть музичне супроводження, яке допомагало занурити аудиторію у створений наратив.

Ще один випадок стосується інформаційних операцій, пов’язаних із політичними виборами у Західних країнах. Наприклад, під час президентських виборів у США в 2016 році було зафіксовано численні спроби розповсюдження фейкових новин через соціальні мережі, що створювало враження, ніби існує широкий розкол у суспільстві, а також підривало довіру до традиційних медіа. Хоча це не завжди класифікується виключно як "тероризм", методи, що використовувалися – масове розповсюдження неправдивої інформації, маніпуляції зображеннями, координація бот-мереж – чітко відповідають

поняттю інформаційного тероризму, оскільки їх головною метою було створення атмосфери невизначеності, страху і підриву громадського порядку.

Також варто зазначити випадки, коли недержавні актори, наприклад, радикальні політичні групи або екстремістські організації, використовують інформаційний тероризм для впливу на своїх прихильників. Вони створюють спеціальні онлайн-спільноти, де за допомогою емоційно зарядженого контенту, мемів та вірусних відео формують альтернативну реальність, в якій їхній наратив здається єдиною правдою. Ці групи часто організовують онлайн-дискусії, використовують так званий "астротерфінг" (штучне створення видимості масової підтримки) і навіть проводять тренінги з медіаграмотності серед своїх учасників, щоб підсилити внутрішню єдність і мобілізувати їх на акції проти "внутрішніх ворогів". Ці приклади показують, що інформаційний тероризм – це явище, яке активно інтегрується у сучасну політичну та соціальну дійсність. Він не обмежується лише простим поширенням фейкових новин, а використовує комплекс технологічних, психологічних та організаційних методів для досягнення стратегічних цілей.[33] Сучасні терористичні кампанії з інформаційного характеру розвиваються практично в реальному часі, адаптуючись до змін у цифровому середовищі, що робить їх особливо небезпечними для демократичних суспільств, здатних втратити контроль над інформаційним простором. Цей виклик потребує не лише технічних рішень, але й активної роботи з підвищення критичного мислення та медіаграмотності серед громадян, адже саме знання та здатність розпізнавати маніпулятивні наративи можуть стати першою лінією оборони проти інформаційного тероризму. Один із відомих прикладів інформаційного тероризму – це кампанія, що розгорнулася під час президентських виборів у США в 2016 році. Державні та недержавні структури, пов'язані з Росією, систематично поширювали фейкові новини через соціальні мережі, створювали бот-акаунти та координували роботу тролів, щоб вплинути на громадську думку виборців. Така кампанія не обмежувалася лише окремими фейковими повідомленнями; вона включала масштабну дезінформацію, що мала на меті створити розкол у суспільстві, підривати довіру до традиційних медіа та стимулювати суперечності серед політичних сил. Цей випадок добре ілюструє,

як через контрольований потік неправдивої інформації можна змінити сприйняття реальності мільйонів людей, вплинути на політичний клімат і навіть результат виборів.

Ще яскравим прикладом є пропагандистські кампанії, які проводили терористичні організації, такі як Ісламська держава (ІД). ІД активно використовувала соціальні мережі, онлайн-платформи та відеоконтент для розповсюдження своєї ідеології. Вони створювали професійно зрежисовані відеоролики, що поєднували жорстокі сцени, релігійні символи та меседжі, що викликали сильні емоції. Ці матеріали не лише залякували потенційних супротивників, але й приваблювали нових рекрутерів з усього світу, особливо серед молодих людей, які активно користувалися цифровими платформами. Завдяки цьому ІД вдалося сформувати мережу прихильників, котра не обмежувалася географічними кордонами, що стало однією з причин швидкого поширення їхніх наративів. Інший приклад – це інформаційні операції, які організовували недержавні актори в Європі, спрямовані на створення альтернативних наративів під час політичних криз або виборчих кампаній. Такі операції часто включають розробку фейкових новинних сайтів, блогів та форумів, де публікуються викривлені або повністю вигадані історії. Завдяки сучасним алгоритмам поширення інформації ці наративи швидко набирають популярності, особливо якщо їх підтримують бот-мережі та тролі, що створюють ілюзію широкої підтримки. Результатом є формування хибних уявлень серед населення, посилення політичних конфліктів і підрив довіри до традиційних джерел інформації.

Сучасні інформаційні атаки також можуть включати використання технологій deepfake, які дозволяють створювати надзвичайно реалістичні відеозаписи. За допомогою цієї технології зловмисники можуть підробляти виступи політиків чи публічних діячів, демонструючи їх у ситуаціях, яких насправді не було. Такі відеоматеріали швидко поширюються через соціальні мережі, викликаючи

паніку, розкол у суспільстві або навіть мобілізуючи певні групи населення на протести чи інші форми активності. Цей метод є надзвичайно небезпечним, адже сприймається як доказ реальних подій, що значно ускладнює боротьбу з дезінформацією.[34]

Ці приклади свідчать про те, що інформаційний тероризм не обмежується лише поширенням фейкових новин. Він включає комплексну стратегію, яка використовує сучасні цифрові технології, психологічні методи впливу та високоефективні алгоритми поширення інформації. Державні та недержавні актори активно експериментують з новими форматами контенту, такими як ефемерні повідомлення, VR-симуляції кризових ситуацій, а також інтегровані кампанії в закритих месенджерах, що дозволяє їм постійно адаптувати свої стратегії до змін у цифровому середовищі. Окрім США, Росії та ісламських держав, багато інших країн та політичних рухів активно використовують пропаганду як інструмент впливу. Сучасні технології дозволяють створювати та поширювати інформаційні кампанії, які впливають не лише на внутрішню політику, а й на міжнародну арену. Давайте розглянемо кілька цікавих випадків з різних куточків світу. Китай має одну з найсильніших інформаційних систем контролю та пропаганди у світі. "Великий Китайський Фаєрвол" не тільки блокує небажані сайти (Google, Facebook, Twitter), а й формує власний інформаційний простір, де домінують китайські наративи. Але китайська пропаганда працює не лише всередині країни, а й на міжнародній арені. Одним із найяскравіших прикладів стала кампанія, пов’язана з пандемією COVID-19. Коли вірус почав поширюватися, китайські державні ЗМІ та дипломати (так звані "вовки-воїни") почали активно просувати ідею, що COVID-19 не має китайського походження, а, можливо, був завезений із США чи Європи. Водночас Китай розгорнув інформаційну кампанію "маскової дипломатії", демонструючи свою допомогу іншим країнам і представляючи себе як глобального лідера в боротьбі з пандемією. Інший приклад – ситуація з уйгурами. Китай активно використовує міжнародні соціальні мережі та дипломатію для спростування звинувачень у переслідуванні мусульманського населення Сіньцзяну. Через мережі китайських

акаунтів, тролів та блогерів Пекін намагається створити альтернативний наратив: нібито уйгури проходять "освітні курси", а не перебувають у таборах примусової праці.

В Індії пропаганда відіграє важливу роль у політичній боротьбі, особливо з приходом до влади націоналістичної партії Бхаратія Джаната (BJP) на чолі з Нарендрою Моді. Соціальні мережі стали головним інструментом інформаційного впливу, і партія Моді використовує їх на повну потужність. Одним із найцікавіших інструментів є величезні фабрики тролів, які систематично поширюють пропагандистські меседжі, дискредитують опозицію та просувають ідеї хінду-націоналізму. Наприклад, під час виборів 2019 року BJP використовувала WhatsApp-ботів для надсилання мільйонів повідомлень з політичними гаслами, фейковими новинами про опонентів та закликами голосувати за правлячу партію. Окрім того, в Індії ведеться активна дезінформаційна кампанія проти мусульманської меншини. Під час пандемії COVID-19 пропагандистські ресурси поширювали фейки про те, що мусульмани спеціально розповсюджують вірус. Це спричинило зростання антиісламських настроїв і навіть насильство[35].

Бразилія стала полем битви інформаційних кампаній у часи президентства Жаїра Болсонару. Його прихильники запустили потужну хвилю пропаганди через соціальні мережі, щоб мобілізувати виборців та дискредитувати опонентів. Одним із найцікавіших методів стало використання WhatsApp-кампаній. Бразильські фабрики тролів масово розсилали політичні повідомлення з фейками, зокрема про те, що якщо опозиція переможе, країну накриє хвиля соціалізму, заберуть приватну власність і знищать традиційні цінності.

Хоча Європейський Союз часто виступає як бастіон боротьби з дезінформацією, навіть тут не обходиться без інформаційних кампаній. Одним із найяскравіших прикладів стало референдум щодо Брекзиту у 2016 році. Прихильники виходу Великої Британії з ЄС розгорнули масштабну пропагандистську кампанію, використовуючи фейки та маніпуляції. Найвідоміший випадок – це обіцянка, що після Брекзиту Британія заощаджуватиме 350 мільйонів фунтів щотижня та

направить ці кошти на медицину. Ця інформація була розміщена навіть на автобусах, хоча згодом її спростували. Ще один приклад – міграційна криза 2015 року. В деяких країнах, зокрема в Угорщині, уряд Віктора Орбана розгорнув кампанію проти біженців, використовуючи фальсифіковані статистичні дані та створюючи образ "загрози для європейської ідентичності". Такі меседжі активно транслювалися державними ЗМІ, що сприяло зростанню ксенофобії та підтримці ультраправих партій.

2.3 Наслідки інформаційного тероризму для міжнародної безпеки

Інформаційний тероризм став серйозною загрозою для міжнародної безпеки, адже його наслідки виходять далеко за межі цифрового простору. Дезінформація, маніпуляція свідомістю та створення штучного хаосу можуть призводити до масштабних політичних, економічних та військових конфліктів. Давайте розглянемо, як саме інформаційний тероризм впливає на світову безпеку та які його найсерйозніші наслідки. Один із головних наслідків інформаційного тероризму – це руйнування довіри до державних інституцій та підрив політичної

стабільності. Коли населення країни починає масово вірити у фейкові новини, теорії змови або маніпулятивні наративи, це може призвести до соціальних заворушень, протестів або навіть революцій. Наприклад, під час виборів в різних країнах часто запускаються дезінформаційні кампанії, які поширюють недовіру до результатів голосування. Це може викликати масові протести, як це сталося у США після виборів 2020 року, коли прихильники Дональда Трампа, натхненні теоріями змови про "вкрадені вибори", штурмували Капітолій. Інший приклад – вплив інформаційного тероризму на країни, що перебувають у стані політичної нестабільності. У державах, де уряди не мають міцної підтримки населення, інформаційні атаки можуть спровокувати повалення влади та хаос, створюючи передумови для громадянської війни або зовнішнього втручання. Інформаційний тероризм став ключовим інструментом ведення гібридних воєн, коли держави або недержавні актори намагаються послабити супротивника без прямого військового зіткнення. Через маніпуляції інформацією можна спровокувати міжетнічні, релігійні або міждержавні конфлікти.

Один із яскравих прикладів – інформаційні атаки під час війни в Сирії. Різні сторони конфлікту – від уряду Асада до ісламістських угруповань – використовували фейкові новини, пропаганду та маніпуляції, щоб створити відповідний образ війни для різних цільових аудиторій. Такі кампанії не лише виправдовували насильство, а й сприяли радикалізації населення. Інформаційний тероризм також використовується для розпалювання міжнародних конфліктів. Наприклад, під час конфлікту між Індією та Пакистаном у 2019 році в соціальних мережах масово поширювалися фейкові відео, які підсилювали ненависть між народами і могли стати тригером для масштабнішої війни. Ще одним серйозним наслідком інформаційного тероризму є руйнування довіри до традиційних медіа. Якщо люди постійно стикаються з фейковими новинами, вони починають сумніватися навіть у правдивих повідомленнях. Це створює інформаційний хаос, де будь-яка точка зору може бути представлена як "альтернативна правда".

Яскравий приклад – пандемія COVID-19. Через величезну кількість конспірологічних теорій про "чіпування", "біологічну зброю" та "зміну ДНК" значна частина населення відмовилася вакцинуватися, що призвело до мільйонів смертей по всьому світу. Маніпуляції навколо пандемії також загострили політичні конфлікти, адже різні держави почали звинувачувати одна одну у створенні та розповсюдженні вірусу. Втрата довіри до медіа та наукових джерел також робить суспільство більш вразливим до пропаганди, що може використовуватися як механізм масового управління. Інформаційний тероризм може мати катастрофічні наслідки для економіки. Маніпуляції фінансовими ринками через фейкові новини, злам корпоративних акаунтів або кібератаки на банки можуть викликати економічні кризи.

Наприклад, у 2013 році в Twitter з’явилося фейкове повідомлення від агентства Associated Press про вибух у Білому домі та поранення Барака Обами. Реакція ринку була миттєвою: фондовий індекс Dow Jones впав на 150 пунктів, а ринки втратили мільярди доларів у лічені хвилини, поки інформацію не спростували. Окрім того, інформаційні атаки можуть використовуватися для економічного шантажу або дискредитації конкурентів. Китай, США, Європа та інші великі гравці часто звинувачують один одного у використанні дезінформаційних кампаній для підриву економічних позицій суперників. Інформаційний тероризм сприяє розколу суспільства, підсилюючи поляризацію та екстремізм. Дезінформаційні кампанії часто будуються на розпалюванні ненависті між різними групами населення – за релігійною, етнічною, політичною чи іншою ознакою. У багатьох країнах спостерігається зростання популістських рухів, які базуються на інформаційних маніпуляціях. Наприклад, кампанії проти мігрантів у Європі та США часто побудовані на перебільшенні загрози від біженців, створюючи ілюзію "вторгнення" та "знищення культури".

Це може призводити до радикалізації молоді, яка починає сприймати світ через призму дихотомії "ми проти них". Особливо небезпечними є випадки, коли такі інформаційні кампанії використовуються для вербування в терористичні організації або екстремістські групи. Інформаційний тероризм сьогодні має наслідки, які виходять далеко за межі короткострокового впливу на громадську

думку, і проникають у саму структуру міжнародної безпеки. Однією з ключових проблем є руйнування легітимності глобальних інституцій. Коли маніпулятивні інформаційні кампанії масово поширюють спотворені дані про діяльність міжнародних організацій або національних урядів, це підриває довіру як до окремих держав, так і до системи глобального управління. Зміщення наративів у медіапросторі може призвести до того, що міжнародна спільнота починає сприймати офіційні повідомлення як суб'єктивні або навіть підроблені, що ускладнює координацію спільних дій у відповідь на кризові ситуації. Ще один важливий аспект — вплив на національну ідентичність та соціальну згуртованість. Інформаційний тероризм, використовуючи точковий вплив на різні групи населення, створює ехо-камери, де повторювані наративи не тільки формують негативне сприйняття опонентів, а й підривають відчуття спільності в суспільстві. Це може стати каталізатором внутрішньої поляризації, коли суспільство розділяється на радикально протилежні табори. Такий розкол часто перетворюється на фактор, який ускладнює вирішення конфліктів на національному рівні, що, у свою чергу, створює передумови для міждержавних протиріч і навіть гібридних воєн[36].

Також важливим є аспект інформаційного впливу на міжнародну економіку та фінансові ринки. Систематичне поширення дезінформації може вплинути на глобальні біржові індекси, валютні курси і інвестиційний клімат. Наприклад, інформаційні атаки, спрямовані на виклик паніки серед інвесторів, можуть спричинити короткострокові фінансові кризи, що, проте, мають довготривалі наслідки для стабільності міжнародних фінансових систем. Втрата довіри до офіційних економічних даних або заяв урядів може підірвати співпрацю між країнами, що вже є надзвичайно важливим в умовах глобалізації. Ще один аспект полягає у впливі на кіберпростір і технологічну залежність сучасних держав. Інформаційний тероризм активно використовує новітні технології, зокрема штучний інтелект, алгоритми обробки великих даних та технології машинного навчання, щоб створювати персоналізовані пропагандистські повідомлення. Це не лише підсилює вплив на окремих користувачів, а й призводить до розростання інформаційних мереж, де зловмисники можуть контролювати потік даних і

маніпулювати інформацією практично в режимі реального часу. Така технологічна залежність створює додаткові ризики для держав, оскільки неспроможність захистити свої інформаційні системи може стати вирішальним фактором у кризових ситуаціях.

Нарешті, важливо зазначити, що наслідки інформаційного тероризму мають глибокий психологічний вимір. Постійне потрапляння в інформаційні "хмаринки" з негативними наративами може призвести до емоційного виснаження населення, зниження рівня суспільної активності та навіть формування хронічного стану недовіри до державних інституцій. Це створює довгострокову загрозу для демократії, адже суспільство, яке втратило віру в чесність і ефективність своїх керівників, може стати легким мішенню для радикалізації та екстремістських рухів. У підсумку, наслідки інформаційного тероризму для міжнародної безпеки охоплюють не лише політичну дестабілізацію, але й порушення економічної стабільності, руйнування соціальної згуртованості, загострення глобальної кіберзагрози та психологічне виснаження населення. Для ефективного протидії цим викликам необхідно розробляти нові технології захисту інформаційного простору, будувати системи раннього попередження та постійно підвищувати рівень медіаграмотності в усьому світі, що дозволить суспільству краще протистояти маніпуляціям і зберегти довіру до своїх інституцій..

