МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРНІВЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЮРІЯ ФЕДЬКОВИЧА

ВОЗНЮК ЄВГЕНІЯ ВАСИЛІВНА

УДК 327-049.5]:323.28:001.102

ІНФОРМАЦІЙНИЙ ТЕРОРИЗМ ЯК ЧИННИК ВПЛИВУ НА МІЖНАРОДНУ ТА НАЦІОНАЛЬНУ БЕЗПЕКУ

23.00.04 – політичні проблеми міжнародних систем і глобального розвитку

Реферат
дисертації на здобуття наукового ступеня
доктора політичних наук

Чернівці – 2025

Дисертацією є рукопис.
Робота виконано самостійно.

Опоненти:

доктор політичних наук, професор
НІКОЛАЄНКО Наталія Олександрівна,
Національний університет «Києво-Могилянська академія»,
професор кафедри політології факультету соціальних наук та соціальних технологій

доктор політичних наук, професор
ДЕРЕВ'ЯНКО Сергій Миронович,
Карпатський національний університет імені Василя Стефаника,
професор кафедри політичних наук факультету історії, політології і міжнародних відносин

доктор політичних наук, професор
ПІПЧЕНКО Наталія Олександрівна,
Навчально-наукового інституту міжнародних відносин, Київський національний університет імені Тараса Шевченка,
професор кафедри міжнародної інформації

Захист відбудеться «19» грудня 2025 року о 10.00 годині на засіданні спеціалізованої вченої ради Д 76.051.03 Чернівецького національного університету імені Юрія Федьковича за адресою: 58012, м. Чернівці, вул. Кафедральна, 2, ауд. 18.

Із дисертацією можна ознайомитися на офіційному сайті https://www.chnu.edu.ua/nauka/zdobuvachu-naukovoho-stupenia/postiino-diiuchi-spetsializovani-vcheni-rady/spetsrada-d-7605103/ та в бібліотеці Чернівецького національного університету імені Юрія Федьковича за адресою: 58012, м. Чернівці, вул. Лесі Українки, 23.

Реферат розісланий «17» листопада 2025 р.

Вчений секретар
спеціалізованої вченої ради **Любов МЕЛЬНИЧУК**

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність дослідження. Дослідження проблеми інформаційного тероризму зумовлене зростанням загроз інформаційному суверенітету держави, що потребує системного посилення її захисного потенціалу. У сучасних умовах державна інформаційна політика стає ключовим елементом як внутрішньої, так і зовнішньої діяльності, охоплюючи всі сфери суспільного життя. Стрімкий розвиток інформаційного простору породжує нові виклики, що впливають на безпеку особи, суспільства й держави. В епоху інформаційних війн і тотальної цифровізації питання інформаційної безпеки набуває стратегічного значення.

Інформаційна революція, замість очікуваної прозорості, спричинила хаотичне зростання потоків неперевірених даних, що створює умови для маніпуляцій та дезінформації. Медіа й інтернет перетворилися на арену політичного впливу, де конструюються потрібні наративи, підмінюються факти та формуються штучні суспільні настрої. Отже, інформаційний простір став полем політичного протиборства, яке дедалі більше набуває посттрадиційних форм.

У політичній науці посилюється розуміння необхідності оновлення підходів до інформаційної політики держави в умовах глобального інформаційного тиску. Дослідники наголошують на важливості створення цілісної системи інформаційного управління, що передбачає стратегічне планування, кризове реагування та мінімізацію інформаційних ризиків. Зміна структури міжнародних відносин і розвиток мережевої взаємодії між державами й громадянським суспільством формують нову модель глобального управління.

Інформаційний тероризм визначається як новітня форма гібридної агресії, спрямована на дестабілізацію суспільств через маніпуляції, дезінформацію, кібернапади та психологічний тиск. На відміну від класичного терору, він уражає свідомість, підриває довіру до інституцій, провокує паніку й хаос. Під час війн, криз чи виборів його вплив особливо небезпечний, що доводять приклади інформаційних атак на США, ЄС та Україну. У теорії міжнародних відносин інформаційний тероризм розглядається як нетрадиційна загроза глобальній безпеці, що діє без прямого застосування сили. Його мета – змінити суспільні настрої, делегітимізувати уряди, послабити міжнародну підтримку супротивника. У межах конструктивізму – це боротьба за контроль над смислами, а у реалізмі – інструмент зміни балансу сил. Отже, інформаційний тероризм є міждисциплінарним феноменом, який поєднує безпекові, комунікаційні та психологічні аспекти.

У контексті російсько-української війни інформаційний тероризм набув особливої актуальності як зброя впливу на громадську думку, деморалізації

населення й підриву довіри до влади. Його вивчення є необхідною умовою формування ефективної системи інформаційної стійкості та національної безпеки України.

Попередні наукові розвідки у сфері міжнародної й інформаційної безпеки, тероризму, кіберзагроз і медіакомунікацій характеризувалися переважно фрагментарністю та одновимірністю аналізу феномену інформаційного тероризму. Більшість досліджень обмежувалися техніко-правовим або соціально-комунікаційним підходом, не охоплюючи його політичний, інституційний та безпеково-цивілізаційний виміри. Отож у науковій літературі залишалися недостатньо висвітленими такі сторони проблеми, які комплексно розв'язує дисертантка, а саме: не проаналізовано інформаційний тероризм як політичний феномен глобального управління, що трансформує архітектуру міжнародної безпеки – якщо раніше інформаційний тероризм розглядали переважно як різновид кібертероризму або дезінформаційної діяльності, то доведено його політико-інституційну природу як інструменту впливу держав і недержавних акторів на баланс сил у світі. Недослідженим залишався взаємозв'язок між інформаційним тероризмом і процесами гібридної війни, а також й відсутні цілісний теоретико-методологічний підхід до вивчення інформаційного тероризму. Недослідженою була категорія «інформаційна стійкість» у контексті політичної безпеки; відсутній комплексний порівняльний аналіз національних моделей протидії інформаційному тероризму; недостатньо вивчені механізми нормативно-правового реагування на інформаційні загрози.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано в рамках науково-дослідних робіт факультету міжнародних відносин ВНУ ім. Лесі Українки, а саме: «Актуальні проблеми формування та розвитку європейського інформаційного простору» (2010–2012 рр.), «Інформація та комунікація в сучасному світі» (2012–2014 рр.) (держреєстраційний № 0112U001779); держбюджетної теми «Інформаційна підтримка транскордонного співробітництва України» (2013–2015 рр.) (держреєстраційний № 0113U002221); 2018–2019 рр. – НДР «Інформаційна війна як новий вимір геополітичної ривалізації» згідно з наказом Міністерства освіти і науки України від 25.06.2018 р. № 695»; «Про фінансування спільних українсько-польських науково-дослідних проектів у 2018 р.» (співвиконавець – Інститут наук про безпеку Краківського педагогічного університету ім. Національної освітньої комісії) (держреєстраційний № 0119U001621), а також міжнародних грантових проєктів програми ERASMUS+ напряму Модуль Жана Моне: 2022–2025 рр. – «Стратегічні комунікації ЄС: протидія деструктивним впливам»; 2024–2027 рр. – «Протидія ЄС дезінформації, маніпуляціям і зовнішньому втручанню» (№ 101172342 ERASMUS-JMO-2024-MODULE).

Мета та завдання дослідження. Мета дослідження полягає у комплексному аналізі інформаційного тероризму як феномену сучасної системи безпеки на глобальному, регіональному й національному рівнях.

Відповідно до поставленої мети сформульовано такі **завдання:**

– проаналізувати еволюцію концепту тероризму в теорії міжнародних відносин, розглянути різні термінологічні та концептуальні підходи до його тлумачення, зокрема в контексті глобалізаційних викликів і багатовимірності явища;

– систематизувати наукову та джерельну базу досліджень тероризму й антитероризму, виявити особливості інтерпретації проблематики в академічному та експертному дискурсах;

– визначити сутність і типологію інформаційного тероризму як складової частини міжнародного тероризму, дослідити такі його прояви, як медіатероризм і кібертероризм, ін.;

– розкрити зміст категорії міжнародної інформаційної безпеки, охарактеризувати її складові частини, уключаючи національний рівень захисту інформаційного простору;

– дослідити характер і структуру сучасних інформаційних війн, зокрема гібридного типу, а також їхні ключові форми: iWar, війна четвертого покоління, асиметрична та посередницька війни, медіавійна;

– проаналізувати основні виклики й загрози міжнародній інформаційній безпеці в цифрову епоху, зокрема роль соціальних медіа, ботоферм і маніпулятивного контенту в умовах інформаційного терору;

– визначити інструменти, механізми та практики протидії інформаційному тероризму, уключаючи роль мас-медіа, омбудсменів, цифрових регуляторів і державних ініціатив;

– проаналізувати досвід окремих держав світу (США, країни ЄС, Японія, КНР, Індія, країни Африки, Латинської Америки тощо) в протидії кібер- та інформаційному тероризму й забезпеченні інформаційної безпеки;

– оцінити стан і виклики інформаційної безпеки в Україні в умовах війни з Російською Федерацією, зокрема в частині інституційного забезпечення, медіаполітики, кіберзахисту та протидії російській дезінформації;

– розробити рекомендації щодо зміцнення інформаційної стійкості до інформаційних загроз з урахуванням міжнародного досвіду й специфіки інформаційної війни в українському контексті.

Об’єкт дослідження – система міжнародної безпеки в умовах інформаційної епохи. **Предметом дослідження** є феномен інформаційного тероризму як форми деструктивного інформаційного впливу та його дія на безпекове середовище сучасних держав і міжнародних інституцій.

Хронологічні рамки дослідження охоплюють період із початку 2000-х до 2024 р., що зумовлено стрімким розвитком інформаційного простору та появою нових загроз цифрової епохи. Саме на початку XXI ст. відбулись інституціоналізація поняття інформаційної безпеки, формування міжнародних стратегій кіберзахисту й поява концепту інформаційного тероризму як окремого явища. Верхня межа – 2024 р. – позначає пік інтенсивності інформаційних протистоянь у контексті російсько-української війни, яка стала центральним елементом глобальної боротьби за контроль над інформаційним простором. Водночас розвиток цифрових технологій, штучного інтелекту та медіаплатформ зумовлює постійну еволюцію форм і наслідків інформаційного тероризму, що потребує подальших міждисциплінарних досліджень.

Гіпотеза дослідження полягає в тому, що в умовах глобальної цифровізації та гібридних конфліктів інформаційний тероризм формується як нова форма політичного насильства, яка поєднує технологічні, комунікаційні та безпекові виміри й трансформує архітектуру міжнародних відносин. Спираючись на міждисциплінарний синтез неореалізму, конструктивізму та неоінституціоналізму, стає очевидно, що у XXI ст. головною ареною протиборства є інформаційний простір, де насильство має когнітивний, а не фізичний характер. У цьому контексті інформаційний тероризм є структурним чинником дестабілізації безпекового середовища через підрив довіри, делегітимацію політичних інститутів і руйнування соціальних наративів. Водночас рівень інформаційної стійкості держави, суспільства та особистості, сформований завдяки розвитку критичного мислення, стратегічних комунікацій і цифрової грамотності, стає новим виміром політичної могутності та запорукою збереження суверенітету, ідентичності й стабільності у світі гібридних загроз.

Методи дослідження. Дослідження інформаційного тероризму здійснено на основі комплексного методологічного підходу, що поєднує загальнонаукові, спеціально-наукові та міждисциплінарні методи. Серед загальнонаукових – аналіз, синтез, індукція й дедукція, які використано для виокремлення складових частин феномену інформаційного тероризму, їх узагальнення в концептуальну модель і перевірки теоретичних гіпотез на практичних прикладах. Застосовано класифікацію та типологізацію для систематизації видів інформаційного тероризму й методів протидії. Із методів політичної науки та міжнародних відносин використано порівняльний та інституціональний аналіз для зіставлення національних стратегій, оцінки ролі державних і міжнародних інституцій у сфері інформаційної безпеки. Метод аналізу політики дав змогу вивчити нормативно-правові документи й стратегії кіберзахисту. У межах міждисциплінарного підходу застосовано дискурс- і контент-аналіз для дослідження пропагандистських практик, наративів та фейкових повідомлень, а також метод

case study – для аналізу конкретних випадків інформаційних атак. Історико-ретроспективний метод використано для вивчення еволюції концепту інформаційного тероризму. Серед емпіричних методів – моніторинг відкритих джерел (OSINT) і статистичний аналіз даних про масштаби інформаційних атак та кіберзагроз. У результаті поєднання якісного й кількісного підходів забезпечено комплексне осмислення феномену інформаційного тероризму та оцінку актуальних безпекових викликів на національному й міжнародному рівнях.

