consciousness, and the manipulation of ideological narratives as factors legitimizing political violence under conditions of socio-economic marginalization. The study examines theoretical approaches to understanding radicalization, extremism, and religious terrorism, and reveals the psychological dimensions of aggressive religious radicalization, including the role of anxiety, identity threat, and feelings of hopelessness. It is demonstrated that radical religious movements employ religious identity as a tool of social mobilization and justification of violence, appealing to the concepts of martyrdom and the sacralization of conflict.

Special attention is devoted to the impact of socio-economic inequality, the weakness of state institutions, and the lack of quality religious education on increasing population vulnerability to extremist propaganda. Based on analytical materials of the UNDP, UNICEF, UNESKO, UNODC it is argued that inclusive religious education can serve as an important factor in strengthening community resilience to radical narratives. The article concludes that countering radicalization associated with ideological and religious distortion requires an interdisciplinary approach that combines socio-economic development, educational strategies, and institutional strengthening, as well as the promotion of interfaith dialogue as a tool for reducing conflict potential.

Keywords: *extremism, radicalization, religious education, social marginalization, religious terrorism, Nigeria, Boko Haram.*

DOI https://doi.org/10.31392/UDU-nc.series22.2025.38.09
УДК 32:316.334.3:004.738.5(477)

Вячеслав Бараболя,
аспірант кафедри політичних наук,
Український державний університет імені Михайла Драгоманова
ORCID: https://orcid.org/0009-0006-9348-4922; e-mail: b.slava79@ukr.net

УЧАСТЬ ГРОМАДЯНСЬКОГО СУСПІЛЬСТВА У ПРОТИДІЇ ІНФОРМАЦІЙНИМ АТАКАМ

У статті розглянуто питання ролі громадянського суспільства в протидії інформаційним атакам в Україні в умовах гібридної війни. Показано, що зростання масштабів дезінформаційних кампаній та інформаційного тиску посилило значення горизонтальних мереж взаємодії громадян, експертних середовищ і волонтерських ініціатив, які змогли оперативно реагувати на виклики там, де державні інституції виявилися недостатньо гнучкими. Особливу увагу приділено аналізу інструментів, які використовуються громадськими структурами для захисту інформаційного простору: фактчекінг, медіамоніторинг, поширення верифікованих даних, інформаційно-просвітницькі кампанії, а також розвиток практик цифрової безпеки. Висвітлено приклади успішних ініціатив, що стали знаковими для українського досвіду – діяльність StopFake, Інституту масової інформації, OSINT-спільнот, громадських платформ із медіаграмотності. Акцентовано увагу на тому, що громадянське суспільство не лише доповнює державні стратегії протидії дезінформації, але й створює альтернативні канали комунікації, які підвищують довіру в суспільстві та зміцнюють стійкість демократичних практик. У статті також підкреслюється, що незважаючи на значний практичний внесок громадянських ініціатив, наукове вивчення їхньої ролі залишається недостатньою мірою розглянутим і фрагментарним, що обмежує можливості для систематизації досвіду та розробки довгострокових стратегій. Зроблено висновок, що подальший розвиток та інституційне закріплення громадянської участі у сфері інформаційної безпеки є стратегічним завданням, від якого залежить ефективність протидії зовнішнім загрозам, формування культури критичного мислення та посилення демократичної стійкості українського суспільства.

Ключові слова: *громадянське суспільство, інформаційна безпека, дезінформація, фактчекінг, цифрова стійкість, медіаграмотність, інформаційні атаки.*

Вступ. Протидія інформаційним атакам стала одним із ключових напрямів діяльності українського громадянського суспільства з 2014 року. Російська агресія супроводжувалася масштабними кампаніями дезінформації, пропаганди та маніпуляцій, спрямованих на підрив довіри до державних інститутів, деморалізації суспільства та послаблення міжнародної

підтримки України. В умовах обмежених ресурсів держави вагому частину завдань із виявлення, нейтралізації та спростування таких атак узяли на себе недержавні актори – громадські організації, волонтерські об'єднання, незалежні медіа та ініціативні групи.

Особливістю українського досвіду стало те, що громадянське суспільство змогло не лише компенсувати слабкі сторони державної комунікації, а й створити нові ефективні інструменти: від фактчекінгових платформ і мереж OSINT-дослідників до освітніх програм із медіаграмотності. Такі практики сприяли формуванню горизонтальних мереж довіри та комунікації, які підвищили суспільну стійкість до дезінформаційних впливів.

У сучасних умовах наукового осмислення потрібує не тільки емпіричний досвід протидії інформаційним атакам, але й питання інституціоналізації цих практик: як вони змінюють роль громадянського суспільства в системі національної безпеки, наскільки стійкими є, та які перспективи мають після закінчення війни.

Аналіз останніх досліджень і публікацій. Проблематика участі громадянського суспільства у сфері інформаційної безпеки та протидії дезінформації є предметом досліджень як українських, так і міжнародних авторів. У роботах Центру Разумкова та Київського міжнародного інституту соціології акцент зроблено на рівні довіри до громадських організацій та волонтерських ініціатив як визначальному чиннику їхньої ефективності у сфері протидії інформаційним загрозам [Razumkov, 2023; КМІС, 2024]. У колективних звітах Національного інститут стратегічних досліджень [НІСД, 2025] та публікаціях Л. Чистоклетова [2024] аналізуються виклики, пов'язані з поширенням дезінформації, та роль недержавних акторів у формуванні комунікативної стійкості.

Окрему увагу приділено діяльності фактчекінгових платформ (StopFake, VoxCheck), що визнані ефективними прикладами громадянської протидії дезінформації [Wilson, 2021], а також OSINT-спільнотам, які документують воєнні злочини та моніторять інформаційні потоки [Bellingcat, 2022; Ukraine today, 2025].

У міжнародних аналітичних звітах Європейської служби зовнішніх дій, Freedom House та East StratCom Task Force підкреслюється унікальність українського досвіду протидії дезінформації, який базується на синергії держави та громадянського суспільства [EEAS, 2024]. Загалом наукові та аналітичні публікації останніх років акцентують увагу на зростанні ролі громадянського суспільства у протидії дезінформаційним впливам, хоча цей напрям досліджень досі залишається відносно новим і недостатньо репрезентованим.

