Міністерство освіти і науки України
Національний університет «Острозька академія»
Навчально-науковий центр заочно-дистанційного навчання
Кафедра національної безпеки та політології

Кваліфікаційна робота

на здобуття освітнього ступеня магістра на тему:

«Пропаганда та контрпропаганда як складова російсько-української війни»

Виконав студент ІІ курсу, групи ЗМНб-2
спеціальності 256 Національна безпека (за окремими сферами забезпечення і видами діяльності)
Ренькас Віталій Валерійович

Керівник – кандидат історичних наук, доцент
Конопка Наталя Олегівна
Рецензент – доктор філософських наук, професор
Слюсар Вадим Миколайович

Острог, 2026

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ ТА ТЕРМІНІВ

рф – російська федерація

ЦПД – Центр протидії дезінформації

ЦСКІБ – Центр стратегічних комунікацій та інформаційної безпеки

РНБО – Рада національної безпеки та оборони України

NATO (НАТО) – North Atlantic Treaty Organization (Організація Північноатлантичного договору, також Північноатлантичний Альянс).

ІПсВ – Інформаційно-психологічний вплив

ІПСО – Інформаційно-психологічна спеціальна операція

EEAS – European External Action Service (Європейська служба зовнішніх дій)

FIMI – Foreign Information Manipulation and Interference (Іноземна інформаційна маніпуляція та вплив)

Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats (Європейський центр експертизи протидії гібридним загрозам)

OSINT – Open Source Intelligence (Розвідка на основі відкритих джерел)

Наратив – стійка смислова конструкція, що задає рамку інтерпретації подій і об’єднує окремі повідомлення у “картину світу”.[1]

Фрейм – рамка подання події (кут зору), що визначає, які елементи вважаються важливими і як вони оцінюються.

Інфодемія – стан інформаційного перенасичення, що ускладнює відрізнення правдивого від маніпулятивного і створює ризики для політичної стабільності.[2]

Цифрові ризики – ризики , що виникають через цифрові технології, платформи, дані та інфраструктури й впливають на інформаційну безпеку.[3]

---

[1] Скрипникова Л.В., Політологія: навчальний посібник. К.: Центр учбової літератури, 2014, 272 с. URL: https://dduvs.edu.ua/biblioteka/biblioteka-studenta-dduvs/pidruchniki-posibniki/politologiya/ (дата звернення: 06.03.2026).

[2] Гаращук, Д., Сергєєв, В. Інфодемія та популізм у цифрову епоху: загрози політичній стабільності та безпекові виклики. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2025-2(8)-61-71 (дата звернення: 06.03.2026).

[3] Наторіна А.О. Синкретичність менеджменту цифрових ризиків та інформаційної безпеки. 27 листопада 2019. URL: https://ema.ztu.edu.ua/article/view/185089 (дата звернення 06.03.2026).

Національна стійкість – здатність держави й суспільства витримувати, адаптуватися та відновлюватися під час кризи/війни, зберігаючи керованість і функціональність.[4]

[4] Ліпкан В.А. Національна безпека України : навч. посібник . К. : Кондор, 2008, 552 с.

ВСТУП

Актуальність теми. Російсько-українська війна, «гаряча» фаза якої у її гібридній та конвенційній формах, триває без малого майже 14 років, де пропаганда та дезінформація рф використовуються як інструменти досягнення воєнно-політичних цілей. У сучасних умовах інформаційні атаки функціонують як операції впливу з розгалуженою екосистемою дійових суб'єктів (акторів), проксі-ресурсів, платформних каналів і повторюваних наративних шаблонів, що підтверджується профільними міжнародними дослідженнями.

Україна, в свою чергу, реагуючи на масштаб і інтенсивність інформаційної агресії з боку російської федерації, намагається інституціалізувати протидію через державні політики та інструменти – зокрема через Стратегію інформаційної безпеки та планування її реалізації, а також через спеціалізовані структури й практики стратегічних комунікацій.