Наукова новизна одержаних результатів. У процесі дослідження здобуто результати, новизна яких конкретизується в таких положеннях:

уперше:

– запропоновано концептуалізацію поняття інформаційної стійкості. У сучасних умовах гібридної війни та інформаційної конфронтації дедалі більшого значення набуває цей концепт, який розглядається як ключова складова частина національної безпеки й соціальної згуртованості. Під *інформаційною стійкістю* розуміємо спроможність держави, інституцій і громадянського суспільства протистояти зовнішнім та внутрішнім інформаційним загрозам, уключаючи дезінформацію, маніпуляції, пропаганду й інші форми інформаційного впливу, що мають на меті дестабілізацію політичного, соціального або культурного середовища. Інформаційна стійкість є комплексним міждисциплінарним феноменом, який уключає технічні, організаційні, нормативно-правові, освітні та психологічні складові частини;

– запропоновано концептуальні напрями модернізації Закону України «Про боротьбу з тероризмом», що відображають трансформацію терористичних загроз у цифрову добу. Запропоновано ввести до національного законодавства категорію «інформаційна стійкість» як ключовий індикатор безпеки й розширити суб’єктний склад боротьби з тероризмом через закріплення правового статусу неурядових структур у сфері інформаційного захисту. Наукову новизну становить також розширення термінологічного апарату антитерористичного законодавства шляхом уведення до нормативного поля нових дефініцій, як-от: інформаційний тероризм, кібертероризм, інформаційно-психологічна операція (ІПсО). Уточнення цих понять становить правову основу для визнання інформаційних і кібернетичних атак формами терористичної діяльності, що дає змогу розширити коло об’єктів та суб’єктів безпеки, підвищити ефективність моніторингу, кваліфікації й запобігання сучасним загрозам у гібридному середовищі;

– обґрунтовано новий підхід до протидії інформаційному тероризму, що полягає у виокремленні та теоретичному узагальненні *трикомпонентної моделі забезпечення інформаційної стійкості*, яка охоплює стратегічні комунікації (як

інструмент консолідації національного наративу, формування довіри до держави й нейтралізації ворожих інформаційних операцій), медіаосвіту (як чинник формування критичного мислення, інформаційної гігієни та спроможності до самостійної ідентифікації інформаційних загроз) і цифрову безпеку (як складову частину інформаційної оборони держави, що включає технологічні та організаційні засоби кіберзахисту, у тому числі на основі національного й міжнародного співробітництва). Уперше здійснено системний аналіз взаємозв'язку між стратегічними комунікаціями, медіаосвітою та цифровою безпекою як ключовими інструментами у структурі національної й міжнародної інформаційної безпеки;

– здійснено комплексне міждисциплінарне дослідження міжнародного тероризму в умовах глобалізації, у якому запропоновано нову концептуалізацію інформаційного тероризму як автономного феномену, що поєднує риси когнітивної війни, кібертерору та ідеологічної агресії. Визначено інституційні, цивілізаційні й правові аспекти інформаційної агресії; виявлено її вплив на структури міжнародної безпеки, політичну стабільність і правовий режим міжнародного гуманітарного права. Обґрунтовано необхідність перегляду засад міжнародного права та безпеки в контексті викликів інформаційної епохи;

– здійснено аналіз унікального українського досвіду протидії інформаційному тероризму в умовах повномасштабної гібридної агресії, що триває з 2014 р. та інтенсифікувалася після 2022 р. Уперше на основі системного підходу досліджено, як держава, перебуваючи в умовах постійного зовнішнього інформаційного тиску, змогла сформувати *цілісну модель інформаційного спротиву,* що поєднує інституційні, технологічні, суспільні й дипломатичні інструменти. У роботі обґрунтовано такі нові компоненти української інформаційної стійкості, як алгоритмічна протидія фейкам, мобілізація цифрового громадянського суспільства (зокрема волонтерських ініціатив, кіберспротиву), які ще не були належно осмислені в науковій літературі. Досвід України розглянуто як перспективну модель, що вже частково імплементується в політику безпеки ЄС, НАТО й окремих країн. Запропоновано авторське бачення українського кейсу як джерела універсальних рішень, придатних до адаптації в інших регіонах, які зазнають інформаційного терору. У цьому контексті акцентовано на необхідності міжнародно-правової інституалізації механізмів боротьби з інформаційним тероризмом з урахуванням українського внеску як одного з головних орієнтирів для формування глобальної стратегії цифрової безпеки;

– запропоновано нову інтерпретацію терористичних атак 11 вересня 2001 р. не лише як воєнного виклику, але і як переломного моменту в *трансформації глобальної парадигми безпеки*, що започаткував якісно нову еру

інформаційно-психологічного, асиметричного й неконвенційного протиборства. Переосмислено роль подій 11 вересня як тригера для еволюції нових типів конфліктів – від традиційного терору до інформаційних та проксі-війн. Доведено, що гасло «боротьби з тероризмом» стало основою для формування нових стратегічних доктрин, які легітимізували втручання в інші країни поза рамками колективної безпеки.

Дістали подальшого розвитку:

– твердження стосовно особливого значення інформаційної стійкості в контексті протидії інформаційним операціям іноземних держав, що можуть впливати на демократичні процеси, створювати соціальну напругу, підривати легітимність влади й дезорієнтувати громадянське суспільство. Отже, інформаційна стійкість є важливою передумовою національного суверенітету в умовах цифрової епохи;

– теза про те, що громадянське суспільство в Україні стало ключовим суб'єктом протидії інформаційним загрозам, особливо після початку російської агресії у 2014 р. Доведено, що ініціативи громадських організацій заповнили прогалини в державному управлінні інформаційною безпекою, запровадили нові практики OSINT-розвідки, цифрового моніторингу, протидії дезінформації й підвищення медіаграмотності. На тлі гібридної війни роль громадянського сектору у сфері інформаційної безпеки зростає. Його залучення до формування національної стратегії захисту інформаційного простору, зміцнення партнерства з державою, розвиток цифрових компетентностей суспільства є критично важливими для стійкості України перед зовнішніми загрозами. Отже, громадські організації підтвердили свою ефективність у протидії інформаційним атакам та повинні залишатися невід'ємною частиною загальнонаціональної системи інформаційної безпеки;

– аналіз інформаційної війни як самостійної вісі гібридної агресії**,** що змістила фокус із фізичної конфронтації до когнітивного впливу, розмиття ідентичності й делегітимації держав. Такий підхід дав змогу визначити інформаційну війну як домінантну форму сучасного глобального конфлікту. Доповнено концепт інформаційної зброї як системного інструменту неконвенційного впливу, що поєднує дезінформацію, психологічний тиск, кібератаки, фейковий контент і маніпулятивні наративи. Доведено, що інформаційна зброя спроможна чинити ефекти, співмірні із застосуванням збройної сили, але з нижчими витратами й вищою адаптивністю. Систематизовано вплив інформаційної зброї на внутрішню стабільність держави в умовах гібридної війни, зокрема на прикладі конфлікту Росії проти України. Показано, що інформаційні атаки – не супровід воєнних дій, а самостійна фаза стратегічного наступу, спрямована на руйнацію довіри, деморалізацію населення

та політичну дезінтеграцію;

– порівняння моделей забезпечення інформаційної безпеки, що охоплює досвід США, держав Європейського Союзу, Японії, Китаю, Індії й країн Латинської Америки. Такий комплексний підхід дає змогу виявити спільні виклики та відмінні стратегії у відповідь на кіберзагрози. Систематизовано чинники вразливості національних цифрових інфраструктур із виокремленням таких критичних елементів, як фрагментарність правової бази, брак міжвідомчої координації, недостатня цифрова грамотність, обмеженість ресурсів, цифрова диктатура;

– трактування інформаційної агресії Російської Федерації як стратегічно спланованої форми гібридної війни, що поєднує інформаційно-психологічні операції, кібератаки, дезінформацію та маніпулятивні кампанії в цифровому середовищі. Обґрунтувано комплексну модель інформаційного терору РФ як багаторівневу, технологічно адаптивну стратегію, що мімікрує під демократичні цінності з метою делегітимізації української державності й деморалізації суспільства.

Поглиблено:

– знання щодо таких аспектів, як інституційна спроможність держави забезпечувати кібербезпеку та контроль за інформаційним середовищем; рівень медіаграмотності населення і його здатність до критичного мислення; ефективність стратегічних комунікацій, спрямованих на посилення довіри до демократичних інституцій; інклюзивна державна політика щодо інформаційної безпеки, спрямована на захист прав людини та свободи слова;

– сучасні підходи до інформаційного тероризму із виокремленням таких його ключових рис, як транснаціональність, мережевість, когнітивна маніпуляція, цифрова анонімність, інституційна невизначеність. Доведено, що інформаційний тероризм має тенденцію до інституціоналізації на рівні державної політики авторитарних режимів і використовується як інструмент зовнішньополітичного тиску. Зокрема, наголошено на ролі таких суб’єктів, як Російська Федерація, Китайська Народна Республіка й ін., що активно використовують інформаційний простір як поле для невоєнної агресії;

– засади національної інформаційної безпеки в умовах нових типів воєн, що включають цифрову стійкість, розвиток критичного мислення громадян, інформаційну гігієну, стратегічну комунікацію та міжнародну кооперацію в межах НАТО, ЄС й ООН;

– обґрунтування ролі стратегічних комунікацій, медіаграмотності, інформаційної гігієни в національній і міжнародній безпеці, зокрема як елементів інформаційної оборони. Показано, що ключовим викликом для держави у XXI ст. є не лише захист територіальної цілісності, а й оборона

інформаційного суверенітету. Проаналізовано структурні вразливості України в інформаційній сфері (низький рівень цифрової грамотності, фрагментарність політики, повільна реакція на ШІ-загрози) та визначенні стратегічних пріоритетів для формування сталої інформаційної стійкості;

– розуміння інституційно-суспільної взаємодії в інформаційній обороні України, зокрема визначено унікальну роль громадянського суспільства як рівноправного суб'єкта протидії інформаційній агресії (на прикладі OSINT-спільнот, цифрових волонтерів, проєктів StopFake, Detector Media тощо). Систематизовано виклики у співпраці між державою та громадськими ініціативами, зокрема правової неврегульованості, етичних дилем, що дає змогу сформувати підґрунтя для розроблення національної моделі врегулювання партнерства в інформаційній безпеці. Посилено аргументацію потенціалу українського досвіду як моделі для транснаціонального використання в системах інформаційної безпеки держав, що протидіють авторитарному інформаційному впливу.

Практичне значення одержаних результатів. На основі проведеного дослідження сформульовано узагальнення та висновки, що можуть бути використані в подальших наукових розвідках із проблем гібридної війни й політик протидії інформаційній агресії. Результати роботи створюють теоретичне та емпіричне підґрунтя для формування державної доктрини гуманітарної й культурної безпеки, поглиблюють розуміння феномену інформаційного тероризму в системі міжнародної безпеки, пропонують міждисциплінарний підхід до аналізу деструктивних інформаційних впливів, типологію загроз та узагальнення міжнародного досвіду їх подолання. Напрацювання дисертації можуть бути використані органами державної влади під час розроблення стратегій інформаційної безпеки, протидії гібридним загрозам і дезінформації, а також сприяти підвищенню інформаційної грамотності населення, формуванню стійкості до маніпуляцій та захисту демократичних цінностей. Матеріали дослідження доцільно застосовувати в навчальному процесі – у курсах із міжнародної безпеки, стратегічних комунікацій, кібербезпеки, конфліктології й міжнародної інформації. Вони можуть стати базою для нових освітніх програм і створення аналітичних центрів, що розроблятимуть україноцентричні гуманітарні стратегії та сприятимуть інтеграції українського культурного простору в європейський.

Особистий внесок здобувача. Дисертаційна робота є завершеним самостійним науковим дослідженням, у якому всі положення, висновки та рекомендації одержано здобувачем особисто. Із праць, опублікованих у співавторстві, використано лише ті результати, що належать дисертанту, про що зазначено в списку публікацій. Внесок здобувача полягає в розвитку концепцій

інформаційної безпеки, стратегічних комунікацій і протидії інформаційному тероризму в системі міжнародних відносин. У наукових працях дисертантка з перших у вітчизняній політичній науці розкрила інформаційний тероризм як структурний чинник гібридних воєн, окресливши його когнітивну, технологічну та комунікативну природу. Розроблено аналітичну модель інформаційно-терористичних впливів і типологію їхніх інструментів – від дезінформації до кібердиверсій. У публікаціях, виконаних у співавторстві, здійснено порівняльний аналіз систем інформаційної безпеки провідних країн (США, ЄС, Японії, Індії, Бразилії), що стало підґрунтям для створення власної моделі кібер-та інформаційної стійкості України. Особливе місце посідають дослідження стосовно формування трикомпонентної моделі інформаційної стійкості України (стратегічні комунікації, медіаграмотність, кіберзахист). Отже, особистий внесок дисертанта полягає в поглибленні теоретико-методологічного осмислення інформаційного тероризму, типологізації інформаційних загроз, розробленні концепції інформаційної стійкості та узагальненні міжнародного досвіду кіберзахисту. Наукові праці здобувача засвідчують вагомий внесок у становлення сучасної української наукової школи дослідження інформаційної безпеки й стратегічних комунікацій.