Метою статті є дослідження ролі громадянського суспільства у протидії інформаційним атакам, зосередивши увагу на механізмах залучення громадських організацій, експертних спільнот і волонтерських ініціатив до забезпечення інформаційної безпеки.

Основними завданнями є: проаналізувати інституційні та неформальні практики участі громадянського суспільства у сфері протидії дезінформації; визначити ключові інструменти і напрями діяльності (фактчекінг, медіамоніторинг, інформаційно-просвітницькі кампанії, цифрова безпека); оцінити рівень довіри до громадських ініціатив як чинник їх ефективності; визначити проблеми нерегулярності та фрагментарності соціологічних вимірювань у цій сфері; простежити перспективи інституційного закріплення участі громадянського суспільства в системі національної інформаційної безпеки.

Методологічну основу дослідження складає системний підхід, що дозволяє розглядати протидію інформаційним атакам як комплексний процес, у якому взаємодіють громадянські ініціативи, державні інститути та міжнародні партнери. Застосовано структурно-функціональний аналіз для вивчення ролі громадських організацій у зміцненні інформаційної стійкості. Використано компаративний метод для порівняння українського досвіду з практиками країн Центрально-Східної Європи. Методи контент-аналізу дали змогу дослідити інформаційні кампанії та публічні комунікації громадянських ініціатив. Метод кейс-стаді використано для розгляду діяльності окремої платформ (StopFake, Інститут

масової інформації, OSINT-спільноти) як прикладів успішної самоорганізації. Додатково застосовано елементи цифрової етнографії для аналізу особливостей взаємодії громадян у соціальних мережах і мережевих платформах, де відбувається мобілізація ресурсів для протидії дезінформації.

Результати та дискусії. Сьогодні інститут громадянського суспільства розглядається як одна з ключових підвалин демократичної державності, що забезпечує стабільність політичної системи, формування механізмів комунікації між владою та суспільством, а також легітимність процесу ухвалення політичних рішень.

Розвинене громадянське суспільство сприяє ефективному функціонуванню демократичних інститутів, адже воно не лише артикулює інтереси соціальних груп, але й створює систему їхнього представництва, впливаючи на політичний порядок денний. Ідеали ліберальної демократії – участь громадян у політичному житті, вільна реалізація прав і свобод, контроль над владою, прозорість і підзвітність – передбачають існування активної недержавної сфери, здатної врівноважувати діяльність органів державної влади та протидіяти проявам авторитаризму.

Глобалізація та стрімкий розвиток інформаційних технологій зробили державу й суспільство значно залежнішими від інформаційної сфери. Це дає можливості для швидкого поширення інформації, мобілізації, комунікацій, але і породжує ризики: пропаганди, дезінформації, інформаційних атак як зі зовнішніх, так і внутрішніх джерел.

Влада самостійно не спроможна ефективно захищати інформаційний простір від усіх загроз. Потреба в ресурсах (фінансових, кадрових, технологічних) забезпечує можливості окремих державних інституцій. У таких умовах громадянське суспільство (громадянські об'єднання (ГО), аналітичні центри, медіа) стає стратегічним партнером держави.

Актуальним проявом співпраці держави та громадянського суспільства стали ініціативи, що інтегрують медіа в процеси планування відновлення України. Зокрема, під час Конференції з відновлення України (URC-2025), яка відбулася у Римі, було запущено платформу «Media Recovery Partnership Track», покликану сприяти партнерству між медійною сферою, державними інституціями та донорськими проєктами у контексті повоєнної відбудови. Важливу роль у цьому процесі виконують ГО, серед яких, наприклад, ініціатива «Жінки в медіа» та низка інших об'єднань. Вони розробляють рекомендації для уряду та міжнародних донорів, зосереджуючи увагу на підтримці регіональних медіа, забезпеченні гендерно чутливого контенту та залученні журналістів до відбудовчих процесів [Петренко, 2025].

Не менш помітною є активність аналітичних центрів, які беруть участь у формуванні державної політики. Так, у 2025 році вони виступили зі зверненнями щодо процесу створення конкурсної комісії для призначення керівництва митної служби, що засвідчує їхню роль у забезпеченні прозорості та демократичного контролю за діяльністю органів влади [Інтерфакс-Україна, 2025].

За даними дослідження «Індекс медіаграмотності українців 2024», проведеного ГО «Детектор медіа» спільно з Національним проєктом «Фільтр» Міністерства культури та стратегічних комунікацій України, 65% українців мають вищий за середній рівень медіаграмотності, а 7% – високий. Проте, порівняно з попереднім роком, частка осіб із вищим за середнім рівнем знизилася з 76% до 72%, що частково пояснюється оновленням методології дослідженням, зокрема розширенням індикаторів цифрової грамотності, зокрема оцінки сприйняття та використання штучного інтелекту [Індекс медіаграмотності, 2025].

Ці дані свідчать про зростання медіаграмотності серед українців, зокрема вміння критично оцінювати медіаконтент, розпізнавати маніпуляції та помічати проникнення ворожих наративів. Це критично важливо для забезпечення інформаційної безпеки країни під час війни та в повоєнний період [Індекс медіаграмотності, 2025].

У протидії інформаційним атакам важливу роль відіграють три групи недержавних суб'єктів громадянського суспільства: громадські об'єднання, аналітичні центри та медіа. Останні, за даними IMI, перебувають під сильним фінансовим тиском: 67% редакцій відмовилися від нових проєктів і планів розвитку, переключившись на виживання [Опитування IMI, 2025]. Майже 45% редакцій скоротили аналітичні матеріали та розслідування через дефіцит фінансування [Опитування IMI, 2025]. Крім того, 29% медіа опинилися у стані виживання після припинення фінансування США [Буняк, 2025]. З іншого боку, довіра до громадських організацій у загальних опитуваннях лишається порівняно вищою, ніж до багатьох державних інститутів – наприклад, відповідно до опитування Центру Разумкова, близько 55% респондентів висловлювали довіру громадським організаціям, тоді як довіра до державного апарату була значно нижчою [Буняк, 2024].