РОЗДІЛ ІІІ

Механізми протидії інформаційному тероризму

3.1. Міжнародно-правові механізми боротьби з інформаційним тероризмом

Перші спроби осмислення проблеми з’явилися ще у 1990-х роках, коли розвиток Інтернету та електронних комунікацій викликав хвилю кіберзлочинності. Тоді увагу приділяли переважно технічним аспектам — несанкціонованому доступу

до даних, шахрайству, порушенню авторських прав. Однак уже тоді окремі дослідники, зокрема Баррі Коллінз і Дорін Карлсон, попереджали, що загроза полягає не лише у злочинах проти даних, а й у використанні інформації як інструменту політичного насильства. Саме з цього контексту у 2001 році з'явилася Будапештська конвенція про кіберзлочинність, яка стала першим міжнародним документом, що регулював поведінку держав у кіберпросторі. Будапештська конвенція залишається базовим інструментом співпраці у галузі кібербезпеки. Вона встановлює юридичні рамки для криміналізації комп'ютерних злочинів, обміну доказами та надання взаємної правової допомоги. Однак вона не містить поняття "інформаційного тероризму", адже була створена до появи соціальних мереж і масових інформаційних атак. У ній не враховано психологічний чи пропагандистський вимір маніпуляцій. Тому на сучасному етапі конвенція потребує модернізації. Рада Європи у 2022 році ухвалила Другий додатковий протокол, який розширює можливості обміну електронними доказами між державами. Але навіть цей документ не вирішує проблеми контентних маніпуляцій, що мають на меті дестабілізацію держав чи підрив демократичних інститутів. ООН займає центральне місце у глобальній системі правового реагування. Проте донині не ухвалено жодної спеціальної конвенції про боротьбу з інформаційним тероризмом. Існуючі документи лише частково торкаються цього питання. Резолюції Генеральної Асамблеї "Про досягнення в галузі інформатизації і телекомунікацій у контексті міжнародної безпеки" визнають загрозу інформаційних атак, але не пропонують конкретних механізмів притягнення до відповідальності. У 2015 році ООН вперше створила Групу урядових експертів із безпеки у сфері інформаційних технологій, яка дійшла висновку, що держави мають утримуватись від атак на критичну інфраструктуру інших держав. Це стало важливим прецедентом, але юридично залишилося рекомендаційним. Найближчим до поняття інформаційного тероризму є визначення, запропоноване у резолюції Ради Безпеки ООН №2341 (2017). У ній зазначено, що терористичні організації можуть використовувати інформаційні технології для пропаганди, вербування, координації і здійснення нападів. Хоча ця резолюція була спрямована насамперед проти "Ісламської

держави", вона заклала основу для подальшого тлумачення інформаційних операцій як потенційної форми тероризму. Водночас Рада Безпеки не надала чітких юридичних критеріїв, які дозволили б розмежовувати інформаційні атаки терористичного характеру від державних пропагандистських кампаній. Європейський Союз розвинув більш системний підхід. З 2015 року, після гібридної агресії Росії проти України, ЄС розпочав формування політики кібер- і інформаційної безпеки. Було створено Європейський центр протидії гібридним загрозам у Гельсінкі, а також систему Rapid Alert System для моніторингу дезінформаційних кампаній у країнах-членах. ЄС розробив Кодекс практик з протидії дезінформації, який зобов'язує соціальні платформи співпрацювати з урядами, зменшувати поширення фейків і звітувати про власні алгоритми. Хоча документ не має сили закону, він заклав основу для формування нової європейської етики цифрової відповідальності. ОБСЄ приділяє особливу увагу інформаційним загрозам у політичному контексті. Її Бюро демократичних інститутів і прав людини (ODIHR) розглядає дезінформацію як загрозу виборчому процесу. Спостережні місії ОБСЄ дедалі частіше фіксують випадки маніпуляцій у соціальних мережах, що можуть впливати на результати виборів. З 2020 року організація пропонує державам запроваджувати етичні кодекси онлайн-комунікації для політичних партій, спрямовані на запобігання інформаційним провокаціям під час виборів. Проте ОБСЄ також стикається з політичним опором, адже окремі держави-члени використовують аргумент "інформаційного суверенітету" для уникнення міжнародного контролю.

НАТО визнало інформаційні атаки окремим типом загрози у своїй Стратегічній концепції 2023 року. Альянс розробив підхід "Comprehensive Defence", який включає не лише кіберзахист, а й інформаційну оборону. Країни-члени зобов'язалися обмінюватися інформацією про дезінформаційні операції, координувати комунікаційні реакції і підтримувати спільні тренінгові центри. Важливо, що НАТО підходить до проблеми не як до технічної, а як до когнітивної — тобто визнає, що об'єктом атаки є не мережа, а свідомість громадян. Це один із небагатьох прикладів, коли безпековий альянс адаптує свою

доктрину до реалій інформаційної війни. У межах Ради Європи формується новий напрям правового регулювання. Після вторгнення Росії в Україну у 2022 році комітет Ради Європи почав роботу над рамковою конвенцією щодо дезінформації та інформаційних маніпуляцій. Основна ідея — встановити баланс між свободою вираження і необхідністю протидії інформаційним загрозам. У червні 2023 року ухвалено "Декларацію про права людини у цифровому середовищі", де наголошується, що право на інформацію включає право на достовірну інформацію. Це перший випадок, коли міжнародний документ визнає дезінформацію порушенням прав людини. На національному рівні законодавчі ініціативи також набувають глобального значення. США застосовують модель "активного стримування". Закон Countering Foreign Propaganda and Disinformation Act (2016) створив Центр глобальної взаємодії (Global Engagement Center), який координує діяльність уряду щодо виявлення та нейтралізації іноземних дезінформаційних кампаній. ЄС реалізує схожу ініціативу через East StratCom Task Force, що працює під егідою Європейської служби зовнішніх дій. Ці структури формують нову практику — інформаційний захист як елемент зовнішньої політики. В Україні питання правової протидії інформаційному тероризму набуло особливої актуальності. Закон "Про основи національної безпеки" (2021) офіційно визначає інформаційну безпеку як один із пріоритетів державної політики. У 2023 році РНБО затвердила "Стратегію інформаційної безпеки України", яка передбачає створення єдиної системи моніторингу інформаційних загроз, розвиток співпраці з ЄС і НАТО та оновлення законодавства з урахуванням міжнародних стандартів. Український досвід став унікальним прикладом того, як держава може одночасно боротися з інформаційним терором і зберігати демократичні свободи. Водночас міжнародно-правові механізми стикаються з низкою об'єктивних обмежень. По-перше, інформаційний тероризм має транснаціональний характер. Актори, що здійснюють атаки, можуть перебувати за межами юрисдикції постраждалої держави. Екстрадиція у таких випадках практично неможлива, оскільки більшість правових систем не визнає інформаційні злочини терористичними. По-друге, швидкість поширення інформації не дає змоги реагувати у межах

традиційних правових процедур. Навіть найоперативніше розслідування може завершитись тоді, коли наслідки вже настали[38].

Міжнародна спільнота усвідомлює потребу створення глобального механізму координації дій. Одним із можливих напрямів є створення Міжнародної агенції з інформаційної безпеки під егідою ООН або Ради Європи. Така структура могла б об'єднати технічні, юридичні та гуманітарні функції, забезпечуючи оперативний обмін інформацією між державами і платформами. Досвід співпраці Інтерполу у сфері боротьби з кіберзлочинами доводить, що подібні механізми можуть бути ефективними, якщо вони поєднують державний і приватний сектори. Одним із найскладніших питань залишається співвідношення між свободою слова і захистом від дезінформації. Право на вільне висловлення думок закріплене у статті 19 Міжнародного пакту про громадянські і політичні права, але цей самий документ дозволяє обмеження, якщо вони необхідні для національної безпеки або громадського порядку. Держави трактують цю норму по-різному. Демократичні країни наголошують на мінімальному втручанні, тоді як авторитарні використовують її для обґрунтування тотального контролю. Саме тому будь-які міжнародно-правові ініціативи у цій сфері потребують чітких запобіжників проти зловживань.

Загальновизнаним напрямом подальшого розвитку є запровадження принципу due diligence — належної обачності. Він означає, що держави зобов'язані не лише утримуватись від інформаційних атак, а й запобігати їх здійсненню зі своєї території. Це положення вже застосовується у практиці Міжнародного суду ООН щодо кіберінцидентів і може бути поширене на інформаційні злочини. Проте для цього потрібно закріпити його у нових міжнародних угодах. Важливим кроком стало створення у 2023 році Глобальної коаліції з інформаційної стійкості (Global Information Resilience Coalition), до якої увійшли понад 40 країн, серед них Україна, Канада, США, Польща, Німеччина, Японія. Її мета — розробка єдиних стандартів реагування на дезінформацію, у тому числі алгоритмів швидкої оцінки і кваліфікації інформаційних інцидентів. Хоча коаліція не має юридично обов'язкового статусу, вона створює передумови для появи нового міжнародного договору, який може стати аналогом "цифрової Женевської

конвенції". Водночас приватний сектор відіграє дедалі важливішу роль у формуванні правового поля. Технологічні корпорації, такі як Meta, Google, Microsoft, уже створили власні етичні кодекси і платформи для співпраці з урядами. Їхня участь у правовому регулюванні стала фактичним замінником міждержавних домовленостей. Це піднімає питання про "приватизацію міжнародного права", коли відповідальність за дотримання норм безпеки переходить від держав до корпорацій. Така тенденція потребує врівноваження: держава має зберігати роль гаранта, а не спостерігача. Подальший розвиток міжнародно-правових механізмів боротьби з інформаційним тероризмом залежить від готовності держав узгодити базові принципи. Без таких кроків боротьба з інформаційним терором залишатиметься фрагментарною і реактивною. Європейський Союз пішов шляхом комбінованої відповідальності. Регуляторні акти накладають вимоги на платформи. Кодекс практик з протидії дезінформації запровадив саморегуляцію під наглядом Єврокомісії. Платформи мають зменшувати видимість фейкових матеріалів, відкривати доступ до даних для дослідників, позначати політичну рекламу. Ці вимоги підсилює Digital Services Act. DSA встановлює обов'язки due diligence для дуже великих онлайн платформ. Йдеться про системні оцінки ризиків, у тому числі інформаційних загроз для виборів, здоров'я, громадського порядку. ЄС не вводить поняття інформаційного тероризму. Він вибудовує техніко-процедурну архітектуру, яка знижує шкоду. Це інший шлях до того самого результату. ОБСЄ працює на перетині безпеки і виборчих процесів. Спостережні місії фіксують маніпуляції в соціальних мережах, координацію бот-мереж, нелегальну рекламу і приховані впливи. Рекомендації стимулюють держави запроваджувати прозорість онлайн-агітації, швидкі механізми спростувань і медіаграмотність для виборців. ОБСЄ наголошує, що обмеження повинні бути необхідними і пропорційними. Це важливо для прав людини. Політична згода учасників обмежена. Частина держав наполягає на пріоритеті інформаційного суверенітету. Це гальмує спільні рішення.

НАТО визнає інформаційні операції загрозою колективній безпеці. Стратегічна концепція фіксує когнітивний вимір оборони. Альянс розвиває навчання, обмін

тактиками контрдезінформації, методики оцінки впливу на аудиторії. Юридична рамка поки що вузька. Вона ґрунтується на добровільних зобов'язаннях держав. Важливий практичний акцент. НАТО сприймає інформаційні атаки як частину гібридних кампаній, тому інтегрує комунікацію у планування оборони. Це зближує право і стратегію.

Рада Європи рухається в бік правового визначення прав людини в цифровому середовищі. Декларації 2023 року стверджують, що право на інформацію включає доступ до достовірних відомостей. Це закладає основу для розуміння системних дезінформаційних кампаній як порушення прав. Паралельно триває робота над інструментами проти маніпуляцій у медіаекосистемі. Мета проста. Захистити простір для свободи слова і одночасно мінімізувати організовані впливи, що руйнують демократичні процеси. Оціночний характер категорій лишається проблемою. Вирішити її здатні тільки чіткі критерії і незалежні процедури.

У підсумку міжнародно-правові механізми вже мають каркас. Його формують Будапештська конвенція та її протоколи, керівні норми ООН щодо відповідальної поведінки, регулювання ЄС, рекомендації ОБСЄ, практики НАТО. Вони не дають повного визначення інформаційного тероризму. Вони забезпечують інструменти, через які можна знизити шкоду і підвищити відповідальність. Наступний крок передбачає консолідацію. Потрібен рамковий договір, який узгодить due diligence, прозорість платформ, маркування синтетики, доступ дослідників до даних, стандарти швидкої взаємодії та захист прав людини.

Міжнародне право звикало до нових технологій століттями. Темп уже не дозволяє повільну адаптацію. Інформаційний тероризм вражає там, де суспільства найвразливіші. Там, де довіра тонка. Право має посилити довіру. Воно повинно бути швидким, передбачуваним і контрольованим. Лише тоді юридичні механізми стануть реальним бар'єром проти страху, паніки і маніпуляцій.

3.2. Роль міжнародних організацій у протидії інформаційним загрозам

Інформаційні загрози у XXI столітті стали викликом не лише для національних урядів, а й для міжнародних інституцій. Жодна держава не здатна ефективно протидіяти інформаційному тероризму самостійно. Його природа транснаціональна. Він діє поза кордонами, використовує глобальні платформи, а наслідки поширюються на політичну, економічну, соціальну та культурну сфери одночасно. Саме тому роль міжнародних організацій у цій сфері стала стратегічною. Вони формують правові рамки, координують спільні дії,

розробляють стандарти етичної поведінки в цифровому середовищі, здійснюють моніторинг і забезпечують обмін інформацією між державами.

ООН традиційно виступає центром глобального регулювання. З початку 2000-х вона включила інформаційну безпеку до порядку денного міжнародного миру. У межах Генеральної Асамблеї діє Група урядових експертів з інформаційної безпеки (GGE), створена резолюцією 57/239. Вона досліджує, як принципи Статуту ООН — суверенітет, невтручання, відповідальність держав — застосовуються до кібер- і інформаційного простору. Головний висновок цих експертів полягає в тому, що держави зобов'язані дотримуватись міжнародного права і не можуть використовувати інформаційні технології для підриву стабільності інших країн.

Паралельно з Групою експертів діє Відкрита робоча група з питань ІКТ (OEWG). Її мандат ширший — вона залучає не лише держави, а й наукові установи, приватний сектор та громадські організації. OEWG підготувала у 2021 році звіт, у якому вперше запропоновано створення системи довіри та прозорості у кіберпросторі, зокрема обміну інформацією про дезінформаційні кампанії та їхніх джерела. Хоча документ не має юридичної сили, він став базовою платформою для розвитку міжнародного діалогу щодо протидії інформаційним загрозам.

У структурі ООН важливу роль відіграє також ЮНЕСКО. Організація просуває концепцію інформаційної грамотності як базового елемента прав людини на освіту і доступ до правди. Програма "Media and Information Literacy" реалізується у понад 100 країнах. ЮНЕСКО розглядає медіаграмотність як довгострокову форму протидії інформаційному тероризму, оскільки саме освічене суспільство здатне протистояти маніпуляціям. У 2022 році організація ухвалила рекомендації "Guidelines for Regulating Digital Platforms", де підкреслено, що держава повинна не лише реагувати на фейки, а й гарантувати відкритість та плюралізм джерел інформації.

Рада Безпеки ООН поступово почала розглядати дезінформацію як загрозу міжнародному миру. Деякі члени, зокрема Франція, Велика Британія і США,

ініціювали дебати про використання інформаційних технологій у гібридних війнах. Проте відсутність консенсусу серед постійних членів не дозволила ухвалити спеціальну резолюцію. Росія та Китай виступають проти універсального визначення інформаційного тероризму, аргументуючи це необхідністю захисту "інформаційного суверенітету". Таким чином, на рівні ООН зберігається політичний розкол між державами, що прагнуть колективних правил, і тими, що вбачають у них загрозу власному контролю над інформаційними потоками[39].

Європейський Союз сформував найрозвиненішу систему інституційної протидії інформаційним загрозам. Після 2014 року, коли ЄС зафіксував масові кампанії російської дезінформації, було створено низку органів. Найважливіші з них — East StratCom Task Force та European External Action Service (EEAS). Їх завдання — виявлення, аналіз і публікація прикладів фейкових кампаній. East StratCom веде базу даних EUvsDisinfo, яка містить понад 15 тисяч кейсів. Це наймасштабніший відкритий каталог дезінформаційних операцій у світі. Крім моніторингу, структура забезпечує комунікацію з урядами країн-членів, ЗМІ та платформами, що робить її центром оперативного реагування.