Апробація результатів дисертації. Основні результати дисертаційного дослідження апробовано на 19 наукових заходах, конференціях, круглих столах тощо, а саме: «Сучасні соціально-гуманітарні дискурси» (Дніпропетровськ, 2014), «Перспективи розвитку науково-практичних досліджень у сфері гуманітарних та суспільних наук» (Київ, 2014), «Актуальні проблеми країнознавчої науки» (Луцьк, 2015), «Зміни в соціально-економічному розвитку країни» (Чернівці, 2015), «Актуальні проблеми зовнішньої політики України» (Чернівці, 2015), «Актуальні проблеми країнознавчої науки» (Луцьк, 2015), «Проблеми і перспективи практичної реалізації наукових досліджень» (Чернівці, 2016), «Актуальні проблеми регіональних досліджень» (Луцьк, 2017), «Проблеми та перспективи наукових досліджень» (Чернівці, 2018), «Інформаційна війна як новий вимір геополітичної ривалізації» (Луцьк, 2019), «Міжнародні та регіональні системи: актуальні питання міжнародних відносин і регіональних студій» (Луцьк, 2019), «Інформаційна війна як новий вимір геополітичної ривалізації» (Луцьк, 2019), «Інформаційна гігієна як напрям національної безпеки» (Луцьк, 2021), «Актуальні проблеми міжнародних відносин і регіональних досліджень» (Луцьк, 2021), «Стратегічні комунікації в контексті безпекової політики: європейський і глобальний рівні» (Луцьк, 2022), «Мультидисциплінарні підходи до аналізу суспільно-політичних проблем в умовах російсько-української гібридної війни» (Львів, 2022), «Актуальні проблеми міжнародних відносин і регіональних досліджень»

(Луцьк, 2023), «Зовнішнє інформаційне маніпулювання та втручання в умовах сучасних конфліктів», (Луцьк, 2025), «Європейська інтеграція України: виклики, досвід, перспективи» (Луцьк, 2025). Також здійснено апробацію основних положень дисертації в професійній діяльності в соціокультурній сфері, здобувачка брала участь у низці курсів і тренінгів. Крім того, основні ідеї дисертації пройшли апробацію на науково-методологічних семінарах кафедр міжнародних відносин і регіональних студій, міжнародних комунікацій та політичного аналізу ВНУ імені Лесі України.

Публікації. Основні положення та висновки дисертаційного дослідження опубліковано здобувачем у 44 працях, у тому числі 7 – це статті в наукових виданнях, що входять у наукометричні бази Scopus та Web of Science, 16 – публікації в наукових фахових виданнях України, 3 – у зарубіжному фаховому виданні, 2 – підрозділи в колективних монографіях, 3 – у довідково-енциклопедичних виданнях, 13 – тези доповідей.

Структура та обсяг дисертаційного дослідження. Дисертація складається зі вступу, 5 розділів, 15 підрозділів та висновків, 8 додатків. Загальний обсяг дисертації становить 470 сторінок, із них 360 сторінок – основний текст, 57 сторінок – список використаних джерел (567 найменувань).

ОСНОВНИЙ ЗМІСТ ДИСЕРТАЦІЇ

У ***Вступі*** дисертаційної роботи обґрунтовано актуальність теми, що зумовлена стрімким зростанням ролі інформаційного простору у формуванні політичних рішень, суспільних настроїв та безпекових стратегій держав. Підкреслено, що інформаційний тероризм перетворюється на новітню форму глобальної загрози, спроможну руйнувати не лише інфраструктуру чи комунікаційні системи, а й підвалини довіри, легітимності й демократичної стабільності. Визначено мету, завдання, об’єкт і предмет дослідження; окреслено його теоретико-методологічну основу, яка поєднує положення політичного реалізму, конструктивізму та неоінституціоналізму. Також аргументовано вибір міждисциплінарного підходу, що дав змогу комплексно проаналізувати феномен інформаційного тероризму у взаємозв’язку політичних, комунікаційних, безпекових і правових процесів.

Розділ 1 «Дослідження тероризму в контексті сучасних міжнародних відносин» має концептуально-теоретичний характер. У ньому розкрито еволюцію уявлень про тероризм у контексті глобалізаційних процесів, визначено його інформаційний вимір і концептуальні підходи до аналізу інформаційних загроз у політичній науці.

У *підрозділі 1.1. «Генеза та концептуалізація поняття «тероризм» у*

політологічному дискурсі» розглянуто динаміку розвитку тероризму від традиційних форм насильства до новітніх, мережевих і гібридних проявів, зумовлених процесами глобалізації, технологічного прогресу та інформатизації. Зазначено, що тероризм перетворився на складне багатовимірне явище, у якому поєднано політичні, економічні, культурні й інформаційні чинники. Глобальні комунікаційні мережі, соціальні медіа та цифрові платформи створили нові можливості для поширення радикальних ідеологій, мобілізації прихильників і маніпуляції суспільною свідомістю. Підкреслено, що в епоху постправди основним ресурсом терористичних угруповань стає не фізичне насильство, а контроль над інформаційними потоками, здатність викликати страх і дестабілізувати державні інститути через інформаційно-комунікаційні засоби. Саме це зумовило формування феномену інформаційного тероризму, який, на відміну від класичного, діє не через знищення матеріальних об'єктів, а через вплив на когнітивну сферу, суспільні емоції та ціннісні орієнтації. У підрозділі зазначено, що сучасний тероризм – це продукт глобалізаційних процесів, у межах яких взаємозалежність держав поєднується з підвищенням вразливості до інформаційних загроз.

У підрозділі 1.2 «Теоретико-методологічні підходи до аналізу глобалізаційних і цифрових трансформацій тероризму» визначено методологічні основи та науково-джерельне забезпечення дослідження інформаційного тероризму. Обґрунтовано доцільність міждисциплінарного підходу, що поєднує інструментарій політичної науки, теорії міжнародних відносин, комунікативістики, безпекових студій і кібернетики. До основних методів належать аналіз, синтез, порівняння, індукція, дедукція, контент- і дискурс-аналіз, а також метод case study, що забезпечує глибоке вивчення конкретних випадків інформаційних атак. Методологічну основу становить поєднання неореалістичного, конструктивістського та неоінституціонального підходів, що дає змогу простежити, як інформаційні інструменти впливають на структуру влади, політичні рішення й поведінку акторів міжнародної системи. Джерельну базу дослідження становлять офіційні документи ООН, НАТО, ЄС, ОБСЄ, національні стратегії інформаційної та кібербезпеки провідних держав світу, аналітичні звіти міжнародних організацій, публікації у фахових наукових виданнях і результати моніторингів цифрового простору. Особливу увагу приділено аналізу інформаційних кампаній та операцій, спрямованих на підрив демократичних інститутів, що дало змогу ідентифікувати механізми інформаційного терору та їх вплив на міжнародну стабільність.

Третій підрозділ 1.3 «Методологія та джерельна база дослідження тероризму в контексті міжнародної безпеки» стосується аналізу методологічних засад феномену тероризму як багатовимірного суспільно-

політичного явища, що істотно впливає на сучасну систему міжнародної безпеки. Виходимо з необхідності відмови від традиційного негативістського трактування тероризму, пропонуючи його осмислення крізь призму конструктивістського підходу, який уможливлює аналіз тероризму як політичного інструменту й чинника глобалізаційних трансформацій. Застосовано системний, структурно-функціональний та івент-аналіз, що сприяє комплексному вивченню генези, функцій і наслідків терористичних практик у зовнішньополітичних стратегіях провідних держав. Підкреслено важливість урахування політичних, ідеологічних та інформаційних аспектів тероризму в контексті гібридних війн і глобальної конкуренції. Джерельна база охоплює широкий спектр зарубіжних та вітчизняних наукових праць, аналітичних матеріалів, документів міжнародних організацій. Окрему увагу приділено проблемі дефініційної невизначеності понять «тероризм» й «антитероризм», відсутності уніфікованих підходів у правовій площині, що ускладнює формування ефективних міжнародних механізмів протидії. У підрозділі наголошено на потребі переосмислення епістемологічних підходів до аналізу тероризму та формування нової коеволюційної парадигми політичного пізнання, спроможної адекватно відобразити взаємозалежність людини, суспільства й глобальної безпеки. Зроблено висновок, що комплексне та багаторівневе дослідження тероризму є передумовою для розроблення інноваційних стратегій протидії, спрямованих не лише на ліквідацію наслідків, а й на усунення соціально-політичних причин його виникнення.

У розділі 2 «Інформаційний вимір тероризму в глобальному середовищі безпеки» здійснено аналіз інформаційного тероризму як чинника трансформації сучасної системи міжнародних відносин. Простежено, як інформаційні технології, цифрові медіа та комунікаційні платформи змінюють характер міжнародних конфліктів, структуру глобальної безпеки й баланс сил між державами. Обґрунтовано, що інформаційний тероризм набуває системного характеру та є не лише інструментом дестабілізації, а й елементом нової стратегії впливу в геополітичному просторі, поєднуючи військові, психологічні, економічні й культурні виміри гібридної агресії.

У *підрозділі 2.1 «Події 11 вересня 2001 р. як детермінанта цифрової трансформації тероризму»* здійснено аналіз подій 11 вересня 2001 р. як ключового чинника, що спричинив цифрову трансформацію тероризму та радикально змінив архітектоніку міжнародної безпеки. Визначено, що теракти в США стали не лише каталізатором глобальних антитерористичних процесів, а й фактором перегляду зовнішньополітичних доктрин провідних держав світу, передусім США й Росії. Показано, що «чорний вівторок» започаткував нову епоху інформаційних і медіавійн, у межах яких формувався цифровий простір

легітимації силових дій, політичного контролю та маніпулювання масовою свідомістю. Розкрито, що трагедія 11 вересня стала каталізатором переходу від традиційних до цифрових форм терористичної діяльності, у яких інформаційно-комунікаційні технології перетворилися на інструмент пропаганди, вербування й координації дій терористичних мереж. Проаналізовано, як під впливом цих подій трансформувалися концепти національної безпеки, політичної відповідальності та глобального лідерства, а також як інституціоналізовано ідеологію «боротьби зі світовим злом» у контексті американського геополітичного домінування. Зроблено висновок, що події 11 вересня 2001 р. стали поворотним моментом у становленні цифрової доби тероризму, який набув мережевого, інформаційно-гібридного характеру, що, своєю чергою, потребує перегляду стратегій міжнародного співробітництва у сфері безпеки та комунікаційної політики держав.

Підрозділ 2.2 «Інформаційний тероризм у структурі сучасного міжнародного тероризму: сутність, механізми, прояви» стосується дослідження феномену інформаційного тероризму як складової частини сучасного міжнародного тероризму; розкрито його сутність, механізми та форми прояву в контексті трансформації системи міжнародної безпеки. Показано, що інформація стала стратегічним ресурсом, а інформаційна безпека – ключовим елементом національної й міжнародної стабільності. Проаналізовано роль міжнародних інституцій (ООН, НАТО, ОБСЄ, ЄС) у регулюванні використання інформаційних технологій та протидії кібератакам, пропаганді й дезінформації. З'ясовано, що інформаційний тероризм є одним із головних викликів глобальній безпеці, оскільки спроможний дестабілізувати політичні системи без застосування збройної сили. Обґрунтовано потребу комплексного підходу до протидії – технічного, правового й комунікаційного, розвитку стратегічних комунікацій і міжнародної співпраці. В українському контексті він постає як інструмент гібридної війни РФ, спрямований на підрив довіри до держави та її міжнародного іміджу, що зумовлює необхідність зміцнення національної системи інформаційної безпеки.

У *підрозділі 2.3 «Інформаційний тероризм як компонент інформаційної війни»* проаналізовано, як феномен інформаційного тероризму змінює архітектуру міжнародної безпеки, створюючи нові форми уразливості для держав і міжнародних організацій. Відзначаємо, що інформаційна агресія порушує класичні принципи суверенітету, колективної оборони та довіри в міждержавних відносинах. Інформаційний тероризм розглянуто як структурний чинник дестабілізації глобальної системи, що руйнує усталені механізми безпекового співробітництва. Особливу увагу приділено ролі НАТО, ЄС й ООН у формуванні політик протидії інформаційним загрозам, а також ініціативам

України щодо зміцнення національної інформаційної стійкості. У висновках підрозділу наголошено, що нові виклики потребують перегляду підходів до міжнародної безпеки, де поряд із військовими та економічними факторами визначальними стають когнітивний і комунікаційний компоненти. Отже, інформаційний тероризм трансформує саму логіку безпекової взаємодії у XXI ст., вимагаючи переосмислення стратегій національного й глобального рівнів.