Актуальність даної теми підсилюється технологічною еволюцією інформаційного середовища, а саме його платформізацією, домінуванням мережевих каналів (зокрема Telegram-спільнот), зростанням ролі проксі-мереж, а також появою нових методів впливу, пов'язаних із алгоритмічним розповсюдженням контенту та ризиками «зараження» інформаційного простору внаслідок масштабованого продукування маніпулятивних матеріалів, в тому числі з використанням ВММ (Велика Мовна Модель, від англійської абревіатури LLM – Large Language Model), так званих «ШІ чат-ботів». Практичну цінність у вирішенні даної проблеми для наукової спільноти та держави загалом можна визначити як необхідність розробки підходів та критеріїв оцінки ефективності пропаганди та контрпропаганди через розробку якісних систем оцінювання та ефективних механізмів технологічних інструментів протидії.

Ступінь розробки проблеми. В українському сегменті ступінь розробки проблеми використання пропаганди та контрпропаганди у війні розвиваються переважно в трьох напрямках, такі як: державна інформаційну політика та

контрпропаганда як інструмент забезпечення інформаційної безпеки; стратегічні комунікації сектору безпеки і оборони як інструмент протидії інформаційним загрозам та прикладні дослідження наративів та інструментів російської пропаганди[5], що описують повторювані смислові конструкції, техніки маніпуляції, аудиторії та канали їх розповсюдження.[6]

Передусім варто відзначити вагомий внесок фундаментальних праць у сфері національної безпеки, зокрема робіт Володимира Анатолійовича Ліпкана, Петра та Юлії Лісовських, які формують базове уявлення про місце інформаційної безпеки в системі державної політики. Суттєвою перевагою зазначених робіт є їх системність та концептуальна завершеність, що дозволяє використовувати їх як методологічний фундамент для подальших досліджень. Сучасні дослідження, представлені працями Сергія Андрієнка, Дмитра Гаращука з В'ячеславом Сєргєєвим, Любові Корнійчук разом з Наталією Матвійчук, Носенка, Загурської-Антонюк та інших авторів, демонструють спробу адаптації наукового дискурсу до нових реалій війни. У цих роботах пропаганда розглядається як невід'ємний елемент гібридної війни, що функціонує у тісному зв'язку з кіберопераціями, інформаційно-психологічними спеціальними операціями, психологічним впливом та політичними процесами.

Окремої уваги заслуговує когнітивно-психологічний вимір пропаганди, який у сучасній літературі представлений нерівномірно. Праця Володимира Станчишина, психолога, аналізує емоційні механізми впливу інформації на індивіда та суспільство. У цьому контексті пропаганда виступає не стільки як інструмент передачі інформації, а як механізм формування емоційних станів, що визначають поведінку аудиторії. Фрагментованість різних підходів у розробці проблеми свідчить про відсутність міждисциплінарної інтеграції, яка є

[5] Веб-портал ЦЕНТР ПРОТИДІЇ ДЕЗИНФОРМАЦІЇ. Analytical research based on the results of the revealed disinformation campaign the "Black hole" of the russian federation aimed at discrediting Ukraine and President Zelensky. 07 червня 2023. URL: https://cpd.gov.ua/en/report/analytical/ (дата звернення: 22.02.2026).
[6] Веб-портал ЦЕНТР ПРОТИДІЇ ДЕЗИНФОРМАЦІЇ. Аналітичний звіт «російська пропаганда на ТОТ в обличчях» . 13 січня 2025. URL: https://cpd.gov.ua/reports/analitychnyj-zvit-rosijska-propaganda-na-tot-v-oblychchyah/ (дата звернення: 22.02.2026).

необхідною для повноцінного розуміння феномену пропаганди в умовах сучасної війни.

Таким чином можна констатувати, що сучасні дослідження створюють необхідний базис для дослідження пропаганди та контрпропаганди, однак водночас виявляють низку теоретичних і методологічних прогалин. Це відкриває можливості для подальшого наукового пошуку, зокрема у напрямі розробки міждисциплінарних підходів, інтеграції когнітивних і технологічних аспектів, а також створення ефективних механізмів оцінки та протидії інформаційним впливам.

Проблема, об'єкт та предмет дослідження. Проблема дослідження полягає у необхідності науково обґрунтувати та емпірично підкріпити розуміння пропаганди і контрпропаганди як взаємопов'язаних процесів у війні та як інструментів, які прямо впливають на національну стійкість і безпекову керованість, при цьому залишаючись у межах правових і етичних обмежень демократичної держави.

Об'єктом даного дослідження виступає інформаційне протиборство у російсько-українській війні як складова національної безпеки.

Предметом ж дослідження виступають механізми, інструменти, канали та ефекти російської пропаганди і української контрпропаганди (контрзаходи), інституційні умови їх реалізації та критерії ефективності.