Інформаційна агресія невід'ємна складова гібридної війни РФ проти України. Поєднання військових дій із активною розвідково-диверсійною діяльністю, політичним і економічним тиском і тотальною інформаційною експансією створює системну загрозу національній безпеці. Одним із ключових інструментів російської стратегії є операції немілітарного впливу – спеціальні інформаційні операції, активні заходи, маніпуляції в кіберпросторі, спотворення фактів, фальсифікація історії, приниження мови, культури, створення альтернативної (фальшивої) інформаційної картини.

Основна мета – розколоти українське суспільство зсередини через загострення існуючих політичних, регіональних, етнічних, соціально-економічних відносин. Такі тактики як: дискредитація влади, заклики до імпічменту, урядових відставок, розпуску парламенту; просування ідей федералізації чи ширшого самоврядування як засобу сепарації; створення та посилення негативних стереотипів між населенням тимчасово окупованих територій і основною Україною; інформаційні натяки на «особливі» економічні зони, порто-франко та інші форми територіальної чи політичної автономії.

Ресурси РФ у сучасній війні суттєво переважають українські, що стосується фінансового забезпечення, медійних мереж, технологій і кадрового потенціалу. У таких умовах відповідь України носить переважно асиметричний характер, зокрема через активне використання потенціалу громадянського суспільства. Недержавні актори здатні забезпечити достатню гнучкість і ефективність у протидії інформаційним атакам, створюючи синергію з державними інституціями.

Спостерігається декілька ключових тенденцій у розвитку участі громадянського суспільства у сфері інформаційної безпеки. Зростає кількість громадських організацій, що свідчить не лише про розширення громадянської активності, але й про посилення ролі організацій у волонтерській діяльності, підтримці прифронтових громад, захисту прав людини та антикорупційних ініціатив [Дузенко, 2025].

Значно розширюються форми та інструменти протидії дезінформації. Важливу роль відіграють фактчекінгові ініціативи, такі як StopFake чи VoxCheck, які системно спростовують ворожі наративи та підвищують рівень довіри до перевірених джерел інформації. Паралельно розвиваються OSINT-розслідування воєнних злочинів, які проводять як професійні, так і громадські організації, а також поширюються освітні програми з медіаграмотності, орієнтовані на регіональне населення, що знижує його вразливість до дезінформаційних впливів [Центр стратегічних комунікацій, 2024].

Державні центри стратегічних комунікацій та інформаційної безпеки залучають громадські організації до підготовки тренінгів, розробки навчальних матеріалів і консультацій із регуляторами медіа, зокрема Національною радою з питань телебачення і радіомовлення. Однією з ключових проблем є необхідність законодавчого визначення терміну «дезінформація» та запровадження чітких механізмів відповідальності за її поширення. Державні стратегії поступово інтегрують положення про роль громадянського сектору як партнера у виявленні, реагуванні та превентивних заходах.

Громадянське суспільство стикається з низкою викликів та обмежень. Серед них: дискредитаційні кампанії проти організацій, що отримують закордонне фінансування; поширення терміну «грантоїди» в публічному дискурсі; нестача фінансових і технологічних ресурсів для масштабних інформаційних кампаній; обмежені можливості контролю потоків російської пропаганди в соціальних мережах та месенджерах, де механізми модерації залишаються недостатньо ефективними [Грантоїдів на заводи, 2025]. У цьому контексті актуальним є створення координаційних платформ чи хабів, що об'єднували б досвід, аналітичні напрацювання та ресурси громадського сектору, держави й приватних структур.

Участь громадянського суспільства в протидії інформаційним атакам характеризується зростанням організаційної спроможності, розширенням інструментів впливу, налагодженням співпраці з державою та одночасним зіткненням із системними викликами, що підтверджує стратегічну значимість громадянського сектору як невід'ємного елемента національної інформаційної безпеки.

Важливою передумовою ефективності протидії інформаційній агресії є довіра до інституцій громадянського суспільства, зокрема, як зазначалося вище, до волонтерських і громадських організацій. Українські соціологічні центри, такі як КМІС та Центр Разумкова, час від часу включають у загальні модулі опитування, які фіксують рівень довіри до волонтерів та громадських організацій. Наприклад, у щорічному звіті КМІС (2024) зазначено, що 53,5% респондентів довіряють волонтерським організаціям, а 37% – громадським організаціям загалом [Грушецький, 2025].

У грудні 2023 року дослідження Центру Разумкова спільно з Фондом «Демократичні ініціативи» показало, що 63% українців довіряють громадським, а 86% – волонтерським організаціям [ZMINA, 2023].

Слід зауважити, що спеціалізовані дослідження, які приділили б виключну увагу оцінці довіри до ГО/аналітичних центрів із регулярними хвилями (наприклад, щоквартально або кожного півріччя), – надзвичайно рідкісні. Найближчим до такого стандарту є дослідження КМІС, яке хоча й включає ГО як одну зі соціальних інституцій у панелі, але не робить фокус лише на ГО, і відповідно дані про цю групу з'являються лише час від часу. Увагу до надійності вимірювань довіри до громадянського суспільства в Україні почали приділяти ще до 2020 року, але тоді йшлося здебільшого про волонтерські рухи та антикорупційні ГО, і збір даних не був систематичним. Наступні подібні вимірювання у 2023-2024 роках показують, що темпи й регулярність таких досліджень підвищилися, але залишиться недостатніми для побудови повної часової серії.

Основні напрями діяльності громадянського суспільства у сфері інформаційної безпеки зосереджуються на консультативно-аналітичній підтримці органів державної влади, протидії дезінформації та розвитку координації з владою. Громадські організації та експертні установи долучаються до формування стратегічних документів і державної політики, здійснюють експертизу та прогнозування ризиків, водночас реалізуючи контрпропагандистські та просвітницькі ініціативи, спрямовані на підвищення рівня медіаграмотності населення. Важливим аспектом їхньої роботи є співпраця з органами влади та міжнародними партнерами, що забезпечує ресурсну та інституційну підтримку для стійкості медіасфери та захисту інформаційного простору України.

Діяльність громадянського суспільства у сфері інформаційної безпеки є багатовекторною та водночас вразливою до низки обмежень. Для більшої наочності доцільно розглянути конкретні приклади проектів, реалізованих за останні п'ять років, які демонструють практичний вимір цієї діяльності (табл. 1).

Таблиця 1.