У розділі 3 «Інформаційна війна як форма глобального інформаційного протистояння» переосмислено феномен інформаційних воєн як ключового середовища поширення інформаційного тероризму та формування нової системи глобальних безпекових викликів. Розглянуто еволюцію воєнних стратегій від традиційних до когнітивно-комунікаційних, визначено структуру, інструменти й наслідки застосування інформаційної зброї, а також окреслено концепт інформаційної стійкості як провідного напряму протидії інформаційному тероризму.

У підрозділі 3.1 «Інформаційний тероризм у системі інформаційних війн: взаємозв'язки та інституціональні характеристики» розкрито взаємозалежність між феноменами інформаційної війни та інформаційного тероризму, які розглянуто як взаємодоповнювальні компоненти єдиного гібридного простору. Проаналізовано розвиток концепцій «війни четвертого покоління», мережево-центричних і проксі-конфліктів, що доводять зміщення акценту з фізичного на когнітивний рівень боротьби. Доведено, що інформаційний тероризм функціонує як структурний елемент гібридних воєн, де метою є не лише дестабілізація, а й контроль над інтерпретацією реальності. Визначено, що сучасні держави стають учасниками «інформаційного поля бою», де об'єктом впливу є масова свідомість, а головним ресурсом — дані. Підкреслено роль інституціональних механізмів, спрямованих на координацію державної політики інформаційної безпеки, розбудову національних центрів стратегічних комунікацій і розвиток міжнародного співробітництва у сфері цифрової протидії.

У *підрозділі 3.2 «Інформаційна війна та інформаційна зброя: функції, цілі, інструменти впливу»* систематизовано інструментарій інформаційних воєн і розкрито зміст поняття інформаційної зброї як комплексу технологічних, когнітивних та комунікаційних засобів впливу. Визначено, що інформаційна зброя діє на рівнях мови, символів, медіа, соціальних мереж і цифрових платформ, створюючи альтернативні реальності та підмінюючи факти емоційно забарвленими наративами. Особливу увагу приділено технологіям дезінформації, фейковим кампаніям, маніпуляціям громадською думкою, кібератакам і когнітивним операціям. Проаналізовано приклади втручань у

виборчі процеси, масові психологічні кампанії страху та приклади «інформаційного тиску» в міжнародних відносинах. Зроблено висновок, що головна мета застосування інформаційної зброї полягає не в знищенні противника, а в нав'язуванні йому потрібного бачення реальності, підриві довіри до власних інститутів і створенні стану постійної невизначеності.

Підрозділ 3.3 «Формування інформаційної стійкості як напряму протидії інформаційному тероризму» стосується розкриття концепту інформаційної стійкості як ключового напряму протидії інформаційному тероризму на національному та міжнародному рівнях. Визначено інформаційну стійкість як багаторівневу систему, що поєднує технологічні, комунікаційні, освітні та правові механізми захисту від деструктивних інформаційних впливів. Для інтегрального вимірювання рівня інформаційної стійкості запропоновано формулу:

$$ІСІС=0.25КС+0.25ЦК+0.25ІД+0.25ІС,$$

де:

КС – когнітивна стійкість;

ЦК – цифрова компетентність;

ІД – інституційна довіра;

ІС – інформаційна стабільність.

У роботі показано, що ефективна протидія можлива лише за умови синергії державних інститутів, громадянського суспільства, медіа та міжнародних партнерів. Особливу увагу приділено досвіду ЄС і НАТО у формуванні політик інформаційної безпеки, створенні центрів стратегічних комунікацій (STRATCOM) та ініціативах з підвищення медіаграмотності. Український контекст розглянуто як приклад практичної реалізації концепції стійкості в умовах російської агресії – через розвиток системи державних стратегічних комунікацій, волонтерських аналітичних спільнот, цифрових волонтерів й інформаційних кампаній, спрямованих на зміцнення довіри та національної ідентичності. Доведено, що формування інформаційної стійкості є не лише оборонною реакцією, а й довгостроковою стратегією розвитку демократичного суспільства, у якому інформаційна безпека стає складовою частиною політичної культури й основою суверенності в цифрову епоху.

Розділ 4 «Порівняльний аналіз національних стратегій протидії інформаційному тероризму» має аналітико-порівняльний характер. Здійснено аналіз міжнародного досвіду протидії інформаційному тероризму та формуванню інформаційної стійкості держав у цифрову епоху. Виконано порівняльне дослідження політик кібер- й інформаційної безпеки США, ЄС, Індії, Китаю, країн Африки та Латинської Америки з метою визначення універсальних принципів побудови ефективної системи захисту від

інформаційних загроз.

У підрозділі 4.1 «Нормативно-інституційні засади забезпечення інформаційної безпеки та кіберстійкості в США і ЄС» проведено комплексний аналіз еволюції нормативно-правових та організаційних механізмів забезпечення інформаційної безпеки в США і Європейському Союзі. Розкрито історичні етапи становлення державних стратегій кіберзахисту – від перших концепцій початку 2000-х років до сучасних, орієнтованих на кіберстійкість, партнерство держави й приватного сектору та колективну безпеку в цифровому просторі. У роботі простежено, як теракти 11 вересня 2001 р. стали каталізатором для формування нової американської парадигми національної безпеки, що включає інформаційний та кібернетичний вимір. Докладно охарактеризовано основні документи стратегічного планування США: «Національну стратегію захисту кіберпростору» (2003), «Огляд із кібербезпеки» (2009), «Ініціативу зі всеосяжної національної кібербезпеки» (2010), стратегії 2011, 2018 і 2023 рр., а також президентський указ № 14028 (2021), який започаткував модернізацію архітектури Zero Trust. Окреслено нормативно-правові основи інформаційної політики США: закони про комп'ютерну безпеку, удосконалення інформаційної безпеки, комп'ютерне шахрайство, свободу інформації та захист персональних даних. Особливу увагу приділено інституційній структурі – діяльності Агентства з кібербезпеки та безпеки інфраструктури (CISA), Кіберкомандування США (USCYBERCOM), Департаменту внутрішньої безпеки, Секретної служби й інших відомств. Показано, що американська модель ґрунтується на принципах превентивності, системності, розвитку кіберстрахування, інформаційної грамотності та партнерства держави й бізнесу.

Європейський досвід представлено через аналіз директив і стратегій ЄС: «Стратегії боротьби з тероризмом» (2005), директив NIS (2013) та NIS2 (2020), «Європейського порядку денного з безпеки» (2015), «Директиви з боротьби з тероризмом» (2017), а також оновленої «Стратегії кібербезпеки ЄС» (2020). Висвітлено діяльність Агентства ЄС із кібербезпеки (ENISA), створеного у 2004 р., та його роль у моніторингу ризиків, розбудові механізмів реагування, підвищенні цифрової грамотності й координації між державами-членами. Проаналізовано інституційну практику країн ЄС – Естонії, Німеччини, Франції, Норвегії та Фінляндії, – які демонструють різні моделі реалізації політики кіберзахисту.

Підкреслено, що США і ЄС сформували різні, але взаємодоповнювальні архітектури інформаційної безпеки: американська система має виразно централізований та наступальний характер, тоді як європейська – багаторівнева, кооперaційна й правозахисна. Обидві моделі поєднує спільне розуміння важливості цифрової грамотності, публічно-приватного партнерства, протидії

дезінформації та розбудови стійких інституцій. Зроблено висновок, що нормативно-інституційні засади інформаційної безпеки США і ЄС становлять основу формування трансатлантичної архітектури кіберстійкості, що ґрунтується на демократичних цінностях, верховенстві права й міжнародному співробітництві.

Підрозділ 4.2 «Моделі державного інформаційного контролю: порівняльний аналіз практик Китаю, Японії та Індії» – це аналіз, що стосується порівняльного дослідження моделей державного інформаційного контролю в трьох провідних азійських державах – Японії, Китаї та Індії, – які репрезентують різні політичні системи, культурні традиції й нормативно-інституційні підходи до забезпечення інформаційної безпеки. У роботі простежено, як історичні, політичні та соціокультурні чинники формують специфіку інформаційної політики кожної країни, визначаючи баланс між свободою слова, правом на приватність і державним контролем цифрового середовища.

Розділ розпочинається з аналізу японської моделі, що демонструє унікальне поєднання демократичних принципів, технологічної досконалості та соціокультурної відповідальності. Вона ґрунтується на принципах soft law, саморегуляції, партнерства держави з бізнесом і розвитку корпоративної етики. Правову основу становлять закони про захист персональних даних, доступ до публічної інформації, базові принципи кібербезпеки (2014) та активну кібероборону (2025). Система координується через Національний центр стратегій кібербезпеки (NISC), Міністерство економіки, торгівлі та промисловості (METI) й Національне агентство цифрових технологій (Digital Agency). Японська модель вирізняється сервісним підходом, поширеним аутсорсингом у сфері кіберзахисту, високим рівнем цифрової грамотності та культурою консенсусу. Водночас наявність неявної цензури, системи пресклубів і корпоративної самообмеженості журналістів обмежує прозорість у кризових ситуаціях. Попри це, Японія формує модель гнучкої демократичної кіберстійкості, заснованої на довірі, правовій відповідальності та балансі інтересів держави, бізнесу й суспільства.

Китайська модель, навпаки, представлена як приклад авторитарного цифрового контролю. Її концептуальною основою є ідея «інформаційного суверенітету» та збереження монополії Комуністичної партії Китаю на управління інформаційними потоками. Законодавчу базу формують так звана тріада CSL–DSL–PIPL — Закон про кібербезпеку (2017), Закон про безпеку даних (2021) і Закон про захист персональної інформації (2021), доповнені актами щодо алгоритмічних рекомендацій, дипфейків, генеративного ШІ й державних таємниць. Центральним координатором є Адміністрація кіберпростору Китаю (CAC). Ключові інструменти – «Великий китайський

фаєрвол», система соціального кредиту, масштабне алгоритмічне моделювання поведінки користувачів і залучення «50-центових армій» до інформаційних кампаній. Контроль за інформацією поєднується з розвитком Digital Silk Road у межах ініціативи «Один пояс – один шлях», що розширює вплив КНР у цифровому просторі інших держав. Китай демонструє феномен «стійкості без довіри», коли технічна досконалість і стабільність системи забезпечуються через репресивні механізми й придушення критичного мислення.

Індія репрезентує демократично-еволюційну модель інформаційної безпеки, що поєднує ліберальні цінності з прагматичною цифровою модернізацією. Основу становлять Закон про інформаційні технології (2000, із поправками 2008 р.), Закон про захист цифрових персональних даних (2023), Національна політика у сфері кібербезпеки (2013) та Національні рекомендації з інформаційної безпеки. Інституційну інфраструктуру становлять CERT-In, Рада безпеки даних Індії (DSCI), Національний центр захисту критичної інфраструктури й Асоціація кібербезпеки Індії (NCSAI). Індія акцентує увагу на розвитку аутсорсингових моделей, міжнародному партнерстві, кіберосвіті та формуванні професійної культури безпеки; водночас через нерівномірну цифрову грамотність і фрагментарність регулювання, залишається вразливою до кібератак і витоків даних, однак зберігає високий потенціал для подальшого посилення кіберстійкості..

У *підрозділі 4.3 «Національні стратегії протидії інформаційному тероризму в країнах Африки та Латинської Америки: регіональні особливості»* проаналізовано особливості проявів інформаційного тероризму й механізмів його протидії в країнах Африки та Латинської Америки. Підкреслено, що обидва регіони поєднують високі темпи цифровізації зі слабкими державними інституціями, що створює сприятливі умови для поширення дезінформації, кіберзлочинності й пропаганди. В африканському контексті інформаційний тероризм проявляється через активність джихадистських медіаструктур (Global Islamic Media Group, GIMF), які використовують цифрові платформи для ідеологічної мобілізації та координації терактів. Незважаючи на ухвалення низки стратегій кібербезпеки в країнах-членах САДК, створення національних агентств й ініціатив (Єгипет, Зімбабве, Нігерія), континент залишається одним із найуразливіших через слабке правове регулювання, нестачу фахівців і низький рівень інформаційної грамотності. У країнах Латинської Америки інформаційний тероризм має переважно кримінально-політичний характер. У Бразилії, попри розвиток Національної стратегії кібербезпеки й закону LGPD, частими залишаються фішингові атаки та кіберзлочини, а система кіберзахисту потребує модернізації. У Мексиці інформаційний тероризм тісно пов’язаний із діяльністю наркокартелів (Сіналоа, Los Zetas, CJNG), які використовують

соціальні мережі для залякування й пропаганди. Урядові ініціативи, зокрема Національна стратегія кібербезпеки 2017 р., не гарантують високої ефективності через корупцію та слабкий контроль. У підсумку встановлено, що рівень інформаційної стійкості в Африці залишається низьким, у Латинській Америці – середнім, а в Бразилії – відносно вищим завдяки розвиненій нормативній базі. Ефективна протидія інформаційному тероризму потребує поєднання правових, технологічних й освітніх інструментів, розвитку цифрової культури та міжнародної координації дій.