Мета і завдання. Метою даної роботи є комплексно проаналізувати пропаганду та контрпропаганду в російсько-українській війні як складові інформаційного протиборства, а також обґрунтувати підходи до побудови ефективної, вимірюваної та легітимної системи контрпропаганди в інтересах національної безпеки України.

Завданнями даної роботи можна визначити наступне:

1. Уточнення понятійного апарату (значення понять пропаганди, дезінформації, ІПСВ/ІПСО, стратегічних комунікацій, контрпропаганди) у рамках національної безпеки.

2. Систематизацію ключових наративів та прийомів російської пропаганди щодо України, охоплюючи період 2014-2026 років, з дотриманням фокусу на період з 2022 по 2026 роки.
3. Аналіз українських контрзаходів. Стратегічні комунікації сектору безпеки і оборони, державні комунікації, співпраця з партнерами та обґрунтування критеріїв ефективності контрпропаганди. Формулювання практичних рекомендацій щодо підвищення спроможності держави у сфері контрпропаганди з урахуванням правових і етичних меж.

Характеристика джерельної бази дослідження. Джерельною базою даного дослідження, першою чергою, виступають державні нормативно-правові акти у сфері Національної безпеки та оборони, зокрема Указ Президента України «Про рішення Ради національної безпеки і оборони України» від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки», дослідження та аналітичні записки Центру протидії дезінформації при РНБО України (Додаток А), публікації та матеріали Центру стратегічних комунікацій та інформаційної безпеки (Додаток Б), звітні документи Кабінету Міністрів, Міністерств та департаментів, зокрема Міністерства культури та інформаційної політики України стосовно плану заходів, здійснених щодо реалізації Стратегії інформаційної безпеки за 2025 рік та інші вітчизняні джерела. Вони дають змогу проаналізувати вектор розвитку національної стратегії протидії пропаганді, координації стратегічної комунікації, аналіз наративів та методів їх протидії, що дає повну картину наявного стану справ у вітчизняній царині пропаганди та контрзаходів щодо неї. Аналіз даних Центру протидії дезінформації при РНБО та матеріали Центру стратегічних комунікацій та інформаційної безпеки дають змогу визначити основні пропагандиські наративи росії, оцінити масштаб їх впливу, а також прослідкувати за розвитком методів протидії та контрзаходів України.

Водночас, зарубіжний сегмент джерел, використаних для підготовки даного дослідження визначений, але не лімітований, звітами про діяльність

EEAS з протидії іноземним інформаційним маніпуляціям та втручанню за 2022-2024 роки, аналітичними статтями та аналізом кейсів пропаганди веб-бази EUvsDisInfo, веб-порталу RAND Corporation (Research And Development Corporation), що спеціалізується, в тому числі, на аналізі пропаганди у західному медіа-просторі. Вони дають змогу зрозуміти вектор розвитку пропагандиських наративів, що націлені на зарубіжну цільову аудиторію. Звіти та постанови Європейської Комісії по стратегіям цифрової протидії за 2026 рік, публікації та звіти NATO Strategic Communications Centre of Excellence допомагають оцінити ефективність підходів та навести аналіз стратегій контрпропаганди держав-партнерів Євроатлантичного Альянсу, що дає змогу визначити можливість їх аплікації до наших реалій війни. Також використані матеріали провідних інформаційних агентств, як Reuters, CNN, звіти та статистику медійних холдингів Meta та X, що стосуються висвітленню проблем російської пропаганди та протидії їй. Ці джерела дають змогу зрозуміти ступені ефективності заходів та контрзаходів, виокремити дієві критерії оцінки та проаналізувати динаміку змін поведінки цільових аудиторій та зрозуміти ефективність протидії дезінформації на рівні провідних приватних медіа.

Методологічна основа та методи. Методологічною основою даної роботи являється міждисциплінарний підхід у межах досліджень національної безпеки із залученням комунікаційних та політико-інституційних меж. Методами дослідження є аналіз документів і політик, контент-аналіз і наративний аналіз меседжів, аналіз наративів, дискурс-аналіз, порівняльний аналіз українських і західних підходів, кейс-стаді інформаційних кампаній, а також, за потреби – елементи OSINT-аналізу ланцюгів поширення меседжів.