Європейська Комісія зосередилася на системному регулюванні платформ. У межах програми "Єдиний цифровий ринок" (Digital Single Market) ухвалено Закон про цифрові послуги (Digital Services Act, 2022), який встановлює юридичну відповідальність великих онлайн-платформ за поширення дезінформації. Комісія також ініціювала Кодекс практик із протидії дезінформації — добровільний, але обов'язковий для компаній, що підписали його. Вони мають звітувати про дії проти інформаційних загроз. Цей кодекс став основою для нової моделі співпраці між державою, приватним сектором і громадськістю.

Рада Європи доповнює цей процес правовими стандартами. У 2023 році вона ухвалила Декларацію про права людини у цифровому середовищі. Документ визнає доступ до достовірної інформації елементом свободи вираження. У ньому

також зазначено, що організована дезінформація, яка підриває демократію або розпалює ворожнечу, є порушенням міжнародних зобов'язань держав у сфері прав людини. Таким чином, Рада Європи закріплює правовий фундамент, на якому ЄС і національні уряди можуть будувати політику протидії інформаційному тероризму.

ОБСЄ відіграє координаційну роль у політичному та гуманітарному вимірі. Її інституції — Представник з питань свободи ЗМІ (RFoM) та Бюро демократичних інститутів і прав людини (ODIHR) — розробили рекомендації для урядів щодо забезпечення прозорості у цифрових кампаніях, запобігання маніпуляціям під час виборів і посилення медіаосвіти. ОБСЄ вважає, що боротьба з дезінформацією не може зводитися до блокування контенту. Її мета — створення середовища, де інформаційна маніпуляція втрачає ефективність. Для цього організація реалізує програму "Building Media Resilience", спрямовану на навчання журналістів і держслужбовців в країнах Центральної та Східної Європи.

НАТО є однією з небагатьох безпекових структур, які інтегрували інформаційний вимір у власну стратегію оборони. Стратегічна концепція НАТО 2023 року визначає дезінформацію і психологічні операції як окремий тип загрози. Центр стратегічних комунікацій НАТО у Ризі (NATO StratCom COE) аналізує інформаційні атаки, розробляє методики контрнаративів, проводить навчання для урядових і військових структур. У межах "Cognitive Resilience Initiative" Альянс підкреслює, що інформаційна стійкість — така сама частина колективної оборони, як кіберзахист чи протиповітряна оборона. Ключова ідея — зберегти когнітивну стабільність суспільства навіть під постійним інформаційним тиском.

Інтерпол залучений до боротьби з кіберзлочинністю і дезінформацією, коли вони мають ознаки кримінального правопорушення. Підрозділ INTERPOL Cybercrime Directorate координує розслідування атак, що супроводжуються інформаційними маніпуляціями. Зокрема, програма "Digital Security Challenge" ідентифікує

фейкові кампанії, пов’язані з фінансовими шахрайствами, фішингом або підробкою офіційних повідомлень. Інтерпол прагне розробити єдину систему класифікації цифрових злочинів, щоб держави могли швидше обмінюватися доказами у справах, де інформаційна дезінформація стає інструментом терору.

ВООЗ, хоч і не є безпековою організацією, відіграла ключову роль у протидії дезінформації під час пандемії COVID-19. Організація вперше в історії ввела термін “інфодемія” — надлишок неправдивої інформації, який ускладнює реагування на кризу. ВООЗ створила платформу EPI-WIN, яка забезпечує достовірні комунікації під час глобальних надзвичайних ситуацій. Цей досвід показав, що інформаційна безпека має міжсекторальний характер. Навіть організації, які не займаються безпекою безпосередньо, мусять розробляти власні протоколи реагування на інформаційні атаки.

ЮНЕСКО, Рада Європи, ОБСЄ і ВООЗ у 2023 році підписали спільну декларацію про медіаосвіту та боротьбу з дезінформацією. Вона наголошує на трьох принципах: освіта, прозорість, відповідальність. Декларація передбачає створення глобальної системи сертифікації програм медіаграмотності, що дозволить уніфікувати стандарти навчання для країн-членів. Таким чином формується горизонтальна мережа взаємодії між міжнародними організаціями — замість ієрархії, яка часто гальмувала реагування.

Важливою тенденцією є формування багаторівневої архітектури протидії. На верхньому рівні — ООН, яка формує базові принципи. На регіональному — НАТО, ЄС, ОБСЄ та Рада Європи, що впроваджують норми у своїх членів. На секторальному — ВООЗ, ЮНЕСКО, Інтерпол, які працюють з конкретними сферами. Така структура забезпечує широту охоплення, але створює ризик дублювання функцій. У багатьох випадках відсутня єдина база даних або система координації. Це знижує швидкість реагування, особливо під час масштабних інформаційних криз.

У відповідь на це у 2023 році ЄС спільно з НАТО та ООН започаткували ініціативу “Joint Response Mechanism on Disinformation”. Її мета — створення

мережі швидкого реагування між державами, платформами та міжнародними структурами. Механізм передбачає, що у разі масштабної інформаційної атаки держави обмінюються сигналами про походження загрози, надають технічну підтримку і координують публічну комунікацію. Це перший крок до створення глобального кризового центру з інформаційної безпеки, який міг би функціонувати подібно до структур, що реагують на терористичні чи природні катастрофи.

Попри активність міжнародних організацій, залишається проблема політичної узгодженості. Держави по-різному розуміють межі втручання у цифрову сферу. Демократичні країни наполягають на мінімальному регулюванні контенту, тоді як авторитарні — на повному контролі. Через це багато ініціатив залишаються консультативними. Проте навіть у таких умовах діяльність міжнародних структур формує загальний морально-правовий стандарт: інформаційні атаки не є проявом свободи слова, а становлять загрозу миру, демократії та розвитку.

Україна є активним учасником більшості цих ініціатив. Вона інтегрувалася у спільні проекти НАТО StratCom, бере участь у програмі ЄС East StratCom Task Force, співпрацює з ОБСЄ та Радою Європи у сфері медіаосвіти. Український досвід боротьби з інформаційною агресією став практичним полігоном для міжнародного співтовариства. На його основі розробляються навчальні курси НАТО, посібники ОБСЄ, рекомендації для Центру протидії дезінформації при РНБО. Це доводить, що міжнародні організації не лише допомагають державам, а й навчаються на їхньому досвіді. Поступово формується концепція “інформаційної стійкості” (information resilience). Її просувають НАТО, ЄС, ООН і ЮНЕСКО як спільну методологічну основу. Вона охоплює три компоненти: правові норми, технологічну безпеку і психологічну готовність населення. Кожна міжнародна організація вносить свій елемент. НАТО — оборонний і когнітивний, ЄС — правовий і регуляторний, ЮНЕСКО — освітній, ВООЗ — комунікаційний. У комплексі ці підходи створюють новий вимір безпеки, де ключовим стає не контроль над інформацією, а довіра до джерел.

Майбутнє міжнародної протидії інформаційним загрозам залежить від здатності організацій координувати зусилля. Ефективна система має базуватися на обміні даними у реальному часі, узгоджених процедурах оцінки загроз і спільній відповідальності за наслідки. Необхідно створити єдину платформу для моніторингу глобальних інформаційних атак, подібну до системи оповіщення про пандемії. Такий центр міг би діяти під егідою ООН, використовуючи інфраструктуру ЮНЕСКО, НАТО StratCom і ЄС East StratCom. Це дозволить швидко фіксувати джерела атак, оцінювати їхній масштаб і надавати державам рекомендації щодо реагування.

Підсумовуючи, міжнародні організації відіграють ключову роль у формуванні нормативного, інституційного та практичного каркасу боротьби з інформаційними загрозами. Їхня діяльність показує, що глобальна безпека у цифрову епоху залежить не від кількості законів, а від рівня довіри, взаємодії та солідарності. Інформаційна війна не може бути виграна окремою країною. Вона вимагає спільної відповідальності міжнародних акторів, узгоджених дій і готовності реформувати застарілі моделі управління. У цьому сенсі міжнародні організації стають не просто майданчиками для переговорів, а архітекторами нового інформаційного порядку, де істина і безпека взаємопов’язані.Попри активну діяльність основних міжнародних організацій, ефективність глобальної протидії інформаційним загрозам залишається нерівномірною. Кожна структура формує власні інструменти, проте бракує узгодженого підходу. Проблема не лише у відмінностях мандатів, а й у різних концептуальних уявленнях про природу інформаційного тероризму. Для одних це продовження кіберзлочинності, для інших — форма політичної агресії або навіть ідеологічна зброя. Саме тому міжнародні організації дедалі частіше намагаються координувати свої підходи через міжінституційні платформи, обмін експертами й спільні навчальні програми.

ООН залишається політичним центром цього процесу. У 2023 році Генеральна Асамблея підтримала резолюцію “Information Integrity in the Digital Age”, ініційовану Кенією, Естонією та Канадою. У документі наголошується, що дезінформація й маніпуляції становлять загрозу праву народів на

самовизначення. Резолюція закликала створити єдиний координуючий орган під егідою ООН, який би інтегрував діяльність ЮНЕСКО, МСЕ, ПРООН і ВООЗ у сфері комунікаційної безпеки. Обговорюється модель на зразок Ради з прав людини — із власним секретаріатом, регіональними представництвами та механізмом звітності. Ідея полягає в тому, щоб не лише реагувати на інформаційні кризи, а й попереджати їх через раннє виявлення маніпуляцій у міжнародному просторі[40,41,42,43,44,45,46].

3.3. Політика держав щодо забезпечення інформаційної безпеки

Інформаційна безпека у сучасному світі перетворилася на один із головних елементів державного суверенітету. Якщо в минулому держава захищала територію, населення і ресурси, то сьогодні вона змушена захищати простір сприйняття, комунікацій і довіри. Політика інформаційної безпеки — це не лише технічні заходи чи закони проти фейків, а комплексна стратегія, що охоплює політичне управління, освіту, правову культуру, міжнародну співпрацю і взаємодію з медіа. Держави, які першими зрозуміли цю динаміку, створили стійкі системи інформаційного управління. Інші опинилися у ситуації постійного реагування. Сучасна архітектура політики інформаційної безпеки формується у трьох вимірах: правовому, інституційному та соціальному. Правовий вимір

визначає межі свободи слова і відповідальності за інформаційні злочини. Інституційний — описує структуру державних органів, відповідальних за безпеку в інформаційній сфері. Соціальний — охоплює рівень довіри громадян до офіційних джерел і готовність протистояти маніпуляціям. Кожна держава вибудовує баланс між цими елементами по-своєму.

Україна належить до держав, для яких інформаційна безпека має екзистенційний характер. З 2014 року, після початку російської агресії, інформаційна політика стала частиною національної оборони. У 2016 році ухвалено Доктрину інформаційної безпеки України, що визначила головні загрози: дезінформацію, пропаганду війни, спроби підриву конституційного ладу, маніпуляції громадською думкою з боку іноземних держав. Доктрина передбачила створення спеціалізованих структур — Ради національної безпеки і оборони, Міністерства культури та інформаційної політики, Служби безпеки України — які координують заходи у цій сфері. У 2021 році створено Центр протидії дезінформації при РНБО. Він став ключовим органом моніторингу та координації дій державних і громадських інституцій у сфері інформаційної безпеки. Українська політика в цій галузі базується на принципі "активної оборони". Це означає, що держава не лише реагує на інформаційні атаки, а й веде проактивну комунікацію — роз'яснює дії влади, спростовує фейки, навчає громадян інформаційній грамотності. Українська модель є унікальною тим, що вона поєднує військовий і цивільний підходи. З одного боку, в інформаційній безпеці беруть участь органи сектору оборони, з іншого — культурні, освітні та медійні інституції. Після початку повномасштабного вторгнення у 2022 році комунікаційна стратегія держави стала інтегрованою частиною національної безпеки. Вона поєднує офіційні повідомлення, кризові інструкції, міжнародні брифінги і взаємодію з платформами. Україна є прикладом держави, що створила стійкість через прозорість і системне пояснення своєї позиції.

Німеччина підходить до питання інформаційної безпеки через правовий та етичний баланс. У 2017 році було ухвалено Закон про покращення правозастосування у соціальних мережах (NetzDG), який зобов'язав платформи видаляти незаконний контент протягом 24 годин після повідомлення. Закон викликав дискусії про межі свободи слова, однак став зразком для інших країн ЄС. Крім того, Німеччина інтегрувала питання інформаційної безпеки у свою Стратегію кібербезпеки 2021 року. Відповідальність розподілена між Федеральним відомством з інформаційної безпеки (BSI), Федеральною розвідувальною службою (BND) і Міністерством внутрішніх справ. Особливістю німецької моделі є акцент на освіті: медіаграмотність включено у навчальні програми шкіл і університетів. Держава вважає, що довгострокова стійкість можлива лише через критичне мислення громадян. Німеччина також є лідером у розвитку інформаційної дипломатії. Вона координує проекти ЄС, пов'язані з боротьбою проти дезінформації, і активно підтримує діяльність East StratCom Task Force. Після російської агресії проти України німецький уряд створив програму "Resilient Democracy Initiative", спрямовану на моніторинг внутрішніх і зовнішніх інформаційних загроз. Програма включає систему раннього виявлення фейкових кампаній, аналітичні центри при університетах і державне фінансування незалежних фактчекінгових організацій. Таким чином, Німеччина розвиває "демократичну оборону" — модель, де держава виступає гарантом прозорості та партнером громадянського суспільства.

Польща посідає проміжне місце між оборонною і регуляторною моделями. Її політика базується на трьох принципах: державна координація, технологічна модернізація і соціальна мобілізація. Основним документом є "Стратегія національної безпеки Республіки Польща" (2020), у якій інформаційна безпека визначена як ключовий елемент національної стійкості. Відповідальним органом є Міністерство цифровізації, яке координує дії державних і приватних структур. Польща активно співпрацює з НАТО і ЄС, бере участь у програмах East StratCom і StratCom COE у Ризі. Важливим елементом є програма "Bezpieczny Internet", яка об'єднує державні органи, ЗМІ, освітні інституції і волонтерів для боротьби з онлайн-маніпуляціями.

США мають найрозвиненішу систему стратегічного управління інформаційною безпекою. У 2018 році було ухвалено “National Cyber Strategy”, а у 2022 році — “National Security Strategy”, де інформаційна безпека визначена як пріоритет національної політики. У 2021 році створено Офіс національного директора з кібер- та інформаційної безпеки (ONCD), який координує діяльність між різними федеральними агентствами. Важливо, що США розглядають інформаційну безпеку не лише як оборону, а як проактивний інструмент зовнішньої політики. Програми “Global Engagement Center” та “Digital Democracy Initiative” фінансують медіаграмотність і розвиток незалежних ЗМІ в усьому світі. Таким чином, інформаційна безпека у США є одночасно інструментом національного захисту і проєкцією впливу.

Американська модель базується на співпраці з приватним сектором. Такі компанії, як Google, Meta, Microsoft і Twitter, залучені до міжагентських ініціатив із боротьби проти дезінформації. У межах “Cybersecurity and Infrastructure Security Agency” (CISA) створено спеціальний підрозділ з аналізу інформаційних операцій, який координує співпрацю між урядом і корпораціями. Проте така модель має і критику — громадські організації наголошують на ризиках концентрації влади в руках технологічних гігантів. Незважаючи на це, США залишаються прикладом держави, яка поєднує технологічну потугу, стратегічне планування і дипломатію цінностей.

Китай вибудував принципово іншу модель, яку можна охарактеризувати як “інформаційний суверенітет”. Політика держави спрямована на повний контроль над інформаційним середовищем. У 2017 році ухвалено Закон про кібербезпеку, який зобов’язує всі технологічні компанії зберігати дані на території Китаю і передавати їх державним органам за запитом. У 2021 році прийнято Закон про захист даних, який формально проголошує захист приватності, але водночас розширює повноваження держави у сфері контролю. Китайська модель виходить з принципу, що інформація — стратегічний ресурс, а її неконтрольований обіг

становить загрозу державній стабільності. Державні ЗМІ, такі як CCTV та Xinhua, виконують функцію централізованої комунікації уряду. Китай також активно розвиває власні платформи (WeChat, Weibo, TikTok/Douyin), які підпорядковуються національному законодавству і забезпечують фільтрацію контенту.

Підхід Китаю має дві сторони. З одного боку, це гарантує високу стабільність внутрішнього інформаційного середовища, з іншого — обмежує свободу слова та плюралізм. Проте китайська держава не приховує свого стратегічного бачення: інформаційна безпека розглядається як частина національного відродження. У рамках 14-го п'ятирічного плану розвитку передбачено створення "Національної системи управління інформаційними ризиками", яка поєднує штучний інтелект, аналіз даних і психологічний моніторинг. Китай також активно експортує свою модель до країн Африки, Близького Сходу і Центральної Азії, де пропонує інфраструктурну підтримку в обмін на політичну лояльність.