Розділ 5 «Протидія Україні інформаційному тероризму РФ: виклики, досвід та перспективи» має прикладний характер, стосується комплексного аналізу інформаційної агресії Російської Федерації проти України, її етапів, цілей, інструментів і наслідків, а також стратегічних напрямів удосконалення державної політики протидії інформаційному тероризму. На основі системного підходу розкрито еволюцію російських інформаційно-психологічних операцій, український досвід кіберзахисту, роль законодавчих і міжнародних механізмів у зміцненні інформаційного суверенітету держави.

Підрозділ 5.1 «Інформаційна агресія Російської Федерації проти України: етапи, цілі, інструменти впливу» здійснено системний аналіз інформаційної агресії Російської Федерації проти України як ключового інструменту реалізації гібридної стратегії Кремля. Простежено етапи її становлення – від формування проросійського медіаполя на початку 2000-х років до розгортання масштабних інформаційно-психологічних операцій у період після 2014 р. та безпрецедентних форм кібертерору після початку повномасштабного вторгнення 2022 р. Підкреслено, що інформаційна агресія РФ має комплексний характер, поєднуючи політичні, економічні, культурні та технологічні механізми впливу. Серед головних інструментів визначено державні медіа RT і Sputnik, кібератаки типу NotPetya, масовані DDoS-атаки на урядові ресурси, використання deepfake-технологій і дезінформаційних кампаній у соціальних мережах. Україна у відповідь створила національну інфраструктуру інформаційної безпеки: ухвалено Доктрину інформаційної безпеки, Закон «Про основні засади забезпечення кібербезпеки України», сформовано інституції CERT-UA, Кіберполіцію, Ситуаційний центр СБУ, налагоджено взаємодію з НАТО і ЄС. У межах аналізу застосовано SWOT-модель, що дало змогу визначити сильні сторони української системи кіберзахисту (наявність досвіду, міжнародне партнерство, розвиток нормативної бази) та її слабкі місця (кадровий дефіцит, фрагментарність політики, вразливість ІТ-інфраструктури). Підкреслено, що формування цілісного інформаційного щита можливе лише за умови інтеграції правових, технологічних і просвітницьких інструментів, спрямованих на підвищення інформаційної культури суспільства та консолідацію державних і

громадських зусиль у сфері кібероборони.

У підрозділі 5.2 «Стратегічні напрями вдосконалення державної політики протидії інформаційному тероризму в Україні» розкрито стратегічні засади, напрями та механізми вдосконалення державної політики України у сфері протидії інформаційному тероризму, який у сучасних умовах є ключовою загрозою національній безпеці. Проаналізовано стан і перспективи вдосконалення державної політики України у сфері протидії інформаційному тероризму в умовах гібридної війни. Розкрито системний характер російської інформаційної агресії, що поєднує пропаганду, дезінформацію, кібероперації та інформаційно-психологічні впливи, спрямовані на підрив єдності суспільства, делегітимізацію влади й дискредитацію України на міжнародній арені. Окреслено основні інструменти агресії РФ – державні медіа, ботоферми, кіберпідрозділи, агентів впливу та соцмережеві кампанії. Проаналізовано реакцію України: санкційне блокування проросійських медіа, ухвалення Закону «Про медіа», участь у міжнародних ініціативах (EUvsDisinfo, NATO StratCom COE) й активність громадянського суспільства (StopFake, Detector Media, VoxUkraine). Наголошено, що попри досягнення, інформаційна стійкість держави залишається вразливою через низький рівень критичного мислення, олігархічний вплив на медіа та поширення анонімних каналів. На основі досвіду США, ЄС й Естонії визначено п’ять стратегічних напрямів удосконалення політики: створення єдиного координаційного центру, упровадження архітектури Zero Trust, оновлення правового поля, розвиток кризових комунікацій і медіаосвіти. Узагальнено, що підвищення інформаційної стійкості України потребує поєднання правових, технічних, інституційних і когнітивних заходів. Такий підхід забезпечить перехід до проактивного управління інформаційними ризиками та зміцнить національний інформаційний суверенітет..

Підрозділ 5.3 «Роль інститутів громадянського суспільства у формуванні системи інформаційного захисту держави» стосується діяльності українських і міжнародних громадських організацій, волонтерських спільнот та незалежних аналітичних платформ, які стали важливою складовою частиною системи інформаційного спротиву російській агресії. Проаналізовано роботу таких структур, як InformNapalm, CAT-UA, Центр стратегічних комунікацій StratCom Ukraine, ініціативи «Українські кібервійська», а також локальні проєкти з медіаграмотності – «НотаЄнота», тренінги Тернопільського пресклубу, ініціативи ГО «Рівненська Горинь». Визначено, що ці організації виконують функцію «інформаційного щита» суспільства, поєднуючи моніторинг дезінформації, аналіз соціальних наративів, фактчекінг, навчання критичного мислення й розвиток цифрової компетентності громадян. Завдяки

волонтерському потенціалу, гнучкості та швидкому реагуванню на інформаційні загрози, такі структури нерідко ефективніше за державні інституції виявляють фейки, викривають пропагандистські мережі й протидіють психологічним операціям супротивника. У підрозділі показано, що саме громадянське суспільство стало центром формування нової моделі інформаційної безпеки, заснованої на партнерстві держави, медіа, науковців і громадських активістів. Ця мережа ініціатив – від OSINT-розслідувань та кібервідсічі до антифейкових освітніх програм – формує унікальну архітектуру інформаційної стійкості, яка забезпечує сталу демократичну протидію дезінформації, зміцнює національну єдність і посилює міжнародну довіру до України як держави, що активно вибудовує власну систему стратегічних комунікацій у межах європейської безпекової спільноти.

У ***Висновках*** наведено основні результати дослідження та визначено напрями подальших наукових розвідок.

ВИСНОВКИ

У роботі досліджено концепт тероризму в теорії міжнародних відносин як складне, багатовимірне та політично чутливе явище з безпековим, соціальним, інформаційним й ідеологічним вимірами. Відсутність універсального визначення зумовлена як складністю феномену, так і політичними інтерпретаціями. Тероризм еволюціонував від державного інструменту насильства до засобу недержавних акторів і став формою асиметричної боротьби, що охоплює фізичне насильство, кібератаки та інформаційні маніпуляції. Використання медіа й цифрових платформ посилило спроможність терористичних структур впливати на глобальні процеси. У неореалістичній, неоліберальній і конструктивістській парадигмах його розглянуто як засіб впливу, загрозу, що потребує координації, або як соціальний конструкт, сформований дискурсом. Отже, тероризм – динамічне поняття, що змінюється під впливом трансформацій міжнародного безпекового середовища й розвитку технологій, а його осмислення є основою ефективної стратегії глобальної протидії.

Схарактеризовано міжнародний тероризм, який сьогодні є не лише загрозою безпеці, а й наслідком глобалізаційних суперечностей між цивілізаціями та політичними системами. Його еволюція зумовлена асиметрією розвитку, геополітичними амбіціями провідних держав і кризою ціннісної рівноваги у світовому порядку. Тероризм стає реакцією на нерівність та виключення, породжені глобалізацією, тому подолання цього явища потребує не лише силових заходів, а й нової парадигми міжнародної взаємодії, побудованої на

принципах цивілізаційного діалогу, справедливості, інклюзивності та етичної відповідальності.

Доведено, що інформаційний тероризм став невід'ємною й надзвичайно небезпечною складовою частиною міжнародного тероризму в умовах цифрової доби. Його вплив поширюється не лише на інфраструктуру, а й на свідомість суспільства, використовуючи інструменти масових маніпуляцій, кіберзлочинів і спеціальних інформаційних операцій. Як засвідчив аналіз наукових підходів, це явище охоплює низку форм – від психологічного тиску й дезінформації до кібернападів на критичні об'єкти держав. Небезпека інформаційного тероризму полягає в його невидимості, швидкості поширення та спроможності руйнувати довіру до влади, інституцій і цінностей. У сучасному світі, де межа між війною й миром розмита, інформаційна зброя часто є не менш потужною за фізичну. Тому боротьба з інформаційним тероризмом повинна стати пріоритетом як для національної безпеки, так і для міжнародного співробітництва, що потребує оновлення правових механізмів, розвитку цифрової стійкості, створення ефективної системи реагування на інформаційні загрози.

Підкреслено, що міжнародний тероризм є складним і динамічним явищем, що постійно трансформується під впливом змін глобального безпекового середовища. Попри значні наукові зусилля, рівень теоретичного осмислення цього феномену все ще не відповідає масштабам його загрози, а одновимірні підходи до протидії виявляються неефективними. Серед ключових чинників терористичної активності виокремлено соціально-економічну поляризацію, релігійний фанатизм, ідеологічний радикалізм, прагнення до самовизначення та міжцивілізаційні розломи. Особливо небезпечним проявом сучасності став технологічний тероризм, що ґрунтується на використанні кіберзброї, засобів масового ураження й елементів «сурогатних» воєн. Глобалізаційні процеси водночас сприяють поширенню екстремістських ідеологій та ускладнюють міжнародне правове реагування. Суб'єктна структура тероризму розширюється: поряд із традиційними угрупованнями діють транснаціональні мережі й гібридні утворення з рисами квазідержав. Унаслідок цього концепти війни та безпеки потребують переосмислення, адже терористичні дії дедалі частіше набувають характеру воєнних операцій із політичними цілями й масштабними наслідками.

Закцентовано увагу на тому, що проблема тероризму сьогодні виходить за межі питань безпеки, відображаючи глибокі структурні дисбаланси сучасного світового порядку. Події 11 вересня 2001 р. та подальші воєнні операції показали обмежену ефективність суто силових і правових підходів. Реальна боротьба з тероризмом потребує усунення його першопричин – бідності, соціальної нерівності, релігійної нетерпимості та викривлених наслідків глобалізації. Необхідний перехід від реактивної до превентивної стратегії, що передбачає

спільні дії держав, міжнародних організацій і громадянського суспільства. Тероризм є не окремим злом, а симптомом глибших цивілізаційних криз, тому його подолання можливе лише в межах ширшої концепції глобальної безпеки, справедливості та сталого розвитку. Теракти 11 вересня стали переломним моментом у переосмисленні міжнародної безпеки й ролі держав у протидії новим загрозам. Вони засвідчили асиметричний характер терористичних викликів у глобалізованому світі. Реакцією США стали воєнні кампанії в Афганістані й Іраку, які викликали критику через відхід від принципів колективної безпеки та утвердження концепції «превентивної війни». Ці події спричинили геостратегічні зміни й посилення пропагандистських практик, коли риторика «світової боротьби з тероризмом» використовувалася для легітимації політичних і воєнних рішень, не спрямованих на усунення глибинних причин цього явища.

Сучасна епоха характеризується стрімкою еволюцією форм воєнних дій, що виходять за межі традиційної «гарячої» війни та охоплюють широкий спектр асиметричних, інформаційних, медійних і проксі-конфліктів. Війна четвертого покоління, гібридна війна, iWar, медіавійна, асиметричні та посередницькі війни дедалі частіше використовуються як ефективні інструменти впливу в умовах, коли відкриті бойові дії стають політично й економічно невигідними для глобальних акторів. Ці форми конфліктів орієнтовані не лише на військове послаблення противника, а й на підрив його внутрішньої стабільності, ідентичності, економіки, легітимності влади та морального духу населення.

Доведено, що інформаційна війна в умовах сучасного глобального протистояння перетворилася з допоміжного інструменту на стратегічну вісь гібридної агресії. Вона охоплює широке коло цілей – від дезорганізації комунікацій, підриву інформаційної інфраструктури, впливу на психіку населення до створення альтернативної реальності в масовій свідомості. Такі війни ведуться не лише державами, а й транснаціональними структурами, терористичними угрупованнями, хактивістами та приватними суб’єктами.