Наукова новизна. Науковою новизною даної роботи є розгляд контрпропаганди як інституційної функції системи національної безпеки, а не тільки як комунікаційної реакції на окремі події чи системний вплив.

1. Запропоновано підхід до вимірювання ефективності контрпропаганди через індикатори стійкості й довіри та показники зменшення шкоди від операцій впливу.

2. В рамках дослідження інтегровано український практичний досвід із західними рамками аналізу/визначення характеристик операцій впливу (зокрема, на базі сучасних підходів NATO StratCom COE).

Практичне значення. Результати даної роботи можуть бути використані для удосконалення координації комунікацій і контрзаходів у державному секторі стратегічних комунікацій та інформаційної політики, розвитку індикаторів інформаційної стійкості, а також у навчальних курсах зі стратегічних комунікацій та інформаційної безпеки.

Апробація результатів дослідження. Апробацією роботи є публікація тез на VII міжнародній науково-практичній конференції «INNOVATIONS OF MODERN SCIENCE AND EDUCATION», яка відбулася 27-29.04.2026 року у Цюриху, Швейцарія. Тези опубліковані у збірнику тез «INNOVATIONS OF MODERN SCIENCE AND EDUCATION» [7] від 27.04.2026 року.

Структура роботи. Дана наукова робота складається зі вступу, трьох розділів, тринадцяти підрозділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 112 сторінок, обсяг основної частини становить 91 сторінка. Список використаних джерел та літератури містить 46 найменувань.

[7] Ренькас В.В. ПРОПАГАНДА ТА КОНТРПРОПАГАНДА В РОСІЙСЬКОУКРАЇНСЬКІЙ ВІЙНІ 2014-2026 РОКИ // Innovation and development in world science. Proceedings of the 7th International scientific and practical conference. MDPC Publishing. Zurich, Switzerland. 2026. Pp. 21-27. URL: https://sci-conf.com.ua/vii-mizhnarodna-naukovo-praktichna-konferentsiya-innovationand-development-in-world-science-27-29-04-2026-tsyurih-shvejtsariya-arhiv/ (дата звернення: 27.04.2026).

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ АНАЛІЗУ ПРОПАГАНДИ ТА КОНТРПРОПАГАНДИ В СИСТЕМІ НАЦБЕЗПЕКИ

1.1. Понятійно-категоріальний апарат

Для дослідження пропаганди та контрпропаганди як складових російсько-української війни критично важливо одразу визначити коректний термінологічний каркас. У підході сфери національної безпеки терміни не являються академічною формальністю. Від того, як ми розрізняємо явища, залежить вибір інструментів протидії, рамки легітимності та критерії оцінювання ефективності.[8]

Пропаганда у контексті війни може розглядатися як систематична, цілеспрямована комунікативна діяльність, спрямована на формування установок, емоцій і поведінки аудиторій в інтересах суб'єкта впливу[9]. Для національної безпеки ключовим в даному аспекті є її інструментальність, тобто пропаганда не просто "переконує", а працює на досягнення конкретних безпекових ефектів , таких як, наприклад, підрив довіри, деморалізація, делегітимація влади чи окремих інституцій, розкол, зниження підтримки серед населення чи партнерів.[10]

Дезінформація, як визначення, відрізняється від пропаганди тим, що центральним елементом є навмисне поширення неправдивої або оманливої інформації з метою завдання шкоди, спотворення ухвалення рішень або спричинення необхідних реакцій зі сторони об'єкта дезинформаційного впливу.[11] В реальних кампаніях рф пропаганда й дезінформація часто переплетені. Наприклад, пропаганда створює основну наративну рамку (так звану «велику

[8] Лісовський П.М. Безпекознавство: особистість, держава, суспільство : навч. посібник. К. : Кондор, 2017, 368 с.
[9] Ліпкан В.А. Національна безпека України : навч. посібник . К. : Кондор, 2008, 552 с.
[10] Лісовський П.М. Безпекознавство: особистість, держава, суспільство : навч. посібник. К. : Кондор, 2017, 368 с.
[11] ЦЕНТР ПРОТИДІЇ ДЕЗИНФОРМАЦІЇ. Веб-портал. 02 грудня 2025. URL: https://cpd.gov.ua/international-direction/ssha/ru-propaganda-poshyryuye-fejky-pro-zlochyny-ukrayinskyh-vijskovyh/ (дата звернення: 05.03.2026).