Проєкти громадянського суспільства в протидії інформаційній агресії: приклади (2020-2025)

Напрям діяльності	**Основні проєкти/ініціативи**	**Ключові результати/ефекти**
Консультативна допомога	Гарячі лінії для громадян, онлайн-консультації з медіаграмотності, юридична підтримка з питань інформаційної безпеки	Підвищення обізнаності щодо інформаційних загроз; надання швидкої допомоги у кризових ситуаціях
Контрпропагандистська діяльність	Випуск інформаційних бюлетенів, кампанії у соцмережах, розвінчування фейків	Зменшення впливу дезінформації; формування критичного мислення у громадян
Збір та аналіз даних	Моніторинг інформаційного простору, аналітичні звіти щодо фейків і пропаганди, дослідження інформаційних потоків	Надання точних даних для державних і громадських організацій; тимчасове реагування на інформаційні загрози
Просвітницька робота	Семінари, тренінги, лекції з медіаграмотності, освітні кампанії для різних вікових груп	Підвищення загального рівня медіаграмотності; формування стійкості до маніпуляцій та пропаганди

Таблиця розроблена автором.

Діяльність громадських організацій, експертних груп і активістів у сфері протидії російській інформаційній агресії набула системного характеру й охопила різні напрями: від оперативного спростування фейків до довготривалих аналітичних досліджень і освітніх ініціатив. Їхня робота не лише сприяла підвищенню рівня інформаційної безпеки в Україні, а й забезпечила міжнародне визнання окремих практик як ефективних інструментів у боротьбі з дезінформацією. Важливо підкреслити, що в умовах війни громадянське суспільство часто діяло там, де державні структури не могли швидко чи гнучко реагувати, чим компенсувало інституційні прогалини. Серед найпомітніших і впливових ініціатив можна виокремити низку платформ, які поєднали волонтерський ентузіазм, цифрові технології та експертний потенціал.

Одним із відомих прикладів громадянської ініціативи у сфері протидії дезінформації є проєкт «Інформаційні війська України» (ІВУ). Він був започаткований при Міністерстві інформаційної політики України з метою організації колективної відповіді на російську пропаганду, насамперед у соціальних мережах. У квітні 2025 року ІВУ набули статусу самостійного проєкту, відокремленого від державних структур, що може свідчити про зростання їхньої організаційної спроможності та незалежності [Укрінформ, 2025]. Основними напрямами їх діяльності залишаються спростування фейків, інформаційний наступ у соціальних мережах та поширення перевіреної інформації. Водночас детальні статистичні дані про кількість учасників чи охоплення авдиторії після 2016 року у відкритому доступі не оновлювалися, що ускладнює комплексну оцінку їхньої ефективності.

Важливу роль у сфері інформаційної безпеки продовжує відігравати Центр «Миротворець». У лютому 2025 року його база даних була поповнена відомостями про 25 тисяч громадян РФ, з яких близько 80% становили найманці, що здійснювали перетин кордону через тимчасово окуповані території Донбасу. У травні 2025 року Центр повідомив про видалення з бази списку російських журналістів, зазначивши, що це пов’язано з завершенням «інформаційної спецоперації»; після цього було анонсовано підготовку узагальнюючого звіту про результати [Центр стратегічних комунікацій, 2024]. Незважаючи на критику, пов’язану з використанням персональних даних, Центр і надалі зберігає функцію інформаційного ресурсу для державних органів, правоохоронних структур і громадськості, забезпечуючи ідентифікацію осіб, потенційно причетних до інформаційних та збройних загрозам.

Суттєвий внесок у протидію дезінформації здійснює також міжнародна волонтерська спільнота InformNapalm, відома своїми OSINT-дослідженнями. У 2025 році активісти організації продовжували моніторинг військових пересувань РФ, зокрема зафіксувавши факти перекидання російської техніки на територію Білорусі, що викликало реакцію міжнародних медіа та спостерігачів. Однак діяльність InformNapalm супроводжується і певними викликами: у 2025 році представники організації заявляли про спроби дискредитації, політичний тиск і загрози з боку різних інституцій [InformNapalm, 2025]

Громадські проєкти, на кшталт «ІВУ», «Миротворця» та InformNapalm виконують важливу функцію у сфері інформаційної безпеки. Вони не лише забезпечують оперативне інформування суспільства, а й формують доказову базу для розуміння масштабів російської інформаційної агресії, сприяючи підвищенню стійкості громадян до дезінформаційних впливів. Разом із тим їхня діяльність стикається з низкою обмежень:

−неповна регулярність оновлення даних;

−відсутність відкритих і верифікованих статистичних показників щодо масштабів авдиторії чи чисельності учасників;

−правові та етичні дилеми, пов'язані з оприлюдненням персональних даних;

−ризик використання інформаційних баз у політичних цілях.

Таким чином, діяльність громадських організацій і волонтерських ініціатив у сфері протидії інформаційним атакам має вагомий вплив на формування інформаційної безпеки держави. Проте для повнішої оцінки ефективності необхідне регулярне оновлення відкритої статистики, посилення прозорості діяльності та інституційне закріплення їхніх результатів у системі національної інформаційної політики.

Недержавні дослідницькі структури в Україні суттєво посилили увагу до вивчення інформаційного простору, наслідків інформаційної агресії та формування науково-методологічних рекомендацій для її протидії. Авторитетні організації – Український центр економічних і політичних досліджень імені Олександра Разумкова, Київський міжнародний інститут соціології (КМІС), Фонд «Демократичні ініціативи імені Ілька Кучеріва», Український інститут соціальних досліджень імені Олександра Яременка, Центр «Соціальний моніторинг» – регулярно проводять регіональні й всеукраїнські соціологічні дослідження. Предметом їхніх досліджень є ставлення громадян до державних інститутів, медіа, до джерел інформації, а також оцінка сприйняття загроз зі зовнішньої та внутрішньої інформаційної агресії.

Фахові об'єднання і медіаорганізації, зокрема ГО «Телекритика», ГО «Детектор медіа», Media Sapiens, «Інтерньюз-Україна», Інститут масової інформації, Національна спілка журналістів України, беруть участь у моніторингу медіаконтенту, підвищенні стандартів журналістської культури, розвитку журналістської етики. Вони також сприяють вдосконаленню законодавчої бази в медійній сфері, беруть участь у підготовці змін, які регулюють діяльність медіа, захист прав журналістів, а також застосування нормативів щодо прозорості та доброчесності.