Російська Федерація використовує інформаційну безпеку як інструмент внутрішнього контролю і зовнішньої агресії. Після 2014 року держава створила замкнену систему цифрового контролю, засновану на законах про "суверенний інтернет" і "захист традиційних цінностей". У 2021 році ухвалено "Доктрину інформаційної безпеки РФ", яка визначає мету — "захист духовних основ російського суспільства" та "протидію деструктивному інформаційному впливу Заходу". Реальною метою є централізація управління інформаційними потоками. Росія створила розгалужену мережу державних медіа, фабрик тролів, хакерських угруповань і культурних проєктів, що діють за межами країни. Інформаційна безпека перетворилася на інструмент гібридної війни — як проти України, так і проти держав ЄС та США.

Російська модель демонструє, як держава може використовувати риторику безпеки для легітимації цензури. Закони про “іноземних агентів” і “фейки про армію” дозволяють переслідувати незалежних журналістів і громадян, які поширюють інформацію, не узгоджену з офіційною лінією. У глобальному масштабі Росія поширює наративи, спрямовані на дискредитацію західних демократій, підрив довіри до інститутів і виправдання власних дій. Це створює пряму загрозу міжнародній інформаційній стабільності. Росія стала прикладом того, як політика інформаційної безпеки може перетворитися на політику інформаційного терору.

Усі розглянуті держави демонструють різні моделі реагування на інформаційні загрози. США, Німеччина та Польща будують системи на засадах партнерства, прозорості та демократичного контролю. Україна розвиває модель стійкості через кризову мобілізацію. Китай і Росія використовують інформаційну безпеку для зміцнення політичного контролю. Спільним для всіх є визнання інформаційного простору як арени національної безпеки. Відмінність полягає у тому, як держава визначає межу між захистом і цензурою[47,48,49,50,51,52,53].

3.4. Нові технологічні інструменти протидії

Нові технологічні інструменти протидії інформаційному тероризму формують основу сучасної архітектури безпеки у цифровому просторі. У другій половині 2010-х і особливо після 2020 року головним полем боротьби стали алгоритми, системи штучного інтелекту та комплексні інформаційно-аналітичні платформи, що дозволяють державам і міжнародним організаціям не лише виявляти дезінформацію, а й аналізувати її структуру, джерела, психологічні механізми впливу та масштаби поширення. Технологічний розвиток змінює саме розуміння інформаційної загрози. Якщо раніше головним джерелом загроз були масові медіа або офіційні пропагандистські платформи держав, то сьогодні ядром інформаційних атак є автоматизовані мережі ботів, глибинні генератори контенту, нейромережеві системи психологічного таргетингу та багаторівневі екосистеми алгоритмічного впливу. Саме тому держави і міжнародні структури

шукають способи адаптувати класичні моделі безпеки до нової цифрової динаміки [54].

Технологічний компонент протидії інформаційному тероризму ґрунтується на трьох ключових блоках: інструментах штучного інтелекту, партнерствах між державами й цифровими платформами та етичних стандартах алгоритмічного контролю. Кожен з них є відповіддю на конкретні виклики. Штучний інтелект дозволяє працювати з великими масивами даних, визначати закономірності та структуру інформаційних атак. Партнерства держав і платформ виникають через те, що приватні корпорації фактично контролюють інфраструктуру цифрового простору, а без їхньої участі державна політика стає неповною. Етичні стандарти необхідні для того, щоб нові інструменти не перетворювалися на засоби утиску свободи слова чи маніпулювання громадською думкою. у США, Brexit та атак під час пандемії COVID-19, головними елементами поширення інформаційного терору були соціальні медіа. Алгоритми машинного навчання дозволяють ідентифікувати штучні зміни в інформаційному трафіку. Наприклад, коли певна тема отримує стрибкоподібне зростання популярності без органічних причин, система сигналізує про можливу координацію. Такі моделі створені у Польщі (платформа ANALIZA24), Німеччині (проєкт Disinfomonitor) та США (CISA Information Flow Tracker). Україна також розробляє подібні системи. Центр протидії дезінформації у співпраці з приватними IT-компаніями працює над нейромережею, здатною визначати бот-активність у Telegram, Facebook та TikTok .

Важливим інструментом стає прогнозування інформаційних атак. Якщо на ранніх етапах головним завданням було виявлення фейків після їхнього поширення, то сьогодні підхід змінюється. Прогностичні системи аналізують попередні хвилі атак, визначають часові закономірності, ключові точки входу та можливі сценарії. Наприклад, НАТО StratCom COE створив мультиагентну модель, яка аналізує реакції суспільства та визначає найвразливіші групи

населення. Це дозволяє державам проводити превентивну інформаційну роботу ще до того, як атака почнеться [55].

Партнерства держав і платформ — інша складова технологічної протидії. Як показано у 3.2 і 3.3, найбільші ризики виникають через те, що інформаційний простір контролюється приватними корпораціями: Meta, Google, X, TikTok. Держави не можуть самостійно управляти потоками даних, контролювати алгоритми чи здійснювати швидке реагування. Саме тому формується нова модель “спільного суверенітету”, коли відповідальність за інформаційну безпеку поділяється між державними і приватними структурами. Вперше така модель була випробувана в США, коли CISA уклала угоди з великими IT-компаніями щодо обміну інформацією під час виборів 2020 року. Погоджена система дій дозволила відстежувати дезінформаційні атаки Росії та Ірану майже у реальному часі.

У Європейському Союзі партнерство реалізується через “Кодекс практик із протидії дезінформації”, відомий з аналізу в попередніх підрозділах. Цей кодекс зобов’язує технологічні компанії публікувати регулярні звіти про модерацію контенту, механізми виявлення маніпуляцій та інформацію про рекламні кампанії політичного характеру. Німеччина, Польща і Франція активно впроваджують національні механізми нагляду за платформами. Це дозволило краще контролювати розповсюдження ворожих наративів, особливо під час кризи на кордоні Польщі та Білорусі у 2021–2022 роках.

Важливим напрямом співпраці є обмін технічними даними. Приватні корпорації мають можливість бачити повну картину інформаційного трафіку, включно з метаданими, які недоступні державам. У той час як уряди володіють експертною інформацією щодо ворожих держав і організацій. Спільна робота дозволяє з’єднати два виміри — технологічний і розвідувальний. У 2023 році ЄС створив

“Європейський форум цифрової безпеки”, до якого увійшли понад 40 IT-компаній та представники держав. Україна отримала статус спостерігача у 2024 році, що дозволяє інтегрувати національні структури у європейські технологічні механізми.

Третій ключовий компонент — етичні межі алгоритмічного контролю. Коли держава отримує доступ до технологій аналізу поведінки, емоцій, соціальних зв’язків і психологічних реакцій, виникає ризик зловживань. Європейські стандарти створюють рамки, які обмежують держави та корпорації у використанні таких інструментів. Наприклад, Європейський акт про штучний інтелект (2024) забороняє застосування систем масового біометричного нагляду та алгоритмів політичних маніпуляцій. Проблема етичного контролю особливо актуальна в Україні, де інформаційне середовище одночасно є полем бою та простором демократії. Під час війни виникає спокуса посилити контроль над контентом, але надмірна централізація може призвести до втрати довіри суспільства. Тому українська модель інформаційної політики, описана в 3.3, орієнтована на партнерство між державою і громадянським суспільством, а не на посилення державної модерації. Поява незалежних фактчекінгових організацій, прозорість рішень медіарегулятора та міжнародний нагляд є важливими інструментами етичного стримування.

У контексті етичних меж виникає питання: хто має визначати, яка інформація є загрозою? Цей виклик зростає паралельно з розвитком технологій. Платформи, держава, міжнародні організації та громадські структури мають різні інтереси. Розробляються моделі багаторівневого контролю, які включають технічний аналіз, участь незалежних експертів, прозорі процедури видалення контенту, апеляційні механізми та публічну звітність. Ці механізми у перспективі можуть стати основою нового міжнародного стандарту, аналогічного до Загального регламенту ЄС із захисту даних (GDPR).

Розвиток технологічних інструментів протидії інформаційному тероризму не можна розглядати ізольовано від контексту, описаного у розділах 2 та 3. Державні і недержавні актори активно освоюють генеративні моделі, автоматичні системи таргетингу, психологічну інженерію. Тому протидія повинна включати не лише технології детекції, а й інструменти пояснення — просвітницькі програми, інформаційні кампанії, системи цифрової освіти. Нові технології допомагають лише тоді, коли суспільство має внутрішню стійкість. Саме тому НАТО, ЄС та уряди демократичних країн дедалі частіше роблять акцент не лише на інструментах виявлення атак, а й на формуванні психологічної та культурної стійкості, що було докладно описано у підрозділі 3.2 . Розвиток технологічних інструментів протидії інформаційному тероризму перетворився на один із ключових напрямів глобальної безпеки. Держави та міжнародні організації усвідомили, що інформаційний простір давно перестав бути пасивною платформою. Він став активним середовищем, у якому взаємодіють мільярди користувачів, автоматизовані системи, комерційні алгоритми та актори, які прагнуть використати вразливості суспільної психіки. Технологічні інструменти більше не доповнюють політику — вони формують її основу. Саме тому сучасна протидія базується не лише на розпізнаванні фейків, а й на аналізі поведінки, інфраструктури, динаміки інформаційних потоків і психологічних реакцій. Сучасна логіка інформаційного захисту переходить від пасивної реакції до активного прогнозування. Технологічні інструменти другого покоління орієнтовані на передбачення атак, а не лише на їхнє виявлення. Прогностичні моделі використовують не лише дані про фейки, а й метрики поведінки користувачів: частоту взаємодії, зміни емоційних патернів, появу нових тем, які раніше не існували у публічному дискурсі. Такі системи працюють за принципом “сигналів слабких змін”. Якщо певна тема починає різко збирати увагу в обмежених групах, якщо з’являються синхронні коментарі або повторювані фрази — система сигналізує про потенційний початок координованої операції.

Показовим є досвід НАТО StratCom COE, який у 2023 році опублікував результати дослідження інформаційної динаміки у Східній Європі. Виявлено,

що інформаційні атаки часто мають “зону підготовки”, коли ворожі актори тестують наративи в малих групах. У цей час можна зупинити кампанію ще до її масового розгортання. Системи прогнозування дозволяють визначити такі точки і застосувати превентивні заходи: офіційні коментарі, комунікаційні інструкції, освітні ініціативи або співпрацю з платформами щодо зниження органічного охоплення шкідливого контенту.

Важливим технологічним інструментом стає ідентифікація мережевих структур. Інформаційний тероризм часто побудований на взаємодії тисяч анонімних акаунтів. Традиційні методи аналізу не дозволяють визначити, як саме вони пов’язані. Тому алгоритми графового аналізу — ще один ключовий елемент нових технологій. Вони дають змогу виявляти групи акаунтів, які синхронно поширюють ті самі теми. Наприклад, алгоритм Polaris (розробка University of Stanford) може виділяти ініціаторів кампанії, периферійні групи та центри координації. Це важливо і для України, де російські операції часто приховують центри управління за десятками рівнів фейкових акаунтів.

Графові алгоритми також дозволяють визначати, які саме групи найбільш вразливі до маніпуляцій. Наприклад, польські дослідники виявили, що під час виборів 2023 року деякі групи молоді віком 18–22 роки були надзвичайно чутливими до емоційних наративів про економічний спад. Для таких випадків створюється цільова стратегія комунікації. Це вже не просто протидія фейкам, а психологічне моделювання, що враховує наративні слабкі місця суспільства.

Особливу роль у створенні нових інструментів відіграє коаліційна взаємодія держав, яка об’єднує національні платформи у спільний інформаційний щит. Підрозділ 3.2 показав, що міжнародні організації стали каталізаторами глобальної співпраці. Проте у 2022–2024 роках з’явився новий рівень — коаліції цифрової оборони, які включають не лише держави, а й компанії, університети

та незалежних дослідників. Прикладом є “Counter-Disinformation Coalition”, що виникла після початку війни в Україні. До неї увійшли США, Британія, Польща, Україна, Естонія, а також Google, Microsoft, Meta й кілька аналітичних центрів. Коаліція працює як спільний механізм оповіщення та координації. Коли фіксується ворожа інформаційна хвиля, країни й компанії отримують сповіщення з рекомендаціями, як діяти. Такий формат вперше продемонстрував високу ефективність у відбитті атак на українську систему енергетики у 2022–2023 роках, коли психологічні операції Росії супроводжувалися кібератаками.

Складовою нових інструментів є розвиток цифрової автентичності контенту. У 2022–2024 роках найбільші IT-компанії створили “Content Authenticity Initiative” — систему цифрових водяних знаків і криптографічних підписів, що додаються до фото та відео ще під час їхнього створення. Якщо контент редагували, система це показує. Такий підхід особливо важливий у часи глибинних фейків, коли відео зі зміною голосу чи обличчя може викликати паніку, про що йшлося у підрозділах 1.4 та 2.4. Ця технологія дозволяє державам і журналістам швидко перевіряти оригінальність матеріалів і зменшувати вплив візуального терору.

Іншою перспективною технологією є створення стійких до маніпуляцій інформаційних систем. Це включає розробку спеціальних алгоритмів, які зменшують можливість “емоційних вибухів” у соціальних мережах. Наприклад, Google тестує механізми уповільнення поширення контенту, що викликає масову реакцію, щоб уникнути миттєвого поширення паніки. Аналогічну практику використовує TikTok, коли платформа сповільнює поширення відео, які набирають популярність занадто швидко і без органічних причин. Ці інструменти створюють версію “дигітальної вентиляції” — штучного уповільнення натовпової реакції.

У рамках нових інструментів формується ще один напрям — алгоритми контрнаративів. Вони аналізують структуру фейкового наративу й автоматично пропонують найефективніші моделі спростування. Дослідження, проведене Університетом Кембриджа у 2023 році, показало, що деякі форми спростування (наприклад, пряме заперечення) лише підсилюють хибну інформацію. Натомість пояснювальні моделі або “інокуляційні” стратегії, які попереджають про можливу маніпуляцію, є значно ефективнішими. Штучний інтелект може визначати, який саме тип комунікації працюватиме для конкретної аудиторії.

Ці інструменти активно впроваджуються в Україні. Центр протидії дезінформації тестує алгоритми автоматичного аналізу російських наративів. У 2023–2024 роках Україна розробляє власну систему протидії deepfake-загрозам, а також випробовує інструменти прогнозування наративних хвиль. Значну роль відіграють приватні компанії. Українські ІТ-фахівці створюють системи моніторингу Telegram — платформи, де традиційні алгоритми великих корпорацій не працюють. Український досвід стає прототипом для інших країн, що зазнають інформаційного тиску.

Однак розвиток технологічних інструментів викликає дискусію щодо ризиків їхнього використання. Головна проблема — можливість перетворення технологій на засіб прихованого контролю над суспільством. Якщо держави використовують системи аналізу поведінки без прозорих рамок, це загрожує порушенням прав громадян. Особливо чутливим є питання алгоритмічного моделювання настроїв, яке може застосовуватися як інструмент політичної мобілізації або маніпуляції. Цей ризик особливо помітний у практиках авторитарних держав, де інформаційна безпека використовується для придушення опозиції. Саме тому підрозділ 3.3 наголошує на ключовій різниці між демократичним і авторитарним підходами. Демократичні держави будують політику на партнерстві та прозорості. Авторитарні — на контролі та цензурі.

Ще один ризик стосується приватних корпорацій. Алгоритми, створені технологічними гігантами, здатні змінювати інформаційну динаміку в масштабах, які більші за вплив держави. Коли компанії володіють даними мільярдів користувачів, вони отримують можливість впливати на інформаційний порядок денний. Це формує нову форму сили, яку в соціології називають “алгоритмічною владою”. Якщо корпорації стають ключовими партнерами держав, з’являється ризик надмірної залежності держави від приватних інтересів. Це особливо актуально для країн, які не мають власних великих платформ і змушені покладатися на компанії США чи Китаю.

Важливим завданням сучасної політики є створення етичних і правових механізмів контролю над використанням технологій. Європейський Союз робить ставку на принцип “технологічної відповідальності”. Це означає, що будь-яка система, здатна впливати на громадську думку, повинна бути прозорою щодо своїх алгоритмів, джерел даних та механізмів модерації. Вперше такі вимоги закріплені в Європейському акті про штучний інтелект. Він встановлює класи ризику для різних технологій. Політична маніпуляція, психологічний таргетинг і системи соціального рейтингу розглядаються як неприйнятні або високоризикові. Це означає, що їх використання суворо обмежене або заборонене.