історію»), а дезінформація підживлює її «фактами» (фейками або псевдодоказами[12]).

Маніпуляція є більш широким визначенням механізму, де вплив здійснюється не лише неправдивою інформацією, а й підміною контексту, емоційним тиском, підміною причинно-наслідкових зв'язків, відволіканням уваги, перевантаженням інформацією та іншим[13]. В контексті національної безпеки це дуже важливо, адже частина впливів не порушує буквальної «фактології», але руйнує здатність суспільства адекватно оцінювати реальність.

Інформаційно-психологічний вплив (ІПсВ) – категорія, що описує впливи, націлені на психіку, моральний стан, волю, групову поведінку та соціальні установки[14]. У війні ІПсВ є мостом між інформаційними повідомленнями та їхнім кінцевим результатом, такими як паніка, апатія, агресія всередині суспільства, "втома від війни", недовіра, відмова від підтримки державних рішень тощо.

Операції впливу чи інформаційні-психологічні спеціальні операції[15] описують комплексні кампанії[16], де поєднуються наративи, канали, проксі-суб'єкти дій, тактики поширення і синхронізація з подіями у фізичному світі (військові дії, дипломатія, теракти, економічні рішення та інше). Для даної

---

[12] Дар'я Маркова. Національна спілка журналістів України. Пропаганда та дезінформація: що найбільше впливає на український інфопростір. 25 грудня 2024. URL: https://nsju.org/novini/propaganda-ta-dezinformacziya-shho-najbilshe-vplyvaye-na-ukrayinskyj-infoprostir/ (дата звернення: 05.03.2026).

[13] Гаращук, Д., Сергєєв, В. Інфодемія та популізм у цифрову епоху: загрози політичній стабільності та безпекові виклики. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2025-2(8)-61-71 (дата звернення: 06.03.2026).

[14] Андрієнко С. С. Психологічна підготовка та підтримка співробітників правоохоронних органів в умовах гібридної війни. Економіка, управління та адміністрування.2025. URL: https://doi.org/10.26642/ema-2024-4(110)-103-108 (дата звернення 06.03.2026).

[15] Лисенко С.О. Стратегічне управління інформаційною безпекою держави : автореферат дисерт. на здобуття наук. ступ. д.н. з держ. упр. ; спец. 25.00.05 - державне управління у сфері державної безпеки та охорони громадського порядку. Житомирська політехніка. 2025. URL: https://ztu.edu.ua/site/files/1/docs/Університет/Спеціалізовані%20вчені%20ради/14.052.03/2025/ref_Лисенко_С.pdf . (дата звернення: 05.03.2026).

[16] Герасимюк К.Х. Механізми державного управління кібер- та інформаційною безпекою: проблеми та шляхи вирішення. Економіка, управління та адміністрування. Жовтень 2021. URL: https://www.researchgate.net/publication/356396763_Mehanizmi_derzavnogo_upravlinna_kiber-_ta_informacijnou_bezpekou_problemi_ta_slahi_virisenna (дата звернення: 07.03.2026).

роботи це можна виділити як один із ключових об’єднуючих термінів. Він дозволяє аналізувати не окремі фейки, а архітектуру впливу.[17]

Стратегічні комунікації – це узгоджене використання комунікацій держави для досягнення стратегічних цілей[18], включно з підтримкою довіри, поясненням політики, мобілізацією підтримки та нейтралізацією ворожих наративів. У цій лозіці стратегічні комунікації – не є синонімом контрпропаганди, а більше її основою, де задаються рамки, як держава повинна висвітлювати правду, координувати меседжі і не втрачати моральної переваги.

Контрпропаганда у контексті національної безпеки доцільно визначати як систему контрзаходів, спрямованих на нейтралізацію ворожого інформаційного впливу та збереження чи посилення національної стійкості[19]. Важливий моментом є те, що контрпропаганда не мусить зводитися до простих спростовувань повідомлень. Вона включає в себе превенцію, тобто зменшення чи знешкодження вразливостей, проактивні інформаційні наративи, кризові комунікації, інституційну координацію та вимірювання ефекту.[20]

З огляду на це, у даній кваліфікаційній роботі, в контексті пропаганди доцільним буде використовувати наступний ієрархічний ланцюжок понять/визначень:

Операції впливу (ІПСО) (найширше поняття) → Пропаганда/Дезінформація (ядро контенту) → Маніпуляції (механізми впливу) → ІПсВ (цільовий психологічно-соціальний ефект).