Інтенсивна діяльність громадських об'єднань у сфері протидії інформаційній агресії демонструє значний потенціал цих структур, однак ефективність їхньої роботи обмежена низкою проблем. Перш за все, відсутня цілісна нормативно-правова база, яка б комплексно регулювала діяльність державних і недержавних суб'єктів у сфері національної безпеки, зокрема інформаційної, та забезпечувала координацію між ними. Нині питання залучення громадянського суспільства до забезпечення інформаційної безпеки відображені лише в загальних положеннях стратегічних документів, без детального визначення форм і механізмів участі громадських об'єднань.

Ще одним викликом є недосконаліть законодавства в інформаційній сфері та потреба в його кодифікації. Зокрема, чинні норми Закону України «Про захист персональних даних» потребують уточнення щодо застосування в контексті протидії інформаційній агресії, аби не

ставати перешкодою для оприлюднення даних про суб'єктів інформаційних загрози [Про захист персональних даних, 2010].

Проблемою залишається недостатній рівень координації дій між різними громадськими об'єднаннями та між ними й державними органами. Відсутність узгоджених процедур може призводити до суперечливих реакцій на окремі події, створюючи ризики для іміджу України та ефективності протидії інформаційним загрозам на міжнародній арені.

Фінансові обмеження громадських організацій також суттєво впливають на спроможність реагувати на інформаційні загрози. Вирішення цієї проблеми можливе через державне фінансування на конкурсній основі, а також залучення коштів міжнародних фондів та програм співробітництва. У цьому контексті доцільним є активне залучення громадських об'єднань до діяльності платформ і центрів міжнародного співробітництва у сфері кібербезпеки та протидії гібридним загрозам, створюваних у партнерстві з НАТО та іншими міжнародними організаціями, що діють в Україні. Детальніше проблеми та виклики та можливі шляхи вирішення цих питань представлено в таблиці 2.

Таблиця 2.

Виклики громадських організацій у сфері інформаційної безпеки

Проблема	Наслідки	Можливі шляхи рішення
Відсутність чіткого законодавчого регулювання	Обмежені можливості для правового захисту, ризики блокування або переслідування	Розробка та ухвалення законів, які регулюють діяльність ГО у сфері інформаційної безпеки
Недостатня координація між організаціями	Дублювання зусиль, низька ефективність спільних проєктів	Створення мережі об'єднань, спільні платформи для обміну даними та досвідом
Обмежене фінансування	Неможливість реалізувати великі проєкти, залежність від донорів	Залучення грантів, партнерство з державними структурами та бізнесом, розвиток донорських платформ
Низький рівень медіаграмотності населення	Складність у протидії дезінформації, високий ризик впливу пропаганди	Проведення освітніх тренінгів і семінарів для різних вікових груп
Загроза кібербезпеки та витоку даних	Ризик компрометації інформації, втрата довіри	Впровадження сучасних систем кіберзахисту, навчання персоналу цифрової безпеки

Таблиця розроблена автором

Отже, реалізація потенціалу громадянського суспільства у протидії інформаційній агресії вимагає комплексного підходу: вдосконалення нормативної бази, посилення координації між державними та недержавними суб'єктами, забезпечення фінансових ресурсів та інтеграції громадських об'єднань у національні й міжнародні системи реагування на інформаційні загрози. Важливим є розвиток людського капіталу через освітні та тренінгові програми, спрямовані на підвищення медіаграмотності та цифрової стійкості громадян. Систематичне документування та аналіз практик громадських ініціатив дозволить створити ефективні моделі взаємодії держави та суспільства, що забезпечать стійкість інформаційного простору та критичне мислення населення. Дослідження мають охоплювати оцінку ефективності різних стратегій протидії дезінформації, вплив громадянських мереж на демократичні процеси та механізми трансформації суспільної довіри під час гібридних викликів. Такий підхід дозволить не лише зміцнити обороноздатність інформаційного простору України, але й сформувати передумови для довгострокового розвитку демократичних інститутів та активної громадянської участі в суспільному житті.

Висновки. Узагальнюючи проведений аналіз, можна стверджувати, що участь громадянського суспільства в протидії інформаційним атакам стала одним із ключових факторів зміцнення інформаційної стійкості України. Громадські організації, експертні спільноти, медіа, ініціативні групи поступово еволюціонували від поодиноких

інформаційних акцій і волонтерських проєктів до створення розгалуженої мережі структур, здатних системно протидіяти дезінформації, здійснювати моніторинг і просвітницьку діяльність. Досвід останніх років показав, що саме громадянське суспільство стало гнучким і оперативним актором, здатним швидко реагувати на нові виклики та заповнювати прогалини в діяльності державних інституцій. Його ефективність значною мірою базується на горизонтальних мережах довіри, цифрових технологіях, інноваційних формах комунікації. Водночас нерегулярність і фрагментарність соціологічних вимірювань рівня довіри до громадських організацій свідчить про потребу в системному моніторингу цього показника, що має стати підґрунтям для стратегічного планування політики інформаційної безпеки.

У перспективі повоєнного відновлення громадянське суспільство постає як стратегічний партнер держави у сфері захисту інформаційного простору. Саме воно здатне забезпечити сталість протидії дезінформації, сприяти підвищенню медіаграмотності населення, а також формувати нові стандарти взаємодії між громадянами, владою та міжнародними організаціями. Таким чином, активність громадянського суспільства у сфері інформаційної безпеки не лише зміцнює демократичні інститути, але й створює підґрунтя для довгострокової стійкості та модернізації України.

Перспективи подальших досліджень слід спрямувати на розширений аналіз взаємодії між державними інституціями, громадянським суспільством та медіа в умовах війни, зосередившись на вивченні механізмів трансформації політичної комунікації, впливу інформаційних операцій на легітимність влади та демократичну участь громадян. Окремої уваги потребує порівняльний аналіз українського досвіду з міжнародними практиками протидії дезінформації, що дозволить виробити рекомендації для підвищення інституційної стійкості та формування ефективної інформаційної політики у повоєнний період.