Сучасні інформаційні конфлікти не обмежуються межами кіберпростору – вони інтегруються в політичну, економічну, культурну сфери життя, вражаючи і структури влади, і масову свідомість, і економіку. Особливо небезпечними є новітні форми мережево-центричної війни, які поєднують інформаційний, психологічний та економічний впливи в єдиний інструмент стратегічного тиску. Така війна не потребує фізичної окупації території – вона спрямована на руйнування довіри, ідентичності, морального духу населення, що створює передумови для внутрішньої дестабілізації. Отже, у XXI ст. саме інформаційна війна визначає нову парадигму глобального конфлікту, і країни, які не готові до активної інформаційної самооборони та стратегічних комунікацій, ризикують утратити не лише контроль над власним інформаційним простором, а й

суверенітет. Ефективна протидія цим загрозам потребує національної інформаційної доктрини, розвитку цифрового опору, критичного мислення громадян і тісної міжнародної кооперації.

Підкреслено, що інформаційна зброя стала одним із ключових інструментів сучасного конфлікту, спроможним завдавати значної шкоди державам без фізичного втручання. Її специфіка полягає у використанні дезінформації, маніпулятивних наративів, кібероперацій, психологічного впливу, фейків і спеціальних інформаційних операцій, які спрямовані на підрив морального духу, дестабілізацію політичної ситуації, ослаблення державного управління та ерозію суспільної довіри. У контексті гібридної війни Росії проти України інформаційна зброя стала стратегічним засобом впливу: зокрема, через поширення пропаганди, підрив довіри до державних інституцій, делегітимацію збройних сил, а також стимулювання паніки, зневіри й розколу всередині суспільства. Такий тип зброї не потребує значних матеріальних витрат, але має високий рівень ефективності завдяки цифровим технологіям, соціальним мережам і глобальному інформаційному простору. Використання інформаційної зброї також змінює традиційні уявлення про воєнні конфлікти – стирається межа між миром та війною, цивільним і військовим, обороною й нападом. У цих умовах держави повинні розвивати спроможність до ідентифікації, нейтралізації та попередження інформаційних атак, зміцнювати цифрову стійкість, стратегічні комунікації й навички інформаційної гігієни громадян. Отже, інформаційна зброя становить загрозу національній безпеці на рівні, зіставному із застосуванням традиційних форм збройної сили, що потребує адекватних заходів реагування як у внутрішній, так і в міжнародній політиці безпеки.

Проаналізовано як у сучасному цифровому середовищі інформаційна стійкість перетворюється на ключовий інструмент протидії інформаційному тероризму, що ускладнює безпекову ситуацію, підриває демократичні інституції та порушує суспільну згуртованість. Комплексний аналіз свідчить, що загроза інформаційного тероризму проявляється не лише через кібернапади чи фейки, а й через деструктивний вплив на політичну культуру, громадянську активність і довіру до державних інституцій. Інформаційна стійкість охоплює широкий спектр заходів – від розвитку стратегічних комунікацій та медіаграмотності до забезпечення цифрової безпеки й інституційного контролю за дотриманням інформаційних прав. Центральним елементом у протидії деструктивним впливам є синергія між державними структурами, громадянським суспільством і технічними інструментами, спрямованими на виявлення, блокування й нейтралізацію інформаційних атак.

Відзначено, що особливу роль у зміцненні інформаційної стійкості відіграють медіаосвіта та критичне мислення, що формують у громадян здатність

розпізнавати маніпуляції й фейки; інституційна спроможність держави, уключаючи роль омбудсмена або інформаційного комісара у захисті інформаційних прав; інструменти ЄС, які слугують ефективною моделлю багаторівневої протидії гібридним загрозам; цифрова безпека та нормативне регулювання, що забезпечують технологічний і правовий захист національної інформаційної інфраструктури.

Схарактеризовано досвід України та країн ЄС, який підтверджує ефективність комплексного підходу, що поєднує превентивні, просвітницькі, нормативні й технічні засоби. У цьому контексті створення незалежного інституту Інформаційного комісара в Україні є логічним кроком до конституційного закріплення інформаційної демократії та адаптації до європейських стандартів. Отже, інформаційна стійкість повинна розглядатися як стратегічна категорія національної безпеки, що забезпечує спроможність суспільства й держави протистояти інформаційним загрозам, зберігати соціальну згуртованість, посилювати громадянську відповідальність і формувати безпечне інформаційне середовище в умовах гібридної війни та цифрових трансформацій.

У XXI ст. інформаційні технології стали основою глобальної взаємодії, економічної діяльності й державного управління. Водночас цифровізація зумовила зростання кіберзагроз, що ставить під сумнів безпечність і стійкість національних інформаційних інфраструктур. Аналіз міжнародного досвіду свідчить, що успішна інформаційна політика потребує поєднання кількох ключових елементів: ефективного нормативно-правового регулювання, належної організації системи управління, розвитку цифрової грамотності населення та впровадження інструментів кіберстрахування. Росія, Китай, а також недержавні актори, зокрема терористичні угруповання, активно адаптують ці моделі до власних стратегічних цілей, що створює серйозні виклики для традиційної системи міжнародного права та безпеки. Такі війни часто залишаються нижче від порога офіційного оголошення конфлікту, що ускладнює міжнародне реагування й відкриває простір для правового нігілізму. Водночас західні демократії, з огляду на високу вразливість до втручання у свої відкриті суспільства, змушені шукати нові моделі стійкості – від реформування інформаційної політики до запровадження систем протидії кіберзагрозам і гібридним операціям.

Доведено, що поширення таких форм війни свідчить про глибоку трансформацію безпекового середовища XXI ст., у якому ключову роль відіграють не лише військові ресурси, а й технологічна перевага, інформаційний контроль, психологічний вплив та здатність до адаптивного мислення. Це потребує оновлення концепцій національної й міжнародної безпеки, міжвідомчої координації, стратегічних комунікацій і консолідації зусиль демократичного

світу задля ефективного реагування на новітні виклики та загрози. США демонструють системний підхід до інформаційної безпеки, зокрема завдяки ухваленню стратегій кіберзахисту, створенню спеціалізованих державних інституцій (CERT, DHS, C3), розвитку цифрової освіти й співпраці з приватним сектором. Суттєве значення має також баланс між захистом персональних даних і забезпеченням інформаційної безпеки в межах загальнодержавної стратегії. Європейський Союз формує комплексну політику кібербезпеки через директиви, мережі CERT, агенцію ENISA, а також заохочення міждержавної кооперації у сфері кіберзлочинності. Успішні приклади Естонії, Франції та Норвегії демонструють ефективність поєднання правового регулювання, інституційної стійкості й стратегічного планування.

У сучасних умовах цифровізації проблема інформаційної безпеки набула глобального значення та стала стратегічним пріоритетом держав. Аналіз досвіду Японії, Китаю й Індії свідчить про різні моделі забезпечення кіберзахисту. У Японії створено розвинену інституційну систему з акцентом на соціальну відповідальність і сервісний підхід, хоча правова база залишається фрагментарною. Китай використовує кібербезпеку як інструмент зовнішньої політики, поєднуючи технологічну експансію з концепцією «кіберсуверенітету», що викликає занепокоєння щодо прозорості та прав людини. Індія, маючи потужний IT-сектор, розвиває інституції кіберзахисту й залучає інвестиції, проте стикається з нерівномірністю цифрового розвитку. Досвід цих держав підкреслює необхідність для України формувати багаторівневу систему інформаційної безпеки, що поєднує технологічні, правові та гуманітарні аспекти й ґрунтується на балансі між безпекою й свободою інформації.

Проаналізовано забезпечення інформаційної безпеки в країнах Латинської Америки, що ускладнюється фрагментарністю законодавства, браком координації та ресурсів. Мексика обмежується декларативною політикою, Бразилія розвиває децентралізовану модель із пріоритетом цифрових прав, Аргентина й Колумбія роблять кроки до створення інституцій кіберзахисту, однак стикаються з нестачею фінансування та узгодженості дій. Для регіону важливо розвивати національні координаційні центри, уніфікувати законодавство, підвищувати цифрову освіту та зміцнювати міжнародну співпрацю. Досвід Латинської Америки може бути корисним Україні для розбудови стійкої цифрової інфраструктури в умовах гібридних загроз і політичної турбулентності.

Закцентовано увагу на тому, що африканські країни перебувають у фазі активної цифрової трансформації, що поряд із можливостями породжує нові ризики – зростання кіберзлочинності та інформаційного тероризму. Основними проблемами залишаються низька цифрова грамотність, слабка правова база й

нестача координації. Попри створення стратегій кібербезпеки в Єгипті, ПАР, Кенії чи Танзанії, регіон залишається вразливим до кібератак і втручань. Для підвищення стійкості потрібно узгодити регіональні політики, адаптувати законодавство, розвивати кадровий потенціал та цифрову культуру. Комплексний і скоординований підхід є ключем до ефективної протидії інформаційному тероризму й формування безпечного цифрового середовища в Африці.

Доведено, що інформаційна агресія Російської Федерації проти України є системною, комплексною та стратегічно вмотивованою формою гібридної війни, що поєднує пропаганду, дезінформацію, кібероперації, інформаційно-психологічні впливи й маніпулятивні кампанії в цифровому середовищі. Її мета – підірвати політичну стабільність, делегітимізувати державні інститути, ослабити національну єдність і знизити міжнародну підтримку України. Аналіз засобів та механізмів, що використовуються РФ, свідчить про високу технологічність, адаптивність і мімікрію під демократичні цінності, зокрема свободу слова, плюралізм та відкритість інформаційного простору. В умовах триваючої війни особливо небезпечною є здатність ІПсО формувати викривлену реальність, деморалізувати населення й впливати на громадську думку як в Україні, так і за її межами.

У результаті дослідження зроблено висновок, що ключовими чинниками ефективної інформаційної безпеки є наявність чіткої законодавчої бази та стратегій кіберзахисту; інтеграція державних, приватних і міжнародних зусиль; розвиток цифрової грамотності населення; створення спеціалізованих органів реагування на кіберінциденти; посилення міжнародного співробітництва в межах глобальної цифрової екосистеми. Зважаючи на гібридні загрози, що постійно еволюціонують, та зростаючу інтенсивність кібератак, забезпечення інформаційної безпеки стає не лише технічним викликом, а й пріоритетом державної політики й міжнародної співпраці.

Аргументовано тезу про те, що інформаційна стійкість є політичним та інституційним маркером зрілості держави, що визначає її спроможність протидіяти інформаційному тероризму без руйнування демократичних засад. Високі значення ICIC корелюють із рівнем відкритості, правової культури й суспільної довіри; натомість низькі – із режимним контролем або структурною слабкістю. Порівняльний аналіз підтверджує: інформаційна стійкість має три моделі – демократичну, режимно-центричну та транзитивну; лише перша забезпечує сталу безпеку й легітимність. Для України релевантним є комбінований підхід, який поєднує технологічну модернізацію, розвиток критичного мислення, медіаосвіту та інституційну координацію з партнерами ЄС і НАТО.

Незважаючи на значні зусилля Української держави у сфері протидії – від нормативно-інституційних ініціатив до блокування проросійських ресурсів, зміцнення стратегічних комунікацій і співпраці з міжнародними партнерами, – Україна залишається вразливою до інформаційних атак. Серед її ключових проблем – низький рівень цифрової освіти, обмеженість незалежних медіа, поширення анонімного деструктивного контенту та повільна реакція на новітні загрози, зокрема з боку генеративного ШІ. У цьому контексті забезпечення інформаційної безпеки повинно стати постійним елементом національної безпекової політики. Протидія інформаційно-маніпулятивному впливу РФ мусить спиратися на такі стратегічні підходи, як підвищення цифрової й медіаграмотності громадян, формування культури критичного мислення, розвиток незалежних медіа, розширення міжнародної співпраці в межах системи інформаційної безпеки та створення ефективної державної політики з превентивного захисту інформаційного простору. Лише в умовах поєднання інституційної спроможності, громадянської активності й міжнародної солідарності можливе стримування російської інформаційної експансії та збереження інформаційного суверенітету України.

Проаналізовано як громадянське суспільство стало ключовим чинником забезпечення інформаційної безпеки України під час гібридної війни. Від початку агресії РФ у 2014 р. неурядові організації, журналістські ініціативи, OSINT-спільноти та волонтерські об’єднання – StopFake, Detector Media, InformNapalm, українські кібервійська, Лабораторія цифрової безпеки – узяли на себе функції моніторингу, спростування дезінформації, цифрового патрулювання й створення контрнаративів. Їхня діяльність сприяла підвищенню цифрової грамотності, формуванню нових стандартів кіберзахисту та міжнародному визнанню українського досвіду. Водночас громадський сектор стикається з проблемами: нестачею фінансування, фрагментарною координацією з державою, правовою неврегульованістю й етичними ризиками, зокрема щодо обробки персональних даних. Приклад проєкту «Миротворець» демонструє потребу у встановленні чітких рамок взаємодії між державними та недержавними структурами. Ефективний захист інформаційного простору потребує партнерства між державою й громадськістю, створення національної стратегії співпраці та розбудови мережі цифрової безпеки. Українське громадянське суспільство довело свою дієздатність як суб’єкт інформаційного спротиву, а його досвід інтегрується в європейські та натівські стратегії безпеки, стаючи взірцем для інших країн.