---

[17] О.В. Потій, Ю.І. Горбенко, О.А. Замула, К.В. Ісірова. «Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки». 2021. URL: https://duikt.edu.ua/uploads/l_1066_72351971.pdf (дата звернення: 05.03.2026).

[18] Лісовський П.М. Безпекознавство: особистість, держава, суспільство : навч. посібник. К. : Кондор, 2017, 368 с.

[19] Лісовський П.М. Безпекознавство: особистість, держава, суспільство : навч. посібник. К. : Кондор, 2017, 368 с.

[20] Веб-портал ЦЕНТР ПРОТИДІЇ ДЕЗИНФОРМАЦІЇ. 02 грудня 2025. URL: https://cpd.gov.ua/international-direction/ssha/ru-propaganda-poshyryuye-fejky-pro-zlochyny-ukrayinskyh-vijskovyh/ (дата звернення: 05.03.2026).

А в контексті контрпропаганди: Стратегічні комунікації[21] (основа, «легітимний каркас»[22], рамки) → Контрпропаганда як система контрзаходів[23] (практичне наповнення інформацією та виконання конкретних завдань).

1.2. Пропаганда як інструмент державної політики та війни

В контексті національної безпеки пропаганда є не стільки медійною кампанією, а як інструментом політичної боротьби та війни, який впливає на суспільство, його поведінку, моральний стан, довіру до влади та здатність витримувати тривале навантаження в надзвичайних умовах та в довготривалих конфліктах. У класичних навчальних підходах до безпекознавства акцент робиться на системному характері загроз, де інформаційні впливи здатні підривати стійкість держави на рівні особистості, суспільства й інституцій.[24] Відповідно, пропаганду доцільно трактувати як цілеспрямовану комунікаційну діяльність, яка вибудовується під конкретні безпекові ефекти, а не лише під «переконання» у загальному сенсі.

Цілі пропаганди у війні в контексті національної безпеки.

В контексті даної кваліфікаційної роботи доцільно описувати цілі пропаганди не як перелік гасел чи наративів, а як систему цілей та ефектів. У загальному вигляді пропаганда у війні прагне:

- легітимувати власні дії (агресію, окупацію, репресії) і пояснити насильство чи інші дії як норму або необхідність;

---

[21] Лісовський П.М. Безпекознавство: особистість, держава, суспільство : навч. посібник. К. : Кондор, 2017, 368 с.

[22] Лисенко С.О. Стратегічне управління інформаційною безпекою держави : автореферат дисерт. на здобуття наук. ступ. д.н. з держ. упр. ; спец. 25.00.05 - державне управління у сфері державної безпеки та охорони громадського порядку. Житомирська політехніка. 2025. URL: https://ztu.edu.ua/site/files/1/docs/Університет/Спеціалізовані%20вчені%20ради/14.052.03/2025/ref_Лисенко_С.pdf . (дата звернення: 05.03.2026).

[23] О.В. Потій, Ю.І. Горбенко, О.А. Замула, К.В. Ісірова. «Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки». 2021. URL: https://duikt.edu.ua/uploads/l_1066_72351971.pdf (дата звернення: 05.03.2026).

[24] Ліпкан В.А. Національна безпека України : навч. посібник . К. : Кондор, 2008, 552 с.

- делегітимізувати державність противника та його інституції (уряд, збройні сили, правоохоронний блок, дипломатію, конкретних діячів тощо)[25], підривати віру у здатність держави захистити громадян;[26]
- деморалізувати населення і сили оборони, знижувати волю до опору через страх, виснаження, зневіру. Війна як тривала травматична подія породжує емоційні коливання, які стають «вхідними точками» для маніпуляцій;[27]
- поляризувати суспільство, розпалити або посилити внутрішні конфлікти[28], зруйнувати соціальну довіру та згуртованість, що є критичною складовою національної стійкості;[29]
- впливати на міжнародну аудиторію, знижувати підтримку жертви агресії, провокувати «втому», нав'язувати вигідні агресору рамки;[30]
- маскувати реальні події й наміри, створювати інформаційне прикриття для військових та диверсійних дій, знижуючи здатність суспільства адекватно реагувати на загрози.