Використані джерела:

1. Буняк, В. (2024). Українським медіа довіряють 47% респондентів. Детектор медіа. https://detector.media/infospace/article/222667/2024-02-07-opytuvannya-tsentru-razumkova-ukrainskym-media-doviryayut-47-respondentiv/
2. Буняк, В. (2025). 29% опитаних українських медіа перебувають у стані виживання після трьох місяців без фінансування від США. Детектор медіа. https://detector.media/infospace/article/241544/2025-06-05-29-opytanykh-ukrainskykh-media-perebuvayut-u-stani-vyzhyvannya-pislya-trokh-misyatsiv-bez-finansuvannya-vid-ssha-imi/
3. Грантоїдів на заводи. Як російська пропаганда воює з громадянським суспільством України (н.д.). Detector.media; Детектор медіа. https://detector.media/infospace/article/238055/2025-02-09-grantoidiv-na-zavody-yak-rosiyska-propaganda-voyuie-z-gromadyanskym-suspilstvom-ukrainy/
4. Грушецький, А. Динаміка довіри соціальним інституціям у 2021-2024 роках (2024) https://kiis.com.ua/?lang=ukr&cat=reports&id=1467&page=1
5. Динаміка довіри соціальним інституціям у 2021-2024 роках (2024). КМІС. Аналітичні матеріали. https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1467&page=1
6. Дузенко, Ю. (2025). Громадські організації планують сформувати стратегію OSINT-розслідування воєнних злочинів. Українські факти. https://uafakty.com/suspilstvo/gromadsk%D1%96-organ%D1%96zac%D1%96%D1%97-planyut-sformyvati-strateg%D1%96u-osint-rozsl%D1%96dyvannia-vo%D1%94nnih-zlochin%D1%96v.html
7. Закон України «Про захист персональних даних» № 2297-VI (2010). https://zakon.rada.gov.ua/laws/show/2297-17#Text
8. Індекс медіаграмотності українців за 2024 рік. (2025). StopFake. https://www.stopfake.org/uk/indeks-mediagramotnosti-ukrayintsiv-za-2024-rik/
9. Медіа відіграють стратегічну роль у відновленні України (2025). Як пройшла розмова про медіа на URC-2025 у Римі. Детектор медіа. https://detector.media/community/article/242550/2025-07-11-media-vidigrayut-strategichnu-rol-u-vidnovlenni-ukrainy-yak-proyshla-rozmova-pro-media-na-urc-2025-u-rymi/
10. Національний інститут стратегічних досліджень. (2025). Стан розвитку громадянського суспільства в Україні у 2024: аналітична доповідь. https://niss.gov.ua/publikatsiyi/analitychni-dopovidi/stan-rozvytku-hromadyanskoho-suspilstva-v-ukrayini-u-2024-na
11. Петренко, Г. (2025, July 12). Роль медіа в обороні. Версія 2025 року. Detector.media; Детектор медіа. https://detector.media/community/article/242556/2025-07-12-rol-media-v-oboroni-versiya-2025-roku/

12. Політика - новини України та світу. (2026). Інтерфакс-Україна. https://interfax.com.ua/news/political.html

13. Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи: тези доп. учасників міжн. наук.-практ. конф. (2023). Анн-Арбор - Харків https://library.pp-ss.pro/index.php/ndippsn_20231212

14. Семенченко, А. (2025). OSINT у кібербезпеці: як розвідка з відкритих джерел допомагає захистити компанії. Ukraine Today. https://zvezda4.com.ua/osint-u-kiberbezpeczi-yak-rozvidka-z-vidkrytyh-dzherel-dopomagaye-zahystyty-kompaniyi/

15. Українці мають високий рівень довіри до громадських та волонтерських організацій – 63% та 86% відповідно: опитування ZMINA. (2023). ZMINA. https://zmina.info/news/ukrayinczi-mayut-vysokyj-riven-doviry-do-gromadskyh-ta-volonterskyh-organizaczij-63-ta-86-vidpovidno-opytuvannya/

16. Укрінформ - актуальні новини України та світу. (n.d.). Www.ukrinform.ua. https://www.ukrinform.ua/

17. Центр стратегічних комунікацій. Протидія дезінформації та гібридним операціям Росії. (2025, December 15). Центр стратегічних комунікацій. https://spravdi.org/

18. Чистоклетов, Л., & Обрембальський, С. (2024). Особливості забезпечення інформаційної безпеки в умовах російсько-української війни. В Академічні візії (Випуск 31). Zenodo. https://doi.org/10.5281/zenodo.11381101

19. Bellingcat Higgins, E. (2023). How Open Source Evidence was Upheld in a Human Rights Court. Bellingcat. https://www.bellingcat.com/resources/2023/03/28/how-open-source-evidence-was-upheld-in-a-human-rights-court/

20. Citizens' assessment of the situation in the country, trust in social institutions, politicians, officials and public figures (2023). Razumkov.org.ua. https://razumkov.org.ua/en/research-areas/surveys/citizens-assessment-of-the-situation-in-the-country-trust-in-social-institutions-politicians-officials-and-public-figures-may-2023

21. Ekman, I., & Nilsson, E. (2023). Ukraine's Information Front Strategic Communication during Russia's Full-Scale Invasion of Ukraine. https://doi.org/10.13140/RG.2.2.14115.22569

22. Freedom House, 2023; Report on EEAS Activities to Counter Foreign Information Manipulation and Interference (FIMI). (2024). EEAS. https://www.eeas.europa.eu/eeas/2024-report-eeas-activities-counter-foreign-information-manipulation-and-interference-fimi_en

23. InformNapalm. (n.d.). *InformNapalm https://informnapalm.org/?s=OSINT*

24. The Twilight of Democracy with Anne Applebaum: Buffett Institute for Global Affairs - Northwestern University. (2025). Northwestern.edu. https://buffett.northwestern.edu/news/2024/the-twilight-of-democracy-with-anne-applebaum.html

25. Top challenges for Ukraine's media in 2025 — IMI survey. IMI. https://imi.org.ua/en/monitorings/stress-money-staff-top-challenges-for-ukraines-media-in-2025-imis-yearly-survey

26. Ukraine: Nations in Transit 2024 Country Report. (n.d.). Freedom House. https://freedomhouse.org/country/ukraine/nations-transit/2024