СПИСОК ПРАЦЬ, ОПУБЛІКОВАНИХ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, у яких опубліковані основні наукові результати дисертації

Статті у виданнях, що індексуються в міжнародних наукометричних базах даних Scopus та Web of Science:

1. Vozniuk Ye., Kunytskyy M., Mykhaliuk N., Novak O. International Information Security. *AD ALTA: Journal of Interdisciplinary Research.* 2021. Vol. 11, Issue 01. P. 381–385 (авторський внесок 25 %). **Web of Science, Scopus, Q3.**

DOI: 10.33543/1101.

URL: https://www.magnanimitas.cz/ADALTA/1101/papers/A_voznyuk.pdf.

2. Shuliak A., Vozniuk Ye., Patlashynska I. [et al.]. The Impact of the 4.0 Technological Revolution on the Hybrid War of the Russian Federation in Ukraine. *AD ALTA: Journal of Interdisciplinary Research.* 2022. Special Issue (12/02-XXX). P. 159–164 (авторський внесок 30 %). **Web of Science, Scopus, Q3.**

DOI: 10.33543/1202.

URL: http://www.magnanimitas.cz/ADALTA/120230/papers/K_15.pdf.

3. Kachkovska L., Blahovirna N., Vozniuk Ye. [et al.]. Documentary-Information Communication in Public Administration: Legal Aspects and Digital Transformation. *International Journal of Basic and Applied Sciences.* 2025. 14 (3) P. 42–47 (авторський внесок 30 %). **Scopus, Q4.**

DOI: 10.14419/v1jmq034.

URL: www.sciencepubco.com/index.php/IJBAS.

4. Shuliak A., Voznyuk Ye, Patlashinska I., Shuliak N. Info-Analytic Support for Ukrainian-Polish Cross-Border Cooperation: a Case Study of Euro-Regions. *Codrul Cosminului*. 2020. Issue 2. Vol. 26. P. 431–454 (авторський внесок 30 %) **Scopus, Q2.**

DOI: 10.4316/CC.2020.02.007.

URL: https://codrulcosminului.usv.ro/article-7-vol-26-2-2020/

5. Kotsan N., Kopachinska G., Vozniuk Ye., Kotsan R. Basic Models of Protection and Functioning of the Ukrainian Border in Modern Geopolitical Realities: a View from Ukraine. *European Spatial Research and Policy.* 2022. Vol. 29. N. 1. P. 79–95 (авторський внесок 25 %). **Web of Science**, **Scopus, Q2.**

DOI: 10.18778/1231-1952.29.1.04.

URL: https://czasopisma.uni.lodz.pl/esrap/article/view/9908.

Статті у наукових фахових виданнях України:

6. Vozniuk E. North Korea Nuclear Program as the Main Source of Instability in Northeast Asia. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини*. 2017. № 6 (355). С. 4–11.

URL: http://nbuv.gov.ua/UJRN/Nvvnum_2017_6_3.

7. Hych I., Vozniuk E. The Threats and Opportunities of Crisis on Ukraine's Accession to the EU. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини*. 2017. № 6 (355). С. 12–16 (авторський внесок 80 %).

URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Nvvnum_2017_6_4.

8. Shimuleni M. S., Vozniuk E. Regional Integration and Development: a Theoretical Review of the SADC Region. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини*. 2017. № 10 (359). С. 111–116 (авторський внесок 80 %).

URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Nvvnum_2017_10_21.

9. Vozniuk E. Principles and Features of Japan's Information Security System. *Політичне життя.* 2017. № 4. С. 8–12.

URL: https://jvestnik-politology.donnu.edu.ua/index.php/pl/article/view/4933.

10. Hrynchuk V., Vozniuk E. Information Security of India. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини.* 2018. № 1 (374). С. 15–20 (авторський внесок 75 %).

11. Ничипорчук Н., Вознюк Є. Секрет успіху США у сфері інформаційної безпеки. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2018. № 1 (3). С. 66–71 (авторський внесок 75 %).

DOI: 10.29038/2524-2679-2018-01-66-71.

URL: https://relint.vnu.edu.ua/index.php/relint/article/view/28.

12. Vetrov K., Voznyuk Ye. Information Terrorism as a Modern Threat for Information Security of European States. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2019. № 1 (5). С. 34–42 (авторський внесок 80 %).

DOI: 10.29038/2524-2679-2019-01-34-41.

URL: https://relint.vnu.edu.ua/index.php/relint/article/view/88.

13. Вознюк Є. Поширення впливу мексиканських картелів засобами інформаційних технологій і пропаганди. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини.* 2019. № 8 (392). С. 35–41.

URL: https://evnuir.vnu.edu.ua/bitstream/123456789/22741/1/35-41.pdf.

14. Бекеша О., Матюшок В., Вознюк Є. Розвиток кібербезпеки Бразилії на сучасному етапі. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини*. 2020. № 2 (406). С. 52–58. (авторський внесок 70%).

URL: https://evnuir.vnu.edu.ua/bitstream/123456789/22730/1/%d0%9d%d0%92_%d0%9c%d0%92_2020_2-52-58.pdf.

15. Вознюк Є., Романцов Д., Рошко І. Кібербезпека в умовах російської агресії. *Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія: Міжнародні відносини*. 2020. № 2 (406). С. 58–66 (авторський внесок 70 %).

URL: https://evnuir.vnu.edu.ua/handle/123456789/22733.

16. Вознюк Є. Громадські об'єднання на захисті інформаційного простору України. *Міжнародні відносини, суспільні комунікації та регіональні студії*. 2021. № 3 (11). С. 48–61.

DOI: 10.29038/2524-2679-2021-03-48-61.

URL: https://relint.vnu.edu.ua/index.php/relint/article/view/230.

17. Вознюк Є. Особливості поширення російських фейків в Україні. *Історико-політичні проблеми сучасного світу:* зб. наук. ст. Чернівці: Чернівец. нац. ун-т, 2021. Т. 44. С. 52–63.

URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=Ippss_2021_44_8.

18. Вознюк Є. SWOT-аналіз стану інформаційної безпеки України. *Науковий часопис НПУ імені М. П. Драгоманова. Серія 22: Політичні науки та методика викладання соціально-політичних дисциплін.* 2021. 22 (30). С. 116–124.

DOI: 10.31392/pnspd.v22i30.1147

URL: https://sj.udu.edu.ua/index.php/pnspd/article/view/116-129.

19. Вознюк Є., Андрюхіна В. Порівняльний аналіз кібербезпеки Європейського Союзу. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2025. № 2 (22). С. 161–180 (авторський внесок 75 %).

DOI: 10.29038/2524-2679-2025-02-136-154.

URL: https://relint.vnu.edu.ua/index.php/relint/article/view/454.

20. Kachkovska L., Vozniuk Ye. Countering Information Threats in Ukraine: Current Issues for Solving at the State Level. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2024. № 1 (18). С. 85–102 (авторський внесок 60 %).

DOI: 10.29038/2524-2679-2024-01-85-102.

URL: https://relint.vnu.edu.ua/index.php/relint/article/view/367.

Статті в іноземних журналах:

21. Novak O., Vozniuk Ye. The Influence of the Information Society Development on Political Ideologies. *Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate.* 2021. 11 (1). P. 19–26 (авторський внесок 70 %).

DOI: 10.24917/26578549.11.1.2.

URL: https://studiadesecuritate.uken.krakow.pl/wp-content/uploads/sites/43/2021/06/2_Novak_Vozniuk.pdf.

22. Morenchuk A., Vozniuk Ye., Morenchuk A. junior Sources of Russian Policy Aggressiveness. *Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate*. 2024. 14 (1). P. 91–105 (авторський внесок 60 %).

DOI: 10.24917/26578549.14.1.5.

URL: https://studiadesecuritate.uken.krakow.pl/wp-content/uploads/sites/43/2025/04/5.-Andriy-Morenchuk.pdf.

23. Bairak S., Buslenko V., Vozniuk Ye. State Policy in the Field of Information Security Providing in Ukraine. *Annales Universitatis Paedagogicae Cracoviensis*. *Studia de Securitate.* 2024. 14 (1). P. 107–117 (авторський внесок 35 %).

DOI: 10.24917/26578549.14.1.6

URL: https://studiadesecuritate.uken.krakow.pl/wp-content/uploads/sites/43/2025/04/6.-Serhii-Bairak.pdf.

Розділи в монографіях:

24. Vozniuk E. Information Terrorism as a Modern Dynamic Part of International Terrorism. *International and National Security: Politics, Information, Ecology, Economy:* collective monograph / ed. by A. Mytko. Kyiv: MPBP «Hordon», 2018. P. 165–174. 320 p.

ISBN 978-966-8398-55-1

URL: https://evnuir.vnu.edu.ua/handle/123456789/23755

25. Вознюк Є. Європейський інспектор із захисту даних. *Зелений і безпечний Європейський Союз:* монографія / [А. О. Бояр (кер. авт. кол.), І. В. Кицюк, Н. І. Романюк та ін.]; за ред. А. О. Бояра, В. Й. Лажніка. Луцьк: Вежа-Друк, 2023. С. 82–85.

ISBN 978-966-940-505-0,
URL: d084d0a1-d0bad0bdd0b8d0b3d0b0_final.pdf (wordpress.com).

Наукові праці,
які засвідчують апробацію матеріалів дисертації:

26. Підлісний А. Ю., Вознюк Є. В. Участь України у миротворчих операціях НАТО. *Актуальні проблеми країнознавчої науки:* матеріали II Міжнар. наук.-практ. інтернет-конференції (м. Луцьк, 14–15 трав. 2015 р.) / за ред. В. Й. Лажніка. Луцьк: Вежа-Друк, 2015. С. 187–189.

27. Подолець С. В., Вознюк Є. В. Особливості забезпечення сучасної інформаційної безпеки держави. *Проблеми і перспективи практичної реалізації наукових досліджень:* матеріали XXXVI Міжнар. наук.-практ. конф., Чернівці, 15–16 берез. 2016 р. Т. 2. Київ: Наук.-вид. центр «Лабораторія думки», 2016. С. 31–33.

28. Voznyuk E. V., Voinkova A. O. The Features of Providing Information Security of European Countries. *Актуальні проблеми регіональних досліджень*: матеріали I Міжнар. наук.-практ. інтернет-конференції (м. Луцьк, 11–12 груд. 2017 р.) / за ред. В. Й. Лажніка. Луцьк: Вежа-Друк, 2017. С. 236–240.

29. Ничипорчук Н. С., Вознюк Є. В. Нормативно-правове регулювання інформаційної безпеки США. *Проблеми та перспективи наукових досліджень:* матеріали LX Міжнар. наук.-практ. конф. (Чернівці, 15–16 черв. 2018 р.). Київ: Науково-видавничий центр «Лабораторія думки», 2018. С. 28–30.

30. Джигалюк Н., Вознюк Є. Особливості стратегічних комунікацій у німецькомовному інформаційному просторі з точки зору національної безпеки України. *Інформаційна війна як новий вимір геополітичної ривалізації:* матеріали II міжнар. наук.-практ. конф. Луцьк, 2019. С. 8–12.

31. Вознюк Є. В. Особливості політичної комунікації сьогодні. *Міжнародні та регіональні системи: актуальні питання міжнародних відносин і регіональних студій*: зб. тез Міжнар. наук-практ. конф. (м. Луцьк, 17 трав. 2019 р.) / за ред. В. Й. Лажніка та С. В. Федонюка. Луцьк: Вежа-Друк, 2019. С. 96–98.

32. Вознюк Є., Дідух Д. Ботоферми як загроза інформаційній безпеці. *Інформаційна гігієна як напрям національної безпеки*: матеріали I міжнар. наук. онлайн-конф. Луцьк, 2021. С. 23–25.

33. Horbach A., Vozniuk Ye. Influence of Non-Governmental Organizations on Information Security of Ukraine. *Актуальні проблеми міжнародних відносин і регіональних досліджень*: матеріали Міжнар. наук.-практ. інтернет-конф.

(м. Луцьк, 6 груд. 2021 р.) / за ред. В. Й. Лажніка. Луцьк: Вежа-Друк, 2021. С. 167–170.

URL: https://wiki.vnu.edu.ua/images/d/df/%D0%9A%D0%9E%D0%9D%D0%A4-2021-%D0%B3%D1%80%D1%83%D0%B4.pdf.

34. Шуляк А., Вознюк Є. Інформаційна сингулярність російсько-української війни 2022 р. *Стратегічні комунікації в контексті безпекової політики: європейський і глобальний рівні*: матеріли інтернет-конф. / за заг. ред. Н. Карпчук. Луцьк: ВНУ ім. Лесі Українки, 2022. С. 67–72.