У такій постановці пропаганда постає як інструмент управління середовищем, де когнітивний вимір (сприйняття, інтерпретації, емоції) перетворюється на чинник боєздатності, керованості та стійкості держави.[31]

---

[25] Ліпкан В.А. Національна безпека України : навч. посібник . К. : Кондор, 2008, 552 с.
[26] Лисенко С.О. Стратегічне управління інформаційною безпекою держави : автореферат дисерт. на здобуття наук. ступ. д.н. з держ. упр. ; спец. 25.00.05 - державне управління у сфері державної безпеки та охорони громадського порядку. Житомирська політехніка. 2025. URL: https://ztu.edu.ua/site/files/1/docs/Університет/Спеціалізовані%20вчені%20ради/14.052.03/2025/ref_Лисенко_С.pdf . (дата звернення: 05.03.2026).
[27] Андрієнко С. С. Психологічна підготовка та підтримка співробітників правоохоронних органів в умовах гібридної війни. Економіка, управління та адміністрування.2025. URL: https://doi.org/10.26642/ema-2024-4(110)-103-108 (дата звернення 06.03.2026).
[28]Лісовський П.М. Безпекознавство: особистість, держава, суспільство : навч. посібник. К. : Кондор, 2017, 368 с.
[29] Мосієнко О., Гордійчук О, Клименко І., Кондратюк Ю. Національна безпека; національні інтереси; глобалізація; глобалізаційні виклики. Society and security. 2024. URL: https://library.ztu.edu.ua/e-copies/sas/2-3(3)/98.pdf (дата звернення: 08.03.2026).
[30] Носенко С., Яковлєв М., Трансформація стримування в контексті російсько-української війни: концептуалізація поняття крізь призму становлення України як середньої держави. Society and security. 2025. URL: https://sas.ztu.edu.ua/article/view/323957/314626 (дата звернення: 09.03.2026).
[31] Ліпкан В.А. Національна безпека України : навч. посібник . К. : Кондор, 2008, 552 с.

Функції пропаганди. Детальне розкладення функцій пропаганди дозволяє зробити аналіз операційним, тобто таким, що є важливим для подальшого проєктування контрзаходів. В контексті підходу національної безпеки доречно буде виділити наступні функції пропаганди:

- рамкова/пояснювальна функція, яка задає «правильну» (тобто таку, що вигідна агресору) інтерпретацію подій і причинність (хто винен, що справедливо, що неминуче);[32]
- мобілізаційна функція, що підтримує готовність до дій, жертв, тривалого напруження, а також виправдовує втрати та репресії серед внутрішньої аудиторії агресора.
- демобілізаційна функція , направлена на противника, що знижує волю до спротиву через страх, зневіру, недовіру, невизначеність;[26]
- ідентифікаційна/інтеграційна функція, що формує образ «свій-чужий», «ми-вони», закріплює групові межі та поляризує сторони конфлікту;[33]
- дискредитаційна функція, що підриває легітимність інститутів і ключових дійових суб'єктів та розхитує політичну стабільність в країні або регіоні.[34]
- відволікаюча або «засмічуюча» функція, яка створює інформаційний шум, перевантажує аудиторію, підсилює інфодемію та ускладнює прийняття рішень;[35]

У сучасному цифровому середовищі ці функції підсилюються технологічно через платформи соціальних мереж, екосистем, їх алгоритми

---

[32] Скрипникова Л.В., Політологія: навчальний посібник. К.: Центр учбової літератури, 2014, 272 с. URL: https://dduvs.edu.ua/biblioteka/biblioteka-studenta-dduvs/pidruchniki-posibniki/politologiya/ (дата звернення: 06.03.2026).

[33] Скрипникова Л.В., Політологія: навчальний посібник. К.: Центр учбової літератури, 2014, 272 с. URL: https://dduvs.edu.ua/biblioteka/biblioteka-studenta-dduvs/pidruchniki-posibniki/politologiya/ (дата звернення: 06.03.2026).

[34] Гаращук, Д., Сергєєв, В. Інфодемія та популізм у цифрову епоху: загрози політичній стабільності та безпекові виклики. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2025-2(8)-61-71 (дата звернення: 06.03.2026).

[35] Гаращук, Д., Сергєєв, В. Інфодемія та популізм у цифрову епоху: загрози політичній стабільності та безпекові виклики. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2025-2(8)-61-71 (дата звернення: 06.03.2026).