Україна рухається у цьому напрямі. У 2024 році Міністерство цифрової трансформації працює над рамковим законом про штучний інтелект, який гармонізуватиметься з європейським. Це дозволить Україні включитися до загальноєвропейської системи стандартів. Такі стандарти допоможуть уникнути ризиків надмірного контролю та забезпечити захист прав громадян, що є ключовою умовою демократичної стійкості. У підсумку нові технологічні інструменти становлять лише частину ширшої системи інформаційної безпеки. Вони мають розглядатися у зв’язку з міжнародними механізмами (3.1), діяльністю міжнародних організацій (3.2), політикою держав (3.3) та структурою

сучасних загроз (розділ 2). Протидія інформаційному тероризму — це не окремі дії, а взаємопов'язані процеси, які формують нову архітектуру світової безпеки. Саме технології дозволяють державам переходити від хаотичного реагування до системного управління ризиками. Проте без етичних рамок, партнерств та довіри вони можуть перетворитися на інструмент контролю, що суперечить демократичним цінностям. Одним із ключових трендів є поява глобальних алгоритмічних систем реагування. Це механізми, які працюють не в межах окремої держави чи регіону, а на рівні міждержавних мереж. Вони створюються у співпраці між міжнародними організаціями, технологічними компаніями та урядами. Платформи більше не є автономними структурам. Вони перетворилися на елемент глобальної безпеки, а отже — на об'єкт політичних зобов'язань.[56,57,58,59,60,61,62,63,64]

РОЗДІЛ IV

Практичні аспекти інформаційного простору

4.1. Україна у глобальній системі протидії інформаційному тероризму

Україна є однією з небагатьох держав світу, яка протягом тривалого часу існує у стані постійного інформаційного терору. Інформаційні атаки проти української державності почалися задовго до 2014 року, але саме після початку російської агресії вони набули системного, комплексного характеру. Росія, маючи значні фінансові, технологічні та організаційні ресурси, створила унікальну систему гібридного впливу, яка поєднує інформаційні операції з політичним тиском, економічними заходами, військовими діями та психологічним впливом на населення. Унаслідок цього Україна опинилася не лише на полі бою, а й у центрі глобальної боротьби за інформаційну безпеку. Саме тому український досвід

став однією з найважливіших моделей протидії сучасному інформаційному тероризму. Він визначає нові стандарти стійкості, створює прецеденти міжнародної взаємодії і формує підходи, які сьогодні застосовують інші держави. Україна фактично стала лабораторією сучасної інформаційної війни, де перевіряються інструменти, підходи та алгоритми, що визначатимуть майбутню архітектуру глобальної безпеки.

Після 2014 року українська інформаційна політика почала формуватися у кризових умовах. Держава опинилася перед ситуацією, коли інформаційний терор був не супутнім елементом конфлікту, а його центральною складовою. Росія використовувала всі доступні канали: державні телеканали, соціальні мережі, бот-мережі, псевдоаналітичні ресурси, мережеві агентури та велику кількість фейкових громадських рухів. Метою було створення хаосу, підрив довіри до української влади, дискредитація української армії та формування у населення відчуття неминучої поразки. Саме цей психологічний компонент став ключовим елементом атаки, описаним у підрозділах 1.4 та 2.4. Російські операції будувалися на принципі “втоми та деморалізації”, що збігається з підходами інформаційного терору, описаними дослідниками НАТО, ЄС та незалежними експертами.

У відповідь Україна почала створювати власну систему інформаційної оборони. Спочатку вона була фрагментованою, але поступово стала більш координованою. Важливою віхою стало ухвалення у 2016 році Доктрини інформаційної безпеки України. У цьому документі вперше було офіційно визнано, що інформаційні операції Росії становлять екзистенційну загрозу, і що держава повинна створити власні механізми протидії. Доктрина визначила пріоритети державної політики, включно з необхідністю створення спеціалізованих структур, гармонізації законодавства, співпраці з міжнародними партнерами й розвитку інформаційної стійкості суспільства.

Одним з найважливіших органів стала Рада національної безпеки і оборони України. Її роль у сфері інформаційної безпеки зростала протягом 2016–2025 років. РНБО координує дії державних структур, забезпечує міжвідомчу взаємодію, формує стратегічні документи й виконує функції кризового реагування. Саме РНБО ініціювала значну частину санкцій проти російських медіаресурсів, платформ та структур, які працювали як елементи інформаційного терору. Санкції проти телеканалів, пов'язаних з російськими спецслужбами, стали одним з ключових рішень, що зменшили можливість Росії впливати на внутрішній дискурс України.

У 2021 році Україна створила один із найбільш важливих органів у сфері інформаційної політики — Центр протидії дезінформації при РНБО. Цей центр став платформою для аналітики, моніторингу та стратегічної комунікації. Він аналізує структуру дезінформаційних атак, систематизує дані про російські наративи, взаємодіє з платформами та іноземними інституціями й публікує спростування та аналітичні матеріали. Його робота ґрунтується на стандартах НАТО StratCom COE та Європейської служби зовнішньої дії, що підкреслює інтеграцію України у глобальну систему інформаційної безпеки.

Окрему роль відіграє Служба безпеки України. Інформаційні операції Росії включають кіберзлочинність, мережеве проникнення, спроби впливу на критичну інфраструктуру, а також діяльність агентурних груп. СБУ стала центром протидії цим загрозам. Після 2014 року було створено нові підрозділи з кібербезпеки та інформаційно-аналітичної роботи, які тісно співпрацюють з міжнародними партнерами — НАТО Cooperative Cyber Defence Centre of Excellence, кіберпідрозділами США, Польщі, Естонії та Німеччини. Досвід України перетворився на основу для нових принципів колективної оборони у кіберта інформаційній сферах.

Важливою особливістю української моделі є її громадсько-державний характер. Інформаційна безпека не може будуватися лише державою, і це стало очевидним ще у 2014 році. Саме громадянське суспільство, волонтерські спільноти, аналітичні центри та незалежні фактчекінгові організації стали першою лінією оборони. Такі проєкти, як StopFake, VoxCheck, Texty.org.ua, Detector Media та інші, виконували роботу, яку у деяких країнах виконують державні агентства. Вони аналізували російські наративи, роз'яснювали фейки, проводили тренінги для журналістів і громадян. Згодом держава інтегрувала їх у свою систему, і сьогодні Україна має одну з найбільш розвинених моделей співпраці між громадськістю та державою у сфері цифрової стійкості.

Українська модель протидії інформаційному тероризму має ще одну унікальну характеристику — інформаційну мобілізацію суспільства. Під час повномасштабного вторгнення у 2022 році українці створили тисячі волонтерських інформаційних ініціатив, від локальних Telegram-груп до міжнародних проєктів у соціальних мережах. Ці ініціативи виконували функцію швидкого оповіщення, спростування фейків та координації дій. Вони стали стихійною, але неймовірно ефективною частиною інформаційної оборони. Соціальна солідарність стала одним з ключових факторів інформаційної стійкості — те, що не може бути створене штучно в інших країнах.

Ще один важливий аспект — розвиток нормативно-правової бази. Після 2014 року Україна ухвалила низку законів, спрямованих на захист інформаційного простору: закон про кібербезпеку, закон про національну безпеку, закон про санкції, закон про медіа. Ці документи стали основою для регулювання діяльності платформ, роботи медіа та співпраці з міжнародними організаціями. Особливо важливим є закон про медіа 2023 року, який гармонізує українське законодавство із законодавством ЄС. Він встановлює нові стандарти прозорості, відповідальності та медіарегулювання, що є важливою умовою євроінтеграції [9]. Однак нормативні акти не були б ефективними без сучасної інституційної

моделі. Міністерство цифрової трансформації, створене у 2019 році, відіграє надзвичайно важливу роль у розвитку цифрової стійкості України. Його програми цифрової грамотності, проєкти взаємодії з платформами і національні системи комунікації (зокрема, інформаційні кампанії під час криз) стали частиною інфраструктури інформаційної безпеки. У співпраці з ЄС та НАТО Україна розвиває державні цифрові платформи, здатні протидіяти дезінформації, зокрема платформу "Дія.ЄОсвіта" та іншу інфраструктуру цифрових комунікацій .

Міжнародна підтримка відіграє фундаментальну роль. Після 2014 року Україна стала стратегічним партнером НАТО у сфері інформаційної та кібербезпеки. Програми НАТО Trust Fund та проєкти StratCom COE надали Україні аналітичні інструменти, обладнання та методологічну допомогу. Європейський Союз координує підтримку України через East StratCom Task Force, яке аналізує російські пропагандистські кампанії. ООН, ОБСЄ та Рада Європи проводять програми навчання для українських журналістів та державних службовців. Це допомагає Україні інтегруватися у світову систему колективної безпеки [11]. Особливо вагомим є міжнародне визнання того, що Україна стала ключовою ланкою у глобальній системі протидії російському інформаційному терору. Досвід України використовують країни Європи для підготовки до можливих атак. Польща, Литва, Латвія та Естонія інтегрували українські методики виявлення наративів у свої системи інформаційної стійкості. Німеччина використовує українські моделі аналізу Telegram-мереж, які довели свою ефективність. США у 2023–2024 роках співпрацювали з українськими аналітиками для вивчення російських deepfake-кампаній.

Феномен української інформаційної стійкості привертає увагу дослідників. Багато аналітичних центрів, включно з RAND, Atlantic Council, NATO StratCom COE та Freedom House, відзначили у своїх звітах, що українська модель базується на унікальному поєднанні трьох факторів: державної координації,

громадянської мобілізації та міжнародної підтримки. Це створює стійкість, яка перевищує можливості окремих технологічних чи політичних інструментів. Україна продемонструвала, що чесна комунікація та прозорість — сильніші за пропаганду і маніпуляції, навіть якщо останні мають величезні ресурси [13]. Важливою складовою є інформаційна дипломатія України. Після 2022 року вона стала невід'ємною частиною зовнішньої політики. Україна змогла створити глобальний інформаційний консенсус щодо природи російської агресії. Українські офіційні джерела, дипломатичні канали, медійні інтерв'ю та соціальні мережі стали інструментами формування глобального розуміння війни. Це дозволило Україні отримати підтримку ЄС, НАТО, країн G7 та багатьох інших держав. Українські комунікаційні стратегії стали прикладом того, як держава може ефективно поєднувати дипломатію, інформаційну політику та технології.

Уроки 2014–2025 років показують, що інформаційна стійкість України має кілька системних характеристик. Перша — здатність до швидкого реагування. Друга — здатність до децентралізованої взаємодії між державою і громадянським суспільством. Третя — психологічна адаптованість суспільства. Українці навчилися не піддаватися паніці, розрізняти маніпулятивні повідомлення, довіряти перевіреним джерелам. Це стало результатом восьми років інформаційної боротьби, яка підготувала суспільство до повномасштабного вторгнення. У 2022–2025 роках українська інформаційна модель стала ще більш структурованою. Було створено нові аналітичні центри, інтегровано європейські стандарти, активізовано співпрацю з платформами. Україна також стала учасником багатьох міжнародних програм з інформаційної та кібербезпеки. Її досвід враховується у документах ЄС, НАТО та ООН, що стосуються стратегічних комунікацій, боротьби з дезінформацією та захисту цифрового середовища.

Завдяки цій взаємодії Україна стала однією з найважливіших ланок глобальної системи протидії інформаційному тероризму. Вона не лише отримує підтримку,

а й надає експертні знання, аналітику та досвід. Українські фахівці беруть участь у тренінгах НАТО, консультаціях для країн ЄС, міжнародних конференціях і дослідницьких програмах. Це формує нову роль України — не просто об’єкта інформаційної війни, а суб’єкта, який активно впливає на формування світових стандартів безпеки.[65,66,67,68,69,70,71,72]

.

4.2. Порівняльна оцінка ефективності міжнародних стратегій

У XXI столітті міжнародна система безпеки переживає трансформацію, у центрі якої перебуває проблема інформаційного тероризму. Держави розробляють різні моделі протидії, що залежать від історичного досвіду, політичної культури, технологічних можливостей і рівня загроз, на які вони реагують. Саме порівняння стратегій різних країн дає змогу оцінити, які підходи виявляються найбільш результативними в умовах сучасних конфліктів. Аналіз моделей Європейського Союзу, США, Ізраїлю та Естонії демонструє різні шляхи побудови інформаційної стійкості, але також виявляє спільні тенденції, які формують новий міжнародний стандарт у боротьбі з інформаційним терором. Порівняльний підхід дозволяє побачити, як ці стратегії можуть бути адаптовані до українського контексту, і чому українська модель, розглянута у підпункті 4.1, поступово стає частиною глобальної архітектури інформаційної безпеки.

Європейський Союз формує найбільш комплексну і нормативно визначену модель боротьби з інформаційними атаками. Після втручання Росії у вибори в ЄС та США у 2016 році Європейська Комісія ухвалила низку документів, що стали основою для сучасної концепції інформаційної стійкості. Серед них слід виділити Кодекс практик із протидії дезінформації, Digital Services Act та ініціативу East StratCom Task Force. Європейський формат передбачає поєднання правового регулювання, саморегуляції платформ і активної участі громадянського суспільства. Ця модель характеризується чіткими юридичними рамками, широкою мережевою співпрацею і високими стандартами прозорості. Вона створена не для контролю інформації, а для її структурованого захисту. Важливо, що ЄС намагається уникати надмірних обмежень свободи слова. Саме тому юридичні інструменти поєднуються з механізмами незалежної модерації контенту і добровільних зобов'язань платформ. Це робить європейську модель однією з найбільш збалансованих у світі.

Однак слабким місцем є повільність прийняття рішень. Система ЄС включає багато етапів погодження між інституціями і державами-членами, що може затримувати оперативне реагування на інформаційні атаки. Росія та Китай використовують такі затримки, запускаючи швидкі хвилі дезінформації, які поширюються швидше, ніж демократичні механізми встигають реагувати. У підсумку ЄС створює стратегічну, але не завжди достатньо оперативну модель реагування. Проте її сильним боком є масштабність, нормативність і можливість формування глобальних стандартів інформаційної безпеки.

США використовують іншу модель, яка базується на силі технологічного сектору, потужних розвідувальних можливостях та інституційній перевазі у сфері аналітики. Американський підхід є більш децентралізованим, ніж європейський. У боротьбі з інформаційним терором значну роль відіграють приватні компанії — Meta, Google, Microsoft, Twitter/X. США не прагнуть встановлювати єдину централізовану систему регулювання, натомість

використовують гібридний формат взаємодії між державою та технологічним сектором. Це дозволяє реагувати на загрози швидко і технологічно, але створює проблеми з прозорістю та підзвітністю. Після подій 6 січня 2021 року питання про необхідність більш жорсткого регулювання цифрових платформ стало предметом політичної дискусії, але досягти єдиного підходу так і не вдалося.

Американська модель має значну аналітичну перевагу. Організації, такі як Cybersecurity and Infrastructure Security Agency, National Security Agency та інші структури, включно з RAND Corporation і Atlantic Council, створюють детальні моделі інформаційних загроз. Це дозволяє США прогнозувати операції Росії, Китаю та Ірану з високою точністю. У цьому полягає її сила: США здатні ідентифікувати загрози ще до того, як вони стануть масовими. Але слабкість полягає у відсутності єдиного державного механізму модерації або контролю інформаційного простору. США є однією з небагатьох держав, де приватні компанії мають більший вплив на інформаційний простір, ніж держава. Це створює ризики, оскільки технологічні компанії не завжди мають чіткі зобов'язання перед суспільством у питаннях безпеки.

Ізраїль формує одну з найбільш агресивних і технологічно розвинених моделей протидії інформаційним атакам. На відміну від ЄС та США, його політика базується на принципі повної інтеграції інформаційної безпеки у національну оборону. Інформаційні операції розглядаються як фактор, який може спричинити фізичну шкоду громадянам, тому Ізраїль застосовує модель "інформаційного парасолькового захисту". Вона передбачає централізовану координацію між військовими, розвідувальними службами та цивільними агентствами. Ізраїль активно використовує технології штучного інтелекту, біометричний аналіз поведінки, моделі психологічного прогнозування і кіберрозвідку. Це робить його одним із світових лідерів у сфері інформаційної оборони [5]. Проте ізраїльська модель має й обмеження. Вона є високорегульованою і вимагає контролю над інформаційним простором, що не завжди відповідає демократичним стандартам.

Жорсткі інструменти можуть спричиняти критику з боку правозахисних організацій, але Ізраїль вважає їх необхідною умовою національної безпеки, оскільки загроза терору є постійною та багатовекторною.

Естонія є прикладом держави, яка формує свою інформаційну політику через розвиток цифрової інфраструктури і суспільної участі. Після масованих атак 2007 року Естонія створила модель, яка поєднує кібербезпеку, цифрову ідентифікацію, системну освіту і соціальну солідарність. Її стратегія базується на тому, що інформаційний простір є елементом суверенітету. Естонська модель унікальна тим, що держава і суспільство є одним цілим у питаннях цифрової безпеки. Естонія першою у світі створила кібердобровольчі сили. Це доводить, що суспільна мобілізація може бути ключовим елементом протидії інформаційному тероризму. Естонська модель відрізняється також високим рівнем прозорості і довіри, що є важливою умовою для формування стійкості.

Цікаво, що країни з найуспішнішими моделями протидії інформаційному тероризму мають різні політичні системи та історичні досвіди. ЄС побудував нормативну систему, спрямовану на баланс між свободою слова і безпекою. США використовують технологічну перевагу і приватний сектор як основу системи. Ізраїль бачить інформацію як частину війни і інтегрує її у національну оборону. Естонія робить ставку на цифрову культуру і громадську участь. Саме ця різноманітність дає можливість створити глобальну модель, у якій різні підходи поєднуються у рамках колективної системи безпеки.