URL: https://inter-dep.vnu.edu.ua/wp-content/uploads/2022/06/%D0%9C%D0%B0%D1%82%D0%B5%D1%80-%D0%BA%D0%BE%D0%BD%D1%84%D0%B5%D1%80-19.05.22.pdf

35. Вознюк Є., Крищук А. Початок активного російсько-українського протистояння в кіберпросторі. *Мультидисциплінарні підходи до аналізу суспільно-політичних проблем в умовах російсько-української гібридної війни*: матеріали. міжнар. круглого столу (28 квіт. 2022 р.). Львів: Вид-во Львів. політехніки, 2022. С. 18–21.

URL: https://lpnu.ua/sites/default/files/2022/6/24/news/20253/tpp-verstkatezikrugliystil2022-1.pdf.

36. Baranyk O. S., Vozniuk Ye. V. Global Impact of Information Weapons. *Актуальні проблеми міжнародних відносин і регіональних досліджень:* матеріали III Міжнар. наук.-практ. інтернет-конф. (м. Луцьк, 15 лист. 2023 р.) / укладачі: С. Кулик; О. Борисюк (технічна підтримка). Луцьк: Волин. нац. ун-т ім. Лесі Українки, 2024. С. 250–253.

37. Вознюк Є. Кібербезпека Європейського Союзу: інституційна архітектура та сучасні виклики. *Зовнішнє інформаційне маніпулювання та втручання в умовах сучасних конфліктів*: матеріли інтернет-конф. / за заг. ред. проф. Н. Карпчук. Луцьк: ВНУ ім. Лесі Українки, 2025. С. 106–110.

URL: https://fimieu.wordpress.com/%d0%ba%d0%be%d0%bd%d1%84%d0%b5%d1%80%d0%b5%d0%bd%d1%86%d1%96%d1%97/

38. Завадська В., Вознюк Є. Інформаційна та кібербезпека країн Африки. *Європейська інтеграція України: виклики, досвід, перспективи:* матеріали міжнар. наук.-практ. конф. (Луцьк, 21 трав. 2025 р.) / за заг. ред. С. Федонюка. Луцьк: ВНУ ім. Лесі Українки, 2025. С. 76–79

URL: https://euaccession.wordpress.com/wp-content/uploads/2025/06/d09ad09ed09dd0a4d095d0a0d095d09dd0a6d086d0af-euaccession-2025-1-1.pdf

Наукові праці,
які додатково відображають наукові результати дисертації:

39. Khoma N. Vozniuk E Turkey's Middle East Policy: Vectors, Aims and Results *Studia Politica. Romanian Political Science Review*. Vol. XXI. No. 2, 2021. P. 577–601. **Scopus, Q4**

URL: https://www.researchgate.net/profile/Nataliya-Khoma-2/publication/361182581_Turkey's_Middle_East_Policy_Vectors_Aims_and_Results_Studia_Politica_Romanian_Political_Science_Review_2021_Vol_XXI_No_2_R_578-601/links/62a18d4bc660ab61f86df60a/Turkeys-Middle-East-Policy-Vectors-Aims-and-Results-Studia-Politica-Romanian-Political-Science-Review-2021-Vol-XXI-No-2-R-578-601.pdf.

40. Kotsan R., Kotsan N., Kopachinska G. Vozniuk E. Transformations of Ukrainian-Polish border regions transformation: experience of Ukraine. *Forum Geographic.* Vol. 21. Issue 1. 2022. Pp. 92–101. ***Web of Science***

DOI 10.5775/fg.2022.071.i.

URL: http://forumgeografic.ro/wp-content/uploads/2022/1/Kopachinska.pdf

41. Кулик С., Вознюк Є. Фейк російської пропаганди: Олена Підгрушна – снайпер АТО. *Міжнародні відносини, суспільні комунікації та регіональні студії.* 2021. № 1 (9). С. 83–101. ***Фахове видання України.***

DOI: 10.29038/2524-2679-2021-01-82-101

URL: https://relint.vnu.edu.ua/index.php/relint/uk/article/view/125.

42. Вознюк Є. Війна свідомості (консцієнтальна війна), гібридні загрози, інформаційна війна, інформаційний омбудсмен, інформаційний тероризм, культура інформаційної безпеки, методи боротьби з інформацією в електронних засобах масової інформації, операційна безпека «OPSEC». *Глосарій: навчальний енциклопедичний словник-довідник з питань інформаційної безпеки* / за заг. ред. д- ра. політ. наук, проф. А. М. Шуляк, 2019. С. 42–45; 54–56; 135–138; 165–166; 168–170; 242–244; 289–293; 343–345.

43. Wozniuk E. Informacyjny ombudsman; Metody walki z informacją w elektronicznych środkach masowego przekazu. *Vademecum bezpieczeństwa informacyjnego* / red. nauk. Olga Wasiuta, Rafał Klepka. T. 1. Kraków: AT Wydawnictwo, Wydawnictwo LIBRON – Filip Lohner, 2019. P. 452–454, 647–651.

44. Wozniuk E. Terroryzm informacyjny. *Vademecum bezpieczeństwa informacyjnego* / red. nauk. Olga Wasiuta, Rafał Klepka. T. 2. Kraków: AT Wydawnictwo, Wydawnictwo LIBRON – Filip Lohner, 2019. P. 466–468.

АНОТАЦІЯ

Вознюк Є. В. Інформаційний тероризм як чинник впливу на міжнародну та національну безпеку. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора політичних наук за спеціальністю 23.00.04 – Політичні проблеми міжнародних систем і глобального розвитку. – Волинський національний університет імені Лесі України, м. Луцьк, 2025 р.

Дисертаційне дослідження є комплексною науковою працею, спрямованою на осмислення феномену інформаційного тероризму як новітньої форми гібридної агресії в системі глобальної безпеки. Актуальність теми зумовлена масштабним використанням інформаційних технологій у політичних, військових і соціальних конфліктах, що потребує розроблення нових теоретичних і практичних підходів до забезпечення стійкості держави в умовах інформаційних загроз.

Мета дослідження – виявлення сутності, структури та динаміки інформаційного тероризму як політичного й комунікативного феномену, визначення його впливу на міжнародну та національну безпеку, а також розроблення науково обґрунтованих механізмів протидії. У роботі сформульовано завдання, що охоплюють аналіз концептуальних підходів до вивчення тероризму в інформаційну добу, визначення типів і форм інформаційного терору, дослідження досвіду протидії цим явищам у провідних державах світу (США, країнах ЄС, Японії, КНР, Індії, державах Африки та Латинської Америки) й оцінку ефективності українських практик протидії дезінформації та кіберзагрозам у період російсько-української війни.

Методологічну основу становить поєднання системного, інституційного, порівняльного, структурно-функціонального, історичного й контент-аналізу. Застосовано як якісні, так і кількісні методи – від OSINT-моніторингу відкритих джерел до статистичного аналізу масштабів інформаційних атак і кампаній впливу. Таке поєднання забезпечило глибоке осмислення сутності феномену інформаційного тероризму та його трансформаційних наслідків.

Наукова новизна дослідження полягає в тому, що вперше:

– здійснено концептуалізацію поняття інформаційної стійкості як ключового елементу національної безпеки, що охоплює технічні, правові, організаційні, освітні й психологічні компоненти;

– обґрунтовано роль стратегічних комунікацій, медіаграмотності та інформаційної гігієни як елементів інформаційної оборони держави;

– систематизовано український досвід протидії інформаційним атакам, зокрема діяльність OSINT-спільнот, цифрових волонтерів, ініціатив StopFake, Detector Media тощо, і визначено їх роль у зміцненні інформаційної стійкості;

– розроблено типологію форм інформаційного тероризму (медіа-, кібер- та когнітивного) й подано хронологічну модель його еволюції від традиційних до цифрових форм насильства;

– сформульовано рекомендації щодо вдосконалення політики держави у сфері інформаційної безпеки, гармонізації національного законодавства з нормами ЄС і НАТО та розвитку партнерства між державою, громадянським суспільством і медіа у сфері протидії інформаційним загрозам.

Практичне значення результатів полягає в можливості використання напрацювань дисертації в діяльності урядових структур, відповідальних за інформаційну безпеку, розроблення стратегії протидії гібридним загрозам і дезінформації, а також у навчальному процесі – у межах дисциплін «Міжнародна безпека», «Стратегічні комунікації», «Кібербезпека», «Міжнародна інформація». Результати дослідження можуть бути корисними для підготовки аналітичних матеріалів, створення навчальних програм і розвитку аналітичних центрів із питань інформаційної та гуманітарної безпеки.

Особистий внесок здобувача полягає в поглибленні теоретико-методологічних засад дослідження інформаційного тероризму, розробленні концепції інформаційної стійкості як інструменту захисту національних інтересів, створенні типології інформаційних загроз й узагальненні міжнародного досвіду протидії інформаційним атакам.

Ключові слова: інформаційний тероризм, інформаційна стійкість, національна безпека, міжнародна безпека, громадянське суспільство, російсько-українська війна, гібридна війна, стратегічні комунікації, дезінформація, ЄС, Україна, НАТО, міжнародні організації, конфлікти.

ABSTRACT

Vozniuk Ye. V. **Information Terrorism as a Factor of Influence on International and National Security.** – Qualification Scientific Work in the Form of a Manuscript.

Dissertation for the degree of Doctor of Political Sciences in the speciality 23.00.04 – Political Problems of International Systems and Global Development. – Lesya Ukrainka Volyn National University, Lutsk, 2025.

The dissertation is a comprehensive study that explores the phenomenon of information terrorism as a new form of hybrid aggression within the contemporary

system of global security. The research is driven by the growing role of the information environment in shaping political decisions, societal perceptions, and security strategies of states, as well as by the urgent need to establish theoretical and practical frameworks for strengthening national resilience against information-based threats.

The purpose of the dissertation is to identify the essence, structure, and dynamics of information terrorism as a political and communicative phenomenon; to assess its impact on international and national security; and to develop scientifically grounded mechanisms of counteraction. The study's object is the phenomenon of information terrorism in the context of global transformations, while its subject comprises political, institutional, communicative, and normative mechanisms of its manifestation and neutralization.

The author set a series of research objectives, including: an analysis of conceptual approaches to terrorism in the information age; the identification of typologies and forms of information terrorism; a comparative study of counteraction strategies in leading states (the USA, EU countries, Japan, China, India, African and Latin American nations); and an assessment of Ukraine's experience in combating disinformation and hybrid aggression amid the ongoing Russian-Ukrainian war.

The methodological framework combines systemic, institutional, comparative, structural-functional, and historical approaches, along with qualitative and quantitative methods — including OSINT-based analysis of open sources and statistical data on information attacks and influence operations. This interdisciplinary synthesis enabled the researcher to examine the multidimensional nature of information terrorism as both a political instrument and a destructive communicative practice.

The scientific novelty of the study lies in several key contributions:

– for the first time, information terrorism is conceptualized as a political and institutional phenomenon that restructures the global security architecture and serves as an instrument of influence by both state and non-state actors;

– the dissertation introduces the concept of information resilience as an essential component of national security, encompassing technological, institutional, educational, and psychological dimensions;

– the author systematizes Ukraine's experience of countering information aggression, highlighting the activities of digital volunteer networks, OSINT communities, and civil society initiatives such as StopFake and Detector Media, and their role in strengthening societal resistance;

– a typology of information terrorism forms (media, cyber, and cognitive) and a chronological model of its evolution from traditional terrorism to digital aggression after September 11, 2001, are developed;

– a set of recommendations is formulated to enhance Ukraine's information security policy, align its legislative framework with EU and NATO standards, and

promote sustainable cooperation between the state, civil society, and the media in the field of countering information threats.

The theoretical significance of the dissertation lies in deepening the scientific understanding of hybrid threats in international relations, while its practical importance is demonstrated through the applicability of its results in designing state information security policies, developing national strategies for combating disinformation and psychological operations, and integrating the findings into educational programs on International Security, Strategic Communications, Cybersecurity, and Global Information Policy.

The author's contribution consists in advancing the theoretical and methodological basis for studying information terrorism, introducing the category of information resilience as a mechanism for safeguarding national interests, systematizing global approaches to information security, and substantiating Ukraine's innovative model of informational resistance during wartime.

The results of the research may serve as a foundation for further academic inquiry into the interdependence between information power, hybrid warfare, and global governance, as well as for the elaboration of practical tools aimed at enhancing democratic resilience and defending the integrity of the information space.

Key words: information terrorism, information resilience, national security, international security, civil society, Russian-Ukrainian war, hybrid war, strategic communications, disinformation, EU, Ukraine, NATO, international organisations, conflict.