27. Wilson, T., & Starbird, K. (2021). Cross-platform Information Operations: Mobilizing Narratives & Building Resilience through both "Big" & "Alt" Tech. Proceedings of the ACM on Human-Computer Interaction, 5(CSCW2), 1–32. https://doi.org/10.1145/3476086

References:

1. Buniak, V. (2024). Ukrainskym media doviriaiut 47% respondentiv. Detektor media. https://detector.media/infospace/article/222667/2024-02-07-opytuvannya-tsentru-razumkova-ukrainskym-media-doviryayut-47-respondentiv/ (in Ukrainian)

2. Buniak, V. (2025). 29% opytanykh ukrainskykh media perebuvaiut u stani vyzhyvannia pislia trokh misiatsiv bez finansuvannia vid SShA. Detektor media. https://detector.media/infospace/article/241544/2025-06-05-29-opytanykh-ukrainskykh-media-perebuvayut-u-stani-vyzhyvannya-pislya-trokh-misyatsiv-bez-finansuvannya-vid-ssha-imi/ (in Ukrainian)

3. Hrantoidiv na zavody. Yak rosiiska propahanda voiuie z hromadianskym suspilstvom Ukrainy (n.d.). Detector.media; Detektor media. https://detector.media/infospace/article/238055/2025-02-09-grantoidiv-na-zavody-yak-rosiyska-propaganda-voyuie-z-gromadyanskym-suspilstvom-ukrainy/ (in Ukrainian)

4. Hrushetskyi, A. Dynamika doviry sotsialnym instytutsiiam u 2021-2024 rokakh (2024) https://kiis.com.ua/?lang=ukr&cat=reports&id=1467&page=1

5. Dynamika doviry sotsialnym instytutsiiam u 2021-2024 rokakh (2024). KMIS. Analitychni materialy. https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1467&page=1 (in Ukrainian)

6. Duzenko, Yu. (2025). Hromadski orhanizatsii planuiut sformuvaty stratehiiu OSINT-rozsliduvannia voiennykh zlochyniv. Ukrainski fakty. https://uafakty.com/suspilstvo/gromadsk%D1%96-organ%D1%96zac%D1%96%D1%97-planyut-sformyvati-strateg%D1%96u-osint-rozsl%D1%96dyvannia-vo%D1%94nnih-zlochin%D1%96v.html (in Ukrainian)

7. Zakon Ukrainy «Pro zakhyst personalnykh danykh» № 2297-VI (2010). https://zakon.rada.gov.ua/laws/show/2297-17#Text (in Ukrainian)
8. Indeks mediahramotnosti ukraintsiv za 2024 rik. (2025). StopFake. https://www.stopfake.org/uk/indeks-mediagramotnosti-ukrayintsiv-za-2024-rik/ (in Ukrainian)
9. Media vidihraiut stratehichnu rol u vidnovlenni Ukrainy (2025). Yak proishla rozmova pro media na URC-2025 u Rymi. Detektor media. https://detector.media/community/article/242550/2025-07-11-media-vidigrayut-strategichnu-rol-u-vidnovlenni-ukrainy-yak-proyshla-rozmova-pro-media-na-urc-2025-u-rymi/ (in Ukrainian)
10. Natsionalnyi instytut stratehichnykh doslidzhen. (2025). Stan rozvytku hromadianskoho suspilstva v Ukraini u 2024: analitychna dopovid. https://niss.gov.ua/publikatsiyi/analitychni-dopovidi/stan-rozvytku-hromadyanskoho-suspilstva-v-ukrayini-u-2024-na (in Ukrainian)
11. Petrenko, H. (2025, July 12). Rol media v oboroni. Versiia 2025 roku. Detector.media; Detektor media. https://detector.media/community/article/242556/2025-07-12-rol-media-v-oboroni-versiya-2025-roku/
12. Polityka - novyny Ukrainy ta svitu. (2026). Interfaks-Ukraina. https://interfax.com.ua/news/political.html (in Ukrainian)
13. Protydiia dezinformatsii v umovakh rosiiskoi ahresii proty Ukrainy: vyklyky i perspektyvy: tezy dop. uchasnykiv mizhn. nauk.-prakt. konf. (2023). Ann-Arbor - Kharkiv https://library.pp-ss.pro/index.php/ndippsn_20231212 (in Ukrainian)
14. Semenchenko, A. (2025). OSINT u kiberbezpetsi: yak rozvidka z vidkrytykh dzherel dopomahaie zakhystyty kompanii. Ukraine Today. https://zvezda4.com.ua/osint-u-kiberbezpeczi-yak-rozvidka-z-vidkrytyh-dzherel-dopomagaye-zahystyty-kompaniyi/ (in Ukrainian)
15. Ukraintsi maiut vysokyi riven doviry do hromadskykh ta volonterskykh orhanizatsii – 63% ta 86% vidpovidno: opytuvannia ZMINA. (2023). ZMINA. https://zmina.info/news/ukrayinczi-mayut-vysokyj-riven-doviry-do-gromadskyh-ta-volonterskyh-organizaczij-63-ta-86-vidpovidno-opytuvannya/ (in Ukrainian)
16. Ukrinform - aktualni novyny Ukrainy ta svitu. (n.d.). Www.ukrinform.ua. https://www.ukrinform.ua/ (in Ukrainian)
17. Tsentr stratehichnykh komunikatsii. Protydiia dezinformatsii ta hibrydnym operatsiiam Rosii. (2025, December 15). Tsentr stratehichnykh komunikatsii. https://spravdi.org/ (in Ukrainian)
18. Chystokletov, L., & Obrembalskyi, S. (2024). Osoblyvosti zabezpechennia informatsiinoi bezpeky v umovakh rosiisko-ukrainskoi viiny. V Akademichni vizii (Vypusk 31). Zenodo. https://doi.org/10.5281/zenodo.11381101 (in Ukrainian)
19. Bellingcat Higgins, E. (2023). How Open Source Evidence was Upheld in a Human Rights Court. Bellingcat. https://www.bellingcat.com/resources/2023/03/28/how-open-source-evidence-was-upheld-in-a-human-rights-court/
20. Citizens' assessment of the situation in the country, trust in social institutions, politicians, officials and public figures (2023). Razumkov.org.ua. https://razumkov.org.ua/en/research-areas/surveys/citizens-assessment-of-the-situation-in-the-country-trust-in-social-institutions-politicians-officials-and-public-figures-may-2023
21. Ekman, I., & Nilsson, E. (2023). Ukraine's Information Front Strategic Communication during Russia's Full-Scale Invasion of Ukraine. https://doi.org/10.13140/RG.2.2.14115.22569
22. Freedom House, 2023; Report on EEAS Activities to Counter Foreign Information Manipulation and Interference (FIMI). (2024). EEAS. https://www.eeas.europa.eu/eeas/2024-report-eeas-activities-counter-foreign-information-manipulation-and-interference-fimi_en
23. InformNapalm. (n.d.). *InformNapalm https://informnapalm.org/?s=OSINT*
24. The Twilight of Democracy with Anne Applebaum: Buffett Institute for Global Affairs - Northwestern University. (2025). Northwestern.edu. https://buffett.northwestern.edu/news/2024/the-twilight-of-democracy-with-anne-applebaum.html
25. Top challenges for Ukraine's media in 2025 — IMI survey. IMI. https://imi.org.ua/en/monitorings/stress-money-staff-top-challenges-for-ukraines-media-in-2025-imis-yearly-survey
26. Ukraine: Nations in Transit 2024 Country Report. (n.d.). Freedom House. https://freedomhouse.org/country/ukraine/nations-transit/2024
27. Wilson, T., & Starbird, K. (2021). Cross-platform Information Operations: Mobilizing Narratives & Building Resilience through both "Big" & "Alt" Tech. Proceedings of the ACM on Human-Computer Interaction, 5(CSCW2), 1–32. https://doi.org/10.1145/3476086