Особливо важливо оцінити місце України у цьому контексті. Хоча Україна не входить до ЄС або НАТО станом на 2025 рік, її стратегія інформаційної оборони все більше зближується з моделями цих структур. Україна запровадила стандарти стратегічних комунікацій НАТО, адаптувала європейські норми медіарегулювання та використовує американські методики аналізу

інформаційних операцій. Таким чином, українська модель перетворюється на гібридний формат, який поєднує елементи різних систем і водночас базується на власному досвіді тривалої боротьби з інформаційним терором. Порівнюючи ці моделі, можна виділити кілька ключових критеріїв ефективності. Перший — оперативність реагування. США та Ізраїль мають перевагу у швидкості дій. ЄС реагує повільніше через багаторівневу систему ухвалення рішень. Естонія та Україна вирізняються середнім рівнем оперативності, але компенсують це високою соціальною мобілізацією. Другий критерій — технологічна спроможність. США, Ізраїль та Естонія мають найрозвиненіші цифрові інфраструктури. ЄС має великий ресурс, але технологічно залежить від приватного сектору. Україна демонструє високий рівень адаптивності, хоча її ресурси обмежені війною. Третій критерій — соціальна стійкість. Тут лідерами є Естонія та Україна. Їхні суспільства мають високий рівень медіаграмотності, довіри до інституцій та здатності до самоорганізації. Четвертий критерій — нормативна інтегрованість. ЄС формує найпотужнішу правову базу, тоді як США та Ізраїль діють через гнучкі механізми. Україна швидко адаптує європейське законодавство і поступово інтегрується у західні стандарти. П’ятий критерій — масштабність. США та ЄС володіють найбільшими ресурсами для глобального протистояння інформаційному терору. Ізраїль та Естонія компенсують обмеженість ресурсів високим технологічним рівнем. Україна має обмежені ресурси, але її стратегічна роль зростає, оскільки вона є головним об’єктом атак і водночас джерелом унікального досвіду.

Порівняльний аналіз демонструє, що всі держави стикаються з однією й тією ж проблемою — зростанням складності інформаційних операцій. У підрозділі 3.4 було показано, що сучасні атаки використовують штучний інтелект, психологічне моделювання, гейміфікацію, соціальну інженерію та мультиплатформні алгоритми. Це створює умови, за яких традиційні методи протидії стають недостатніми. Саме тому країни намагаються створити нові формати співпраці та інтеграції. ЄС працює над системою спільного аналізу ризиків, США розвивають механізми партнерства з технологічним сектором,

Ізраїль інтегрує штучний інтелект у військові структури, а Естонія вдосконалює цифрову ідентифікацію як бар'єр проти інформаційних атак. Україна, зі свого боку, впроваджує комплексну модель, яка базується на поєднанні інституційної координації, суспільної солідарності та міжнародної інтеграції.

Особливо показовим є те, як різні країни оцінюють загрозу з боку Росії. ЄС і США розглядають її як головне джерело зовнішніх інформаційних атак. Ізраїль менше концентрується на Росії, але аналізує її методи. Естонія та Україна стикаються з російськими атаками щодня, що робить їхні моделі найбільш "польовими" та адаптивними. Цей досвід дозволяє їм створювати методики, які згодом використовують інші країни. Після 2022 року Естонія і Польща активно застосовують українські підходи до моніторингу Telegram-мереж. Це демонструє, що українська модель вже не є локальною. Вона впливає на формування нових міжнародних стандартів інформаційної безпеки.

У глобальному вимірі стає очевидним, що ефективна стратегія боротьби з інформаційним терором потребує поєднання чотирьох компонентів. Перший — технологічна спроможність. Другий — правове регулювання. Третій — суспільна довіра та медіаграмотність. Четвертий — міжнародна координація. Жодна держава не здатна самостійно протистояти інформаційному терору, оскільки атаки є мультиплатформними, транснаціональними і психологічно адаптивними. У цьому контексті роль України стає все більш важливою. Саме її досвід дозволяє будувати моделі, які враховують найсучасніші інструменти інформаційних атак, описаних у підрозділах 2.3 та 3.4.

У підсумку перша частина аналізу демонструє, що моделі ЄС, США, Ізраїлю та Естонії мають різні сильні сторони та різні обмеження. ЄС забезпечує нормативну стабільність. США — технологічну динаміку. Ізраїль — оборонну інтеграцію. Естонія — цифрову культуру та суспільну мобілізацію. Україна — унікальний досвід ведення тривалої інформаційної війни. Порівняння цих

моделей дозволяє визначити, як можна створити міжнародну систему інформаційної безпеки, здатну реагувати на загрози XXI століття.

Порівнюючи моделі Європейського Союзу, США, Ізраїлю, Естонії та України, можна виявити системні закономірності, які визначають ефективність державних стратегій протидії інформаційному тероризму. Друга частина аналітичного огляду зосереджується на структурних обмеженнях, ризиках і можливостях розвитку цих стратегій, а також на тому, яким чином вони можуть бути інтегровані у єдину міжнародну систему. Цей підхід дозволяє визначити оптимальні напрями для майбутньої глобальної архітектури інформаційної безпеки, що стає особливо важливим з урахуванням інтенсивного впливу технологій, які описані у підрозділі 3.4, та ускладненням інформаційних операцій, проаналізованих у розділі 2.

Ефективність міжнародних стратегій багато в чому залежить від здатності держав не лише реагувати на загрози, а й передбачати їх. Саме у цьому аспекті проявляється різниця між США та Європейським Союзом. Американська модель орієнтується на прогностичні інструменти, які створюють великі технологічні компанії в партнерстві з державними структурами. Їхні системи аналізу інформаційних потоків використовують машинне навчання, великі дані, алгоритмічний аналіз поведінки користувачів і багаторівневий моніторинг цифрових платформ. Це дозволяє США ідентифікувати нові загрози на ранніх етапах. Наприклад, втручання Росії у вибори 2020 року було частково локалізовано через швидку взаємодію між Facebook, Google та американськими спецслужбами, що свідчить про ефективність гібридного підходу. Однак ця модель має обмеження, оскільки рівень автономії приватних платформ не завжди дозволяє державі контролювати інформаційний простір. Відсутність єдиної нормативної бази ускладнює формування системи відповідальності, що створює ризики як для демократії, так і для безпеки.

Європейський Союз демонструє ефективність у сфері нормативного регулювання, але часто втрачає швидкість реагування через надмірно бюрократичну структуру. Створення Кодексу практик із протидії дезінформації стало важливим кроком у формуванні транснаціональної системи відповідальності платформ. Digital Services Act заклав основи нової моделі взаємодії між державами-членами та цифровими компаніями. Проте ЄС усе ще стикається з проблемою, коли загрози поширюються значно швидше, ніж ухвалюються рішення. Російські та китайські інформаційні операції використовують слабкі місця європейської багаторівневої структури. Затримки у реагуванні часто призводять до того, що інформаційні хвилі встигають вплинути на громадську думку до того, як ЄС здійснює офіційні дії. Це демонструє, що навіть найкраща нормативна база не може повністю компенсувати відсутність оперативної мобільності.

Ізраїльська модель, навпаки, є максимально швидкою, проте її застосування обмежене політичними й культурними особливостями країни. Високий рівень централізації дозволяє Ізраїлю блокувати ворожі інформаційні кампанії ще на початкових етапах. Його кіберпідрозділи мають право негайно втручатися у цифрові процеси, що забезпечує короткий час між виявленням загрози і діями у відповідь. Ізраїль також використовує технології штучного інтелекту для моніторингу соціальних мереж, ідентифікації мереж ботів і створення “психологічних карт” населення. Такий рівень втручання забезпечує високу ефективність у сфері безпеки, але викликає побоювання щодо меж приватності. Це обмежує можливість імплементації ізраїльської моделі у європейські країни, які зосереджені на захисті прав людини.

Естонія продемонструвала, що невелика держава може створити надзвичайно ефективну систему інформаційної стійкості завдяки цифровій культурі населення. Естонська модель вирізняється тим, що її основою є не тільки технологічні рішення, а й соціальна згуртованість. Після атак 2007 року Естонія

зробила висновок, що суспільство має бути частиною оборонної системи. Створення кібердобровольчих сил стало однією з найбільш інноваційних практик у сфері інформаційної безпеки. Естонія надає особливу увагу освіті, що сприяє формуванню відповідального інформаційного простору. Але її успішність частково залежить від розміру держави і високого рівня цифрової довіри. Цю модель складно перенести до країн, де довіра до інституцій є нижчою, а суспільство більш поляризоване.

Україна становить окремий випадок у глобальному порівняльному аналізі. Українська модель формувалася під тиском реальної війни, що зробило її унікальною. Інформаційний терор, спрямований проти України, є системним, жорстким і спрямованим на руйнування державності. Тому українська стратегія має адаптивний характер. Вона поєднує елементи американської технологічної аналітики, європейського нормативного регулювання, ізраїльської безпекової інтеграції та естонської соціальної мобілізації. Це робить українську модель гібридною і водночас гнучкою. Вона постійно вдосконалюється, оскільки загрози швидко змінюються. Українські аналітичні центри розробляють нові методики моніторингу пропаганди, які потім використовують інші держави. Прикладом є аналіз Telegram-мереж, що став новим напрямом у дослідженнях інформаційної безпеки.

Україна також демонструє високу стійкість у співпраці з міжнародними організаціями. Участь у проєктах НАТО, ЄС, ОБСЄ та ООН дозволила Україні інтегрувати свої моделі у глобальні підходи. Важливим аспектом є взаємне навчання: не лише Україна переймає досвід інших країн, а й інші держави залучають українських фахівців для аналізу російських методів. Це підтверджує, що українська модель інформаційної безпеки стала глобально релевантною. Держави Європи, зокрема Польща, Литва і Німеччина, використовують український досвід у боротьбі з пропагандою, що демонструє синергетичний ефект між Україною та її партнерами.

Якщо порівнювати системи управління інформаційною безпекою, видно, що їхня ефективність пов’язана із здатністю координувати різні інституції. США мають потужні аналітичні агентства, але проблему становить відсутність масштабної централізації. ЄС має високу нормативність, але низьку швидкість. Ізраїль має високий рівень координації, але обмежений у застосуванні демократичних стандартів. Естонія має ідеальну внутрішню інтеграцію, але обмежену можливість впливати на глобальну політику. Україна, незважаючи на обмежені ресурси, демонструє високий рівень ефективності завдяки поєднанню державної координації та громадської активності. Система, у якій Рада національної безпеки і оборони, Центр протидії дезінформації та Служба безпеки України працюють у зв’язці з волонтерськими організаціями та журналістськими інституціями, є прикладом динамічної, багаторівневої моделі оборони [18]. У цьому контексті надзвичайно важливим є питання етичних меж державної політики. США та ЄС роблять акцент на захисті свободи слова, що сповільнює їхні реакції, але забезпечує довгострокову стабільність демократії. Ізраїль застосовує жорсткі інструменти, але часто стикається з критикою щодо порушень прав людини. Естонія зберігає баланс, але її модель неможливо масштабувати без відповідної культури довіри. Україна, яка перебуває у стані війни, змушена обмежувати російські платформи і канали, але при цьому намагається уникати надмірної цензури. Це складний компроміс. Однак міжнародні партнери визнають, що українські обмеження є пропорційними до загрози. Саме тому українська політика не сприймається як порушення свободи слова на міжнародному рівні.

Порівняння показує, що держави з високим рівнем інформаційної стійкості поділяють одну спільну рису — розуміння того, що інформаційна безпека є питанням національного виживання. Це особливо актуально для Естонії та України, але також стає важливим і для країн ЄС, які зазнають постійних інформаційних атак. Сучасні загрози не є локальними. Інформаційні операції

мають транснаціональний характер. Вони поширюються миттєво і не визнають кордонів. Тому жодна держава не може ефективно боротися з ними самостійно. Потреба у міжнародній координації сьогодні є очевидною. Держави розуміють, що їхні національні моделі повинні стати частиною глобальної системи.[73.74,75,76,77,78,79,80,81,82,83]

4.3. Рекомендації щодо вдосконалення політики України

Сучасна інформаційна безпека України є результатом складного та довготривалого процесу адаптації державних інституцій, медіасистеми, цифрової інфраструктури та суспільства до умов постійного інформаційного терору. Досвід, отриманий у період 2014–2025 років, показав, що ефективність державної політики залежить не лише від технічної спроможності чи правової

бази, але й від здатності держави формувати довіру, забезпечувати відкритість та вибудовувати системну взаємодію між усіма учасниками інформаційного простору. Війна створила унікальне середовище, у якому інформаційні загрози змінюються швидко, а суспільство постійно перебуває під впливом психологічних операцій, що вимагає від держави гнучкої та адаптивної політики.

Рекомендації щодо вдосконалення політики України повинні виходити з аналізу світових моделей, які були розглянуті у підпункті 4.2, а також на основі досвіду України, який докладно описано в підпункті 4.1. Ключовим викликом залишається питання, як Україна може інтегрувати найкращі міжнародні практики, зберігаючи при цьому власну унікальність та враховуючи контекст війни. Важливо усвідомлювати, що рекомендації мають не лише теоретичний характер, а й практичну спрямованість. Вони повинні забезпечити державі здатність протистояти сучасним інформаційним атакам, підвищити рівень інформаційної стійкості населення та сформувати підходи, які будуть релевантними для повоєнного розвитку.

Найважливішим напрямом удосконалення є створення цілісної та інтегративної моделі інформаційної безпеки. На сьогодні інформаційна політика України складається з кількох блоків: державна комунікація, регулювання медіа, діяльність силових структур, цифрова грамотність, співпраця з міжнародними партнерами та участь громадянського суспільства. Кожен із цих блоків важливий, але проблема полягає у недостатній координації. Різні органи дублюють функції або діють паралельно. Це частково зменшує ефективність державної політики. Загрози, що надходять з боку Росії, мають комплексний характер і потребують взаємодії між усіма інституціями без винятку. Тому Україна повинна поступово перейти до створення національної системи інформаційної безпеки, що базується на спільних стандартах, централізованій координації та децентралізованій реалізації.

Важливо, щоб ця система враховувала особливості сучасних інформаційних операцій, які описані у підрозділах 1.3 та 1.4. Інформаційні атаки дедалі більше використовують штучний інтелект, психологічне моделювання, мережеву сегментацію, платформні алгоритми та нейронні технології. Ці інструменти здатні створювати ефекти, які важко помітити у традиційних системах моніторингу. Тому державна політика має включати розробку нових методик аналізу цифрових платформ із використанням алгоритмів прогнозування, автоматичного виявлення маніпулятивних патернів та аналізу поведінкових відхилень. Україна вже робить перші кроки у цьому напрямі завдяки діяльності Центру протидії дезінформації та низки громадських проєктів, але потрібна систематизація цих зусиль і створення єдиного технічного стандарту для аналізу інформаційних операцій [2]. Другим важливим напрямом удосконалення є формування стійкої стратегії державної комунікації. У період активних бойових дій державна комунікація стала одним із найважливіших інструментів стабілізації суспільства. Вона включає офіційні брифінги, повідомлення у соціальних мережах, пояснювальні кампанії та протокол кризового реагування. Україна показала високу ефективність у створенні оперативних повідомлень, що дозволили зменшити вплив паніки та запобігти дезінформаційним хвилям. Проте післявоєнний період вимагатиме не лише оперативної, а й довгострокової комунікаційної політики. Вона повинна забезпечувати довіру громадян до держави, пояснювати реформи, створювати інформаційні бар'єри проти фейків і формувати культуру критичного мислення.

Одним із ключових викликів є потреба у підсиленні інституційної координації. Рада національної безпеки і оборони відіграє провідну роль у стратегічному плануванні, але оперативне виконання завдань здійснюють інші органи — Служба безпеки України, Міністерство цифрової трансформації, Міністерство оборони, Центр протидії дезінформації, Національна рада з питань телебачення і радіомовлення. У кожному з цих органів є свої повноваження, але недостатня інтеграція призводить до фрагментарності політики. Сучасні інформаційні загрози потребують створення постійної міжвідомчої структури, що

координуватиме спільні дії, забезпечуватиме обмін даними та здійснюватиме аналітичну підтримку. Важливо, щоб ця структура не дублювала вже існуючі органи, а інтегрувала їхні функції на рівні стратегічного управління [4]. Третім напрямом має стати модернізація нормативно-правової бази. Україна зробила значні кроки у цьому напрямі, імплементувавши європейське законодавство у сфері медіа та кібербезпеки. Закон про медіа 2023 року став важливим етапом у приведенні українського законодавства у відповідність до стандартів ЄС. Проте необхідно продовжувати гармонізацію законодавства з вимогами Digital Services Act, Digital Markets Act та Audiovisual Media Services Directive. Це стосується прозорості медіавласності, відповідальності платформ за дезінформацію, регулювання алгоритмічних рекомендацій та забезпечення правового механізму для міжнародної взаємодії у сфері інформаційної безпеки.

Україна має також забезпечити баланс між безпекою та свободою слова. У період війни держава змушена обмежувати діяльність російських медіа, блокувати канали з ворожими зв’язками та боротися з пропагандою. Такі кроки є необхідними, але після завершення активної фази війни постане питання про відновлення демократичних стандартів. Це потребує поступового переходу до моделі, яка забезпечуватиме ефективний захист інформаційного простору без надмірного втручання у свободу слова. Рекомендації Ради Європи та Європейського Союзу можуть стати основою для такого реформування [6].

Удосконалення політики має також включати розвиток людського капіталу. Підтримка державних службовців, аналітиків, журналістів і працівників платформ повинна стати стратегічним напрямом. Підготовка фахівців з інформаційної безпеки є критично важливою, оскільки сучасні інформаційні операції вимагають не лише технічних знань, а й розуміння психології, соціології, медіалінгвістики та міжнародних відносин. Наприклад, аналіз психологічних механізмів впливу, описаний у підрозділі 1.4, свідчить про те, що інформаційні атаки спираються на емоційні реакції, групову динаміку та

когнітивні спотворення. Фахівці повинні мати навички роботи з такими категоріями, що вимагає створення спеціалізованих освітніх програм.

Україна повинна розвивати систему медіаосвіти. Освіта є фундаментальним елементом стійкості, оскільки інформаційні атаки здебільшого спрямовані на психіку громадян. Підвищення рівня медіаграмотності може зменшити вплив паніки, дезінформації та маніпуляцій. Потрібно формувати критичне мислення не лише у молоді, а й серед дорослого населення. Державні програми цифрової грамотності мають бути спрямовані на різні вікові групи, професійні середовища та регіони. У цій сфері Україна може використати досвід Фінляндії, Естонії та інших європейських країн, які зробили освіту основним елементом інформаційної безпеки [8]. Важливо також сформувати систему співпраці між державою та приватним сектором. У XXI столітті цифрові платформи мають вирішальний вплив на інформаційні потоки. Тому держава не може протидіяти інформаційному терору без партнерства з технологічними компаніями. Україна вже має досвід взаємодії з Google, Meta, YouTube, Microsoft та іншими платформами, але необхідно розширювати і поглиблювати цю співпрацю. Потрібен механізм, який дозволить державі отримувати доступ до аналітичних даних про інформаційні атаки, а платформам — отримувати експертні консультації від українських аналітичних центрів щодо специфіки російських операцій.

Серед стратегічних рекомендацій важливим є розвиток інфраструктури інформаційного моніторингу. Україна вже має розвинену систему аналітичних платформ, але потрібно забезпечити інтеграцію між державними і недержавними структурами. Система моніторингу повинна включати аналіз соціальних мереж, месенджерів, інформаційних каналів, платформ для відеоконтенту, а також аналіз транснаціональних медіа. Особливу увагу потрібно приділяти Telegram, оскільки він став одним з основних інструментів російських інформаційних операцій. Українські аналітичні центри вже мають значний досвід у цьому

напрямі, але потрібно забезпечити постійне фінансування і технічне оновлення систем моніторингу. Ще одним ключовим напрямом є розвиток системи стратегічних комунікацій у секторі оборони. Стратегічні комунікації Збройних Сил України продемонстрували свою ефективність у період війни, але потребують інституційного посилення. Потрібно створити національний центр стратегічних комунікацій, який поєднає можливості державних органів, військових структур та громадських організацій. Такий центр забезпечить єдині стандарти комунікаційної політики, підвищить якість кризових повідомлень та дозволить швидко реагувати на інформаційні атаки . Важливо також забезпечити розвиток міжнародної взаємодії у сфері інформаційної безпеки. Україна вже має значний досвід співпраці з НАТО, ЄС, ОБСЄ та окремими державами, але потрібно розширювати участь у глобальних і регіональних проєктах. Особливо важливим є створення механізмів спільного аналізу загроз, обміну даними між національними агентствами різних держав, а також розробка спільних стандартів відповідальності платформ. Україна може відігравати ключову роль у цих процесах завдяки унікальному досвіду протидії російському інформаційному терору.

Підсумовуючи першу частину рекомендацій, можна зазначити, що удосконалення політики інформаційної безпеки потребує комплексного підходу. Держава повинна забезпечити координацію інституцій, модернізувати законодавство, розвивати людський капітал, підтримувати медіаграмотність, формувати партнерства з платформами та створювати сучасні інфраструктурні рішення. Лише поєднання цих елементів може забезпечити високий рівень стійкості держави перед сучасними інформаційними загрозами. Друга частина підпункту буде зосереджена на перспективних напрямах розвитку, питаннях міжнародної інтеграції, етичних аспектах та довгостроковому баченні української інформаційної політики.

Друга частина рекомендацій зосереджується на стратегічних напрямах, що визначатимуть майбутню трансформацію української політики у сфері

інформаційної безпеки. В умовах тривалого конфлікту інформаційне середовище України піддається безперервним атакам, які стають дедалі складнішими. Технологічні інновації, розвиток штучного інтелекту, мережеві операції, інформаційно-психологічні методи та міжнародна конкуренція за вплив формують ризики, які не можуть бути нейтралізовані старими підходами. Тому Україні потрібна довгострокова стратегія, що не лише відповість на сучасні виклики, а й визначить перспективи розвитку безпечного інформаційного простору у післявоєнний період. Ця стратегія має базуватися на поєднанні технологій, дипломатії, освіти, комунікації, нормативного регулювання та міжнародної взаємодії. Саме інтегративний підхід створить основу для стабільного розвитку і допоможе Україні стати повноправним учасником глобальної системи інформаційної безпеки. Окремої уваги потребує питання інституційної модернізації. Україна вже має низку органів, які відповідають за інформаційну безпеку, але їхня взаємодія потребує подальшого вдосконалення. Потрібно створити постійно діючий координаційний центр, що об’єднає можливості РНБО, СБУ, Міністерства цифрової трансформації, Міністерства оборони, Центру протидії дезінформації та Національної ради з питань телебачення і радіомовлення. Така структура повинна мати широкий мандат і забезпечувати оперативний обмін інформацією, аналітичний моніторинг та стратегічне планування. Рекомендації міжнародних партнерів, зокрема НАТО та ЄС, свідчать про те, що міжвідомча координація є ключовим чинником інформаційної стійкості держави. Приклади успішних моделей в Естонії та Ізраїлі показують, що централізована координація не обмежує свободу слова, якщо поєднується з прозорістю і чітким розподілом повноважень.

Потрібно також реформувати підходи до державної комунікації. У воєнний період Україна змушена застосовувати кризові комунікаційні методи, але у довгостроковій перспективі важливо створити модель, що ґрунтується на відкритості, системності та послідовності. Українське суспільство потребує достовірних повідомлень про ситуацію в країні, реформи, міжнародну політику і наслідки конфлікту. Важливо забезпечити регулярні брифінги, аналітичні

матеріали, пояснювальні кампанії та механізми, які сприятимуть формуванню довіри між громадянами та державою. Міжнародний досвід свідчить, що комунікація відіграє ключову роль у забезпеченні безпеки. Наприклад, у США, країнах ЄС та Канаді уряди активно співпрацюють з журналістами та академічними колами, щоб забезпечити прозорість рішень. Україна може використати ці практики для формування стабільного інформаційного середовища.

Окремий елемент рекомендацій стосується ролі громадянського суспільства. Україна має одну з найактивніших екосистем громадських організацій у сфері боротьби з дезінформацією. Проєкти StopFake, VoxCheck, Texty.org.ua, Detector Media та інші демонструють високий рівень професіоналізму й аналітичної спроможності. Проте їм бракує стабільного фінансування. Держава може створити систему грантів, партнерських програм та механізмів співпраці, які забезпечать сталий розвиток громадських ініціатив. Це дозволить зміцнити горизонтальні структури інформаційної стійкості, які є ключовими у протидії російським інформаційним атакам. Досвід Естонії та країн Скандинавії свідчить про те, що активне громадянське суспільство є необхідним елементом сучасної інформаційної політики.

Наступним важливим напрямом є технологічний розвиток. У підрозділі 3.4 було показано, що нові технології формують нову епоху інформаційних загроз. Штучний інтелект, генеративні моделі, глибинні фейки, автоматизовані ботоферми та алгоритмічні маніпуляції є інструментами, які змінюють характер інформаційних операцій. Україні потрібно створити власні технологічні ресурси для аналізу та нейтралізації таких загроз. Це включає розробку систем автоматичного моніторингу, платформ машинного аналізу, інструментів для виявлення deepfake, систем поведінкового аналізу та технологій ідентифікації ботів. Також важливо створити національні сховища даних, що забезпечать можливість для роботи алгоритмів штучного інтелекту. Важливо, що українські

фахівці вже працюють у сфері технологічної оборони, але для створення повноцінної системи потрібно інвестиції, політична підтримка та співпраця з міжнародними партнерами.

Серйозним викликом залишається питання інформаційної безпеки критичної інфраструктури. Сучасні інформаційні атаки часто спрямовані не лише на дезінформацію, а й на порушення роботи енергетичних систем, транспортних мереж, державних реєстрів та інших критично важливих систем. Україна вже має досвід протидії таким атакам, зокрема атакам на енергетичну інфраструктуру у 2015 та 2016 роках. Проте ризики зберігаються. Потрібно створити систему, яка забезпечить постійний моніторинг та захист критичних об'єктів від інформаційно-кібератак. Ця система має включати сучасні технології, міжнародну кооперацію та навчання персоналу. Безпечна інфраструктура є основою функціонування держави, тому питання її захисту повинно бути у центрі державної політики.

Надзвичайно важливою частиною рекомендацій є розвиток інформаційної дипломатії. Україна вже має вагомі успіхи у цій сфері, але потрібно розширювати її інституційні можливості. Інформаційна дипломатія включає комунікацію з міжнародними партнерами, участь у глобальних дискусіях, пояснення українських позицій у медіа різних країн, а також протидію російській пропаганді на міжнародній арені. Під час війни це стало одним із ключових факторів міжнародної підтримки України. Проте довгострокова інформаційна дипломатія потребує професійного персоналу, стратегічного планування та сучасних комунікаційних методів. Україні слід розвивати спеціалізовані центри комунікації для роботи з міжнародними медіа, аналітичні структури для моніторингу міжнародного дискурсу та програми підготовки дипломатів у сфері інформаційної безпеки.

Суттєвим елементом є також участь України у формуванні міжнародних стандартів. У підпунктах 3.1 та 3.2 було показано, що міжнародні організації активно працюють над створенням механізмів боротьби з дезінформацією. Україна повинна не лише приєднуватися до цих ініціатив, а й впливати на їхній зміст. Досвід України дозволяє оцінювати ефективність заходів, які розробляють у ЄС та НАТО, з урахуванням реального бойового та інформаційного середовища. Тому Україна може пропонувати власні моделі аналізу інформаційних загроз, брати участь у міжнародних робочих групах, розробляти спільні стандарти та створювати ініціативи, спрямовані на формування глобальної інформаційної стійкості.

Одним із найважливіших стратегічних напрямів є розвиток співпраці з цифровими платформами у питаннях модерації та боротьби з дезінформацією. Платформи відіграють вирішальну роль у поширенні інформації. Україна повинна мати можливість впливати на політику платформи, надавати дані про інформаційні атаки, обговорювати алгоритмічні ризики, вимагати прозорості у маркуванні фейків та блокуванні ворожих акаунтів. Потрібно розвивати партнерства, що дозволяють проводити спільні дослідження, обмінюватися аналітичними інструментами та брати участь у формуванні механізмів модерації. Це забезпечить кращий захист українського інформаційного простору та вплине на зміцнення міжнародної системи модерації .

Окремого аналізу потребує питання регіональної політики інформаційної безпеки. Різні регіони України мають різний рівень вразливості до інформаційних атак. Східні області тривалий час зазнавали впливу російських медіа. Південні регіони були під сильним впливом проросійських наративів до 2022 року. Західні регіони мають іншу специфіку через історичний контекст, інформаційні зв’язки з Європою і високий рівень участі громадян у політичних процесах. Тому державна політика повинна враховувати регіональні особливості. Необхідно створити регіональні програми медіаосвіти, локальні

комунікаційні центри, систему локальних медіамоніторингів та програми співпраці з місцевими громадами. Цей підхід дозволить зменшити ризики локальних інформаційних криз і підвищити загальну стійкість держави.

Важливо також враховувати психологічний вимір інформаційної політики. У підрозділі 1.4 було показано, що інформаційні атаки спрямовані на емоції та когнітивні процеси. Вони намагаються створити відчуття страху, безпорадності та невизначеності. Тому психологічні аспекти повинні бути частиною інформаційної політики. Потрібно створити програми підтримки населення у кризових ситуаціях, механізми пояснення складних подій, ресурси для стабілізації суспільних емоцій та психологічної підтримки. Україна повинна розуміти, що психологічна стійкість є такою ж важливою, як і технологічна [22]. Окрему увагу слід приділити механізмам боротьби зі стомленням суспільства. Російські інформаційні операції спрямовані на виснаження українців. Хронічна тривога, емоційне виснаження, інформаційна перевтома та зниження довіри до джерел є наслідком постійного інформаційного тиску. Держава повинна розробити політику, яка допоможе громадянам протидіяти виснаженню. Це може включати регулярні кампанії підтримки, пояснювальні відеоматеріали, доступну інформацію про безпеку, психологічні рекомендації, зменшення кількості дублікатів інформації у медіапросторі та підвищення якості офіційних джерел. Такі заходи зменшать вразливість до інформаційного терору.

Перспективним напрямом є розвиток української медіасфери. Потрібно створювати якісні медіа, що працюють на основі етичних стандартів, дотримання фактчекінгу та прозорого фінансування. Суспільне мовлення повинно стати центром інформаційної довіри, особливо у кризових ситуаціях. Держава може забезпечити стійку підтримку Суспільного, щоб воно могло виконувати функцію нейтрального інформатора. Також потрібно підтримувати регіональні медіа, які відіграють важливу роль у формуванні локальної інформаційної стійкості [24]. Україна також повинна спрямувати увагу на формування культури

відповідального використання інформації. Кожен громадянин повинен розуміти, що його дії у цифровому середовищі мають наслідки. Потрібно формувати культуру обережного поширення інформації, уникнення панічних повідомлень та перевірки джерел. Цей елемент може бути інтегрований у шкільні програми, курси університетів, професійні стандарти та державні інформаційні кампанії.

У післявоєнний період Україна зіткнеться з новими викликами. Росія продовжуватиме інформаційний терор, намагаючись вплинути на внутрішню політику, створити соціальне напруження, дискредитувати реформаторські процеси та знизити довіру до Західних партнерів. Тому інформаційна політика повинна включати проактивні методи. Держава може формувати власні інформаційні наративи, які сприятимуть консолідації суспільства, пояснювати складні процеси реформ, підтримувати національну ідентичність та формувати позитивне бачення майбутнього. Такий підхід допоможе зменшити вплив зовнішніх маніпуляцій і стабілізувати суспільство у тривалому періоді.

Одним з найважливіших напрямів є відновлення довіри до державних інституцій. Висока довіра зменшує вплив дезінформації. Якщо громадяни довіряють офіційним джерелам, то маніпуляції мають менший ефект. Держава повинна забезпечити прозорість, регулярність комунікацій, звітність та чесність у повідомленнях. Це довів досвід країн ЄС, де рівень довіри до держави став основою стійкості до інформаційних атак у період пандемії.

Підсумовуючи, можна сказати, що рекомендації щодо вдосконалення політики України повинні ґрунтуватися на системному, багатовимірному підході. Держава повинна зміцнювати інституції, удосконалювати нормативну базу, розвивати людський капітал, формувати партнерства, модернізувати технологічні інструменти, розширювати міжнародну взаємодію та підсилювати соціальну стійкість. У сучасному світі інформаційний тероризм є одним із

ключових викликів, і лише комплексні рішення дозволять Україні протистояти йому ефективно. Ці рекомендації створюють основу для формування політики, що буде не лише реактивною, а й проактивною. Саме така політика забезпечить здатність держави захищати свій інформаційний простір, формувати стабільне суспільство та інтегруватися у глобальну архітектуру інформаційної безпеки.[84,85,86,87,88,89,90]

ВИСНОВКИ

Інформаційний тероризм у сучасному світі – це надзвичайно небезпечне явище, яке здатне впливати на всі сфери життя: політичну, економічну, соціальну та культурну. Його загроза не обмежується простим поширенням фейкових новин, а проникає у глибину суспільних структур, розколює суспільство, підриває довіру до державних інституцій і може стати каталізатором конфліктів. Сучасні технології, зокрема штучний інтелект, deepfake, алгоритмічне розповсюдження інформації та бот-мережі, створюють умови, коли

дезінформація може розповсюджуватися з неймовірною швидкістю та охопленням, що ускладнює завдання навіть найпотужніших державних систем безпеки. Україна, як країна, що вже зазнала численних інформаційних атак і гібридних загроз, повинна вчитися боротися з інформаційним тероризмом через інтеграцію багаторівневих стратегій. Це означає модернізацію законодавства, розбудову систем кібербезпеки, оперативне реагування на кібератаки та активну роботу з підвищення медіаграмотності серед громадян. Навчальні програми, тренінги для журналістів та співпраця з міжнародними експертами – все це є критично важливими елементами оборони, які допомагають суспільству критично оцінювати інформацію та не піддаватися маніпуляціям.