Barabolya Vyacheslav,
postgraduate student of the Department of Political Science,
Educational and Research Institute of Law and Political Science,
Ukrainian Mykhailo Drahomanov State University

Civil Society Participation In Countering Information Attacks

The article examines the role of civil society in countering information attacks in Ukraine under the conditions of hybrid warfare. It is shown that the growing scale of disinformation campaigns and information pressure has

increased the importance of horizontal networks of citizen interaction, expert communities, and volunteer initiatives, which were able to respond promptly to challenges where state institutions proved insufficiently flexible. Particular attention is paid to the analysis of tools used by civil society structures to protect the information space: fact-checking, media monitoring, dissemination of verified data, information and educational campaigns, as well as the development of digital security practices. Examples of successful initiatives that have become emblematic of the Ukrainian experience are highlighted – the activities of StopFake, the Institute of Mass Information, OSINT communities, and civil platforms for media literacy. Emphasis is placed on the fact that civil society not only complements state strategies to counter disinformation but also creates alternative communication channels that enhance public trust and strengthen the resilience of democratic practices. The article also underlines that despite the significant practical contribution of civic initiatives, their role has been insufficiently studied and remains fragmented, which limits opportunities for systematizing experience and developing long-term strategies. It is concluded that the further development and institutional consolidation of civic participation in the field of information security is a strategic task on which the effectiveness of countering external threats, the formation of a culture of critical thinking, and the strengthening of democratic resilience of Ukrainian society depend.

Keywords: *civil society, information security, disinformation, fact-checking, digital resilience, media literacy, information attacks.*

DOI https://doi.org/10.31392/UDU-nc.series22.2025.38.10
УДК 324

Руслан Дем'янюк,
аспірант кафедри політичних наук,
Навчально-науковий інститут права та політології,
Український державний університет імені Михайла Драгоманова,
ORCID: *https://orcid.org/0009-0000-6431-3397; e-mail: r.a.demianiuk@udu.edu.ua*

НОВІТНІ ЄВРОПЕЙСЬКІ ПРАКТИКИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ПОЛІТИЧНИМ МАНІПУЛЯЦІЯМ: МОЖЛИВОСТІ ТА ПРОБЛЕМИ ЗАПРОВАДЖЕННЯ В УКРАЇНІ

Протидія інформаційним політичним маніпуляціям стає одним із найпріоритетніших завдань сучасного цифрового суспільства. Прогрес надає нові широкі можливості для політичних маніпуляцій, від великої швидкості якого розроблені заходи запобігання стають малоефективними. Використання фейкових новин, маніпулятивних наративів і пропаганди негативно впливає на громадську думку. Попередження політичного маніпулювання у високотехнологічному суспільстві потребує невідкладного пошуку нових методик та удосконалення існуючих для впровадження високоефективної цифрової освіти. Європейські країни активно розробляють і впроваджують новітні методи боротьби з дезінформацією та пропагандою, що охоплює як правові та політичні механізми, так і суспільно-освітні заходи. В Україні, яка перебуває в умовах війни, необхідність адаптації та імплементації таких практик є особливо актуальною, оскільки інформаційні атаки є частиною російської стратегії агресії проти нашої держави. Актуальність теми полягає у необхідності дослідження новітніх європейських практик протидії інформаційним політичним маніпуляціям із метою своєчасного використання такого досвіду в Україні. Метою дослідження є вивчення та аналіз можливостей і проблем у запровадженні в Україні європейських практик протидії інформаційним політичним маніпуляціям, для адаптації найкращих із них і подальшої їх імплементації.

Результатами дослідження є визначення основних понять та термінів; характеристика протидії інформаційним політичним маніпуляціям; встановлення та аналіз європейських практик протидії інформаційним політичним маніпуляціям; визначення можливостей та основних проблем у їх запровадженні в Україні; розроблення рекомендацій щодо адаптації кращих із них та подальшої їх імплементації. Запропоновано розробити, змінити та удосконалити механізми протидії інформаційним політичним маніпуляціям в Україні з урахуванням європейських практик. У статті проаналізовано європейські практики протидії інформаційним маніпуляціям як комплексу узгоджених заходів, спрямованих на доповнення один одного. За результатами системного аналізу визначено, що комплексний підхід з розвитку медіаграмотності та встановлення апробованих європейських практик щодо обмежень та заборон створення та поширення за допомогою інформаційних технологій політичної реклами, щодо регулювання платформ соціальних мереж і штучного інтелекту мають стати основою для запобігання інформаційним маніпуляціям в Україні.

Ключові слова: *політичні маніпуляції, інформаційні політичні маніпуляції, європейські практики*