Міжнародна політика вже почала знаходити способи захисту від інформаційних атак – через укладення міжнародних договорів, створення спільних інформаційних центрів та публічно-приватих партнерств. Однак ці зусилля потребують ще більшої координації, обміну досвідом та інтеграції новітніх технологій. Створення єдиних стандартів та законодавчих механізмів на глобальному рівні може стати основою для більш ефективної протидії інформаційному тероризму, зменшуючи його вплив і забезпечуючи стабільність у цифрову епоху. Соціальні наслідки інформаційного тероризму мають довготривалий характер. Поширення маніпулятивного контенту руйнує внутрішню єдність, провокує конфлікти, сприяє агресії та розколу. У суспільстві формується втома від надмірної кількості інформації, що знижує здатність людей критично мислити. Виникає феномен інформаційної апатії. Люди перестають довіряти будь-яким джерелам, що створює середовище для ще глибших маніпуляцій. Інформаційний тероризм у такий спосіб підриває суспільну стійкість. Важливим аспектом стало зростання ролі штучного інтелекту. Ці технології одночасно зміцнюють інформаційний тероризм і створюють нові засоби протидії. Атакувальна сторона застосовує AI для автоматизації кампаній, створення гіперреалістичних підробок, масштабного аналізу аудиторій та поширення психологічного впливу. Захисна сторона використовує AI для аналізу великих масивів даних, виявлення фейків, прогнозування кризових ситуацій та блокування ботмереж. Це свідчить про те, що інформаційні конфлікти стають

дедалі алгоритмічнішими. Штучний інтелект перетворюється на центральний інструмент у боротьбі за контроль над інформаційним полем. У практичному вимірі протидія інформаційному тероризму вимагає інтегрованої політики. Ефективна модель повинна включати державні інституції, приватні компанії, медіаорганізації, громадянське суспільство та міжнародних партнерів. Жодна держава не здатна самостійно контролювати інформаційний простір у масштабах сучасних загроз. Інституційна взаємодія, обмін аналітичними даними, спільні програми підготовки спеціалістів та розвиток спільних технологій стають основою нової системи інформаційної оборони. Без цього індивідуальні зусилля держави залишаються недостатніми.

Український досвід продемонстрував, що інформаційна стійкість формується там, де існує синергія держави та суспільства. В умовах війни, інформаційний тиск був спрямований на деморалізацію, провокування паніки та створення хаосу. Попри це, Україна змогла сформувати ефективну модель інформаційної оборони завдяки динамічній взаємодії між державними установами, медіа, громадськістю та міжнародними союзниками. Цей досвід є унікальним прикладом того, як комплексний підхід забезпечує стабільність навіть у найскладніших умовах.

Фінальний висновок полягає у тому, що інформаційний тероризм став структурним елементом сучасної політики. Він формує нову реальність міжнародних відносин, суспільних процесів та внутрішньої безпеки. Його вплив неможливо нейтралізувати одним інструментом. Потрібна системна модель, що охоплює психологічні, інформаційні, технологічні, дипломатичні та освітні напрями. Лише поєднання цих компонентів здатне забезпечити стійкість держави та суспільства у довгостроковій перспективі. Одним з головних результатів дослідження є розуміння того, що інформаційний тероризм не існує окремо від соціальної структури. Він впливає на всі рівні суспільства, включно з макрополітичним, інституційним, міжособистісним та індивідуальним. На макрополітичному рівні він змінює логіку міжнародних відносин. Держави вимушені захищати інформаційний суверенітет так само, як територіальний. Інформація стає формою зброї, і цей факт визнається у стратегічних документах

багатьох країн. На інституційному рівні інформаційний тероризм підриває здатність держави забезпечувати стабільність, адже руйнує довіру до уряду, державних структур і демократичних процедур. На міжособистісному рівні він провокує конфлікти, роз'єднання та ворожість. На індивідуальному рівні вплив відбувається через емоції, страхи, упередження і психологічну втому.

Отже, боротьба з інформаційним тероризмом є складною та багаторівневою задачею, яка вимагає комплексного підходу. Держава зі слабкими інституціями, низьким рівнем довіри до влади, фрагментованими медіа та політичною поляризацією набагато вразливіша. Це пояснює, чому деякі країни швидше руйнуються під впливом інформаційних атак, ніж інші. Водночас інформаційно стійкі держави здатні зменшувати вплив атак через ефективні механізми комунікації, швидке реагування, надійні інституції та формування культури критичного мислення. Таким чином, рівень інформаційної стійкості визначається структурою держави та її інформаційним середовищем, а не лише наявністю технологічних засобів. Для України важливо використовувати досвід інших країн, таких як Ізраїль, Естонія та Німеччина, інтегрувати сучасні технологічні рішення, удосконалювати законодавчу базу та активно працювати над підвищенням медіаграмотності населення. Міжнародна співпраця, створення спільних нормативних актів та обмін досвідом стають ключовими чинниками в забезпеченні інформаційної безпеки. Лише таким чином можна зменшити ризики дестабілізації суспільства та гарантувати стабільність національної та глобальної безпеки у цифрову епоху.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[] Почепцов Г. Інформаційні війни. Київ, 2015.

[2] NATO StratCom COE. Hybrid Threats and Information Operations. Riga, 2022. https://rigastratcomdialogue.org/images/static/Buklets-RSD-Final.pdf

[3] Rid T. Cyber War Will Not Take Place. Oxford University Press, 2013. https://csl.armywarcollege.edu/SLET/mccd/CyberSpacePubs/Cyber%20War%20Will%20Not%20Take%20Place%20by%20Thomas%20Rid.pdf

[4] EU DisinfoLab. Russian Information Operations 2023 Report. Brussels, 2023. https://www.disinfo.eu/investigations/

[5] NATO ACT. Cognitive Warfare: The Battle for Your Mind. Norfolk, 2021. https://www.act.nato.int/activities/cognitive-warfare/

[] Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування, 2021. https://sprotyvg7.com.ua/wp-content/uploads/2022/12/inform-bezpeka.pdf

[8] Chesney R., Citron D.K. Deepfakes and the New Disinformation War. Foreign Affairs, 2019. https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war#

[9] NATO Cooperative Cyber Defence Centre of Excellence. BlackEnergy and Cyber Attacks on Ukrainian Infrastructure. 2016. https://www.ccdcoe.org/uploads/2025/07/Tkachuk_N_Tallinn_Paper_15_Ukraine-as-the-Frontline-of-European-Cyber-Defence.pdf

[10] Ferrara E., Varol O., Davis C., Menczer F., Flammini A. The Rise of Social Bots. Communications of the ACM. 2016. https://www.semanticscholar.org/paper/The-rise-of-social-bots-Ferrara-Varol/6f90ad2553c2a73948f614d19c763ec3d5e58542

[11] Jakobsson M., Myers S. Social Engineering: The Art of Human Hacking. 2006. http://repo.darmajaya.ac.id/4637/1/Social%20Engineering_%20The%20Science%20of%20Human%20Hacking%20%28%20PDFDrive%20%29.pdf

[12,] Freedom House. Disinformation and Pandemic Anxiety. 2021. https://freedomhouse.org/country/ukraine/freedom-net/2021

[13] Persily N., Tucker J.A. Political Persuasion and Digital Data. 2019. https://books.google.com.ua/books?hl=uk&lr=&id=NEjzDwAAQBAJ&oi=fnd&pg=PR11&dq=Persily+N.,+Tucker+J.A.+Political+Persuasion+and+Digital+Data.+2019&ots=5k4NknEpdG&sig=05h6PqSfwPo7_7ib8IhIfgoQOsY&redir_esc=y#v=onepage&q&f=false

[14] Bundeszentrale für politische Bildung. Studien zur Demokratiefestigkeit. 2020. https://www.bpb.de/system/files/dokument_pdf/APuZ_2020-14-15_online_0.pdf

[15] Galeotti M. Hybrid War or Gibridnaya Voina? 2016. http://visnyk.nuou.org.ua/article/view/325378

[16] Financial Action Task Force. Illicit Finance and Digital Platforms. 2019. https://www.moodys.com/web/en/us/kyc/resources/faq/risk-compliance.html?cid=62EFF960F8A17502&gclsrc=aw.ds&gad_source=1&gad_campaignid=18527004193&gbraid=0AAAAAoctWHzPZ_8gYLKwDjOpZMIJj8Aca&gclid=CjwKCAiAlfvIBhA6EiwAcErpyX7oxDV-8Spl4iCd9FnAMFZWkCdcY6Jbnd-LLBfM-1FQf3s_ZMccFRoC3v4QAvD_BwE

[17] Dyer W., Farrell H., Winer S. Shadow Budgets and Hidden Influence. 2020.

[18] Howard P.N., Kollanyi B. Bots and Automation in Elections. Oxford, 2018.

[19] Polyakova A., Boyer S. The Future of Political Warfare. Brookings, 2018.

[20] Brady A.-M. China's Foreign Propaganda and Domestic Control. 2017. https://www.researchgate.net/publication/389235024_Marketing_Dictatorship_Propaganda_and_Thought_Work_in_Contemporary_China

[21] NATO StratCom COE. Information Influence Campaigns in Europe. Riga, 2022.

[22] US Senate Report. The Role of Social Media in the Capitol Attack. Washington, 2022.

[23] Інститут масової інформації. Аналітичний звіт про фейки у воєнний період. Київ, 2023. https://imi.org.ua/monitorings/i58282

[24] German Federal Office for Civic Education. Countering Disinformation Strategies. Berlin, 2021. https://www.bundeswahlleiterin.de/en/bundestagswahlen/2021/fakten-fakenews.html

[25] Lewandowsky S., Ecker U. Misinformation and Its Correction. Psychological Science, 2020. https://journals.sagepub.com/doi/abs/10.1177/1529100612451018

[26] EUvsDisinfo. Hybrid Tactics and Cognitive Warfare. Brussels, 2023.

[27] РНБО України. Центр протидії дезінформації: Звіт 2023. Київ, 2023. https://cpd.gov.ua/announcement/zvit-operatyvnoyi-informacziyi-26-06-2023-02-07-2023/

[28] WHO. Mental Health and Information Overload. Geneva, 2023. https://www.tandfonline.com/doi/abs/10.1080/0144929X.2023.2281500

[29] Finnish Ministry of Education. Media Literacy Education Report. Helsinki, 2022.

[30] Fenton N., Freedman D. Digital Media and Trust. London, 2021. https://www.researchgate.net/publication/284912050_Left_out_Digital_media_radical_politics_and_social_change

[31] Nye J. Soft Power and Information Warfare. Harvard University Press, 2021.

[32] Gerasimov V. The Value of Science in Prediction. Military-Industrial Courier, 2013. https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf

[33] US Senate Intelligence Committee. Russian Active Measures Campaigns and Interference in the 2016 Election. Washington, 2020. https://www.intelligence.senate.gov/wp-content/uploads/2024/08/sites-default-files-documents-report-volume1.pdf

[35] NATO StratCom COE. Russia's Global Media Ecosystem. Riga, 2022.

[36] China State Council. White Paper on Internet Sovereignty. Beijing, 2020. http://www.scio.gov.cn/zfbps/zfbps_2279/202303/t20230320_709283.html

[37] Xinhua News Agency. Global Communication Strategy of China. 2021.

https://english.news.cn/20251114/2e8e0718f7164bcebb7a7314457fef8f/c.html

[38] Atlantic Council. Iran's Disinformation Networks. Washington, 2022.

[39] UN Security Council. Report on DPRK Cyber Activities. New York, 2023. https://www.securitycouncilreport.org/un-documents/dprk-north-korea/

[40] RAND Corporation. US Strategic Communications in Conflict Zones. Santa Monica, 2019.

[41] European Commission. StratCom Task Force Reports. Brussels, 2023.

https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

[42] Buzan B. People, States and Fear. London, 2007. https://share.google/YSom5yPVFv9c9BFKF

[43] Freedom House. Beijing's Global Media Influence Report. 2023.

[44] European Centre for Media Resilience. EU Code of Practice on Disinformation. Brussels, 2022. https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

[45] РНБО України. Звіт про інформаційні атаки 2023. Київ, 2023. https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf

[46] NATO. Cognitive Warfare Doctrine. Brussels, 2023. https://www.sto.nato.int/wp-content/uploads/20240223-uc--sto-highlights-web.pdf

[47] Council of Europe. Legal Challenges of Hybrid Threats. Strasbourg, 2022.

[48] OSCE. Information Integrity and Security Report. Vienna, 2023.

[49] Hoffman B. Inside Terrorism. Columbia University Press, 2017. https://cup.columbia.edu/book/inside-terrorism/9780231174770/

[50] The Soufan Center. ISIS Media Strategy Report. New York, 2020. https://www.jstor.org/stable/27255596

[51] Europol. Terrorist Propaganda Online. The Hague, 2022. https://www.europol.europa.eu/cms/sites/default/files/documents/EU_TE-SAT_2025.pdf

[52] UNODC. Cyber-Enabled Radicalization and Recruitment. Vienna, 2021. https://www.unodc.org/unodc/en/cybercrime/home.html

[53] UN Security Council. Foreign Terrorist Fighters Report. 2019.

[54] Bergen P. The Longest War: The Enduring Conflict between America and Al-Qaeda. New York, 2011.

[55] Norton B. Hacktivism and Cyberwars. Routledge, 2019..

[56] Carnegie Endowment. Iran's Information Proxy Operations. Washington, 2022.

[57] Freedom House. Telegram and Digital Extremism. Washington, 2023.

[58] Europol. The Darknet and Terrorist Financing. The Hague, 2022. https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated%20Annual%20Activity%20Report%202022. PDF

[59] INTERPOL. Global Financial Crime Report. Lyon, 2023.

[60] Pew Research Center. Social Media and Radicalization. 2023 https://www.pewresearch.org/internet/2023/12/11/teens-social-media-and-technology-2023/

[61] NATO StratCom COE. Hybrid Warfare and Non-State Actors. Riga, 2023.

[62] Atlantic Council. Proxies and Plausible Deniability in Information Warfare. Washington, 2022.

[63] European Commission. Disinformation from State-Linked Actors. Brussels, 2023. https://www.europarl.europa.eu/doceo/document/A-9-2023-0187_EN.html

[64] UNODC. Terrorist Use of the Internet. Vienna, 2022. https://www.unodc.org/copak/en/Stories/SP4/countering-the-use-of-internet-for-terrorist-purposes-3-5-august-2022.html

[65] CyberPeace Institute. Volunteer Cyber Armies in Ukraine. Geneva, 2023.

[66] Oxford Internet Institute. The Velocity of Misinformation. Oxford, 2022. https://www.oii.ox.ac.uk/news-events/oii_tag/disinformation/

[67] Freedom House. Platform Accountability and State Narratives. Washington, 2023.

[68] Human Rights Watch. National Internet Projects and Digital Authoritarianism. New York, 2023.

[69] The Bureau of Investigative Journalism. The PR Industry of Disinformation. London, 2023.

[70] European Union. Code of Practice on Disinformation. Brussels, 2022.

[71] Ministry of Digital Transformation of Ukraine. Digital Diplomacy Report. Kyiv, 2023.

[72] Europol. AI-Driven Disinformation Networks. The Hague, 2024.

[73] Pew Research Center. Emotional Dynamics in Online Propaganda. 2023.

[74] Council of Europe. Cybercrime Convention and Information Warfare. Strasbourg, 2023.

[75] OSCE. Information Resilience Framework. Vienna, 2023.

[76] UNESCO. Critical Thinking and Media Literacy in Global Security. Paris, 2023.

[77] UNDP. Integrated Responses to Hybrid Threat

[78] Buzan B. People, States and Fear. London, 2007.

[79] US Senate Intelligence Committee. Russian Active Measures Campaigns and Interference in the 2016 Election. Washington, 2020.

[] Freedom House. Freedom on the Net. Washington, 2023.

[81] Nye J. Soft Power and Global Politics. Cambridge, 2021.

[82] Atlantic Council. Digital Authoritarianism Report. Washington, 2022.

[83] NATO StratCom COE. Hybrid Warfare and Strategic Communication. Riga, 2023.

[84] NATO. Strategic Concept 2023. Brussels, 2023.

[85] WHO. Managing the COVID-19 Infodemic. Geneva, 2020.

[86] World Bank. Economic Impact of Disinformation. Washington, 2021.

[87] OECD. Public Expenditure on Disinformation Countermeasures. Paris, 2023.

[88] Harvard Kennedy School. Polarization and Social Trust Report. Boston, 2023.

[89] Oxford Internet Institute. Identity and Online Radicalization. Oxford, 2022.

[] Council of Europe. Legal Frameworks for Information Security. Strasbourg, 2023.