поширення та охоплення повідомлень (постів) та інформаційні технології як інструмент безпеки/небезпеки.[36]

Рівні пропаганди. Стратегічний, оперативний, тактичний. Поділ за рівнями виконання чи впливу дає можливість прив'язати пропаганду до задач управління війною.

Так, стратегічний рівень формує «велику історію» та довготривалі рамки, а саме чому та чи інша війна або конфлікт «правильні», що є «перемогою», що є «зрадою», та де є межі моралі. Він тісно пов'язаний із геополітичними інтерпретаціями і конструюванням карти світу.[37]

Оперативний рівень підтримує конкретні політичні/військові цілі кампаній, наприклад як злам підтримки партнерів, розхитування довіри до управлінських рішень, конструювання «втоми» та конфліктів всередині суспільства чи груп. [31]

Тактичний рівень більше швидкі інформаційні вкиди під конкретні події, на кшталт розгону реакцій після обстрілів, криз, інформаційних приводів. Тут пропаганда найчастіше використовує емоційні тригери й психологічний тиск.[38]

Цей поділ також є важливим через призму контрзаходів, що також можуть поділятись на різні рівні. Стратегічні можуть бути націлені на довіру та встановлення етичних та моральних рамко. Оперативні направлені на формування стійкості та опрацювання системних рішень. Тактичні, в свою чергу, направлені на швидкість реагування і кризові комунікації.[39]

---

[36] Сумін, П. Інформаційні технології як інструмент забезпечення національної безпеки на сучасному етапі розвитку: проблеми та перспективи. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2024-6(6)-37-43 (дата звернення: 06.03.2026).

[37] Гольцов А.Г. Геополітика та політична географія : підручник. К. : ЦУЛ, 2021, 416 с. (дата звернення: 13.03.2026).

[38] Андрієнко С. С. Психологічна підготовка та підтримка співробітників правоохоронних органів в умовах гібридної війни. Економіка, управління та адміністрування.2025. URL: https://doi.org/10.26642/ema-2024-4(110)-103-108 (дата звернення 06.03.2026).

[39] Лисенко С.О. Стратегічне управління інформаційною безпекою держави : автореферат дисерт. на здобуття наук. ступ. д.н. з держ. упр. ; спец. 25.00.05 - державне управління у сфері державної безпеки та охорони громадського порядку. Житомирська політехніка. 2025. URL: https://ztu.edu.ua/site/files/1/docs/Університет/Спеціалізовані%20вчені%20ради/14.052.03/2025/ref_Лисенко_С.pdf. (дата звернення: 05.03.2026).

Аудиторії та вразливості. В умовах війни аудиторії доцільно поділяти на внутрішню (суспільство , регіон впливу агресора), зовнішню (суспільство жертви агресії та міжнародна спільнота) та, як підвид обох, вузькі професійні групи, характеризуючи впили на них. Так, внутрішня аудиторія агресора зазнає впливу задля забезпечення підтримки війни, раціоналізація втрат, нейтралізація сумнівів серед населення. Аудиторія жертви агресії зазнає впливу задля деморалізації, недовіри, паніки, поляризації суспільства. Вразливості тут пов'язані з тривалим стресом, виснаженням, психологічними коливаннями, так званими «гойдалками», коли з доволі високою частотою чергуються «хороші» та «погані» новини/ повідомлення націлені на виснаження та сприяння впливу.[40]

Міжнародні аудиторії, в свою чергу, зазнають впливу через формування «втоми», сумнівів у доцільності підтримки, розмивання причинно-наслідкових зв'язків війни тощо.[31] Вузькі професійні групи (правоохоронці, держслужбовці, енергетики, медики, військовослужбовці, дипломати тощо) сприймаються як об'єкти точкового впливу задля отримання тактичних чи навіть стратегічних переваг. [41] Вразливості в цифрову епоху посилюються інформаційними технологіями[42] та структурою цифрових ризиків.[43]

Канали й екосистеми поширення. Аналіз сучасної пропаганди показує її як цілу екосистему з традиційних медіа, цифрових платформ, проксі-ресурсів та мережеві «розгонів» наративів чи меседжів. В контексті національної безпеки принципово, що протидія потребує розуміння мережевої логіки, а саме як дані, смисли й меседжі циркулюють у середовищі, як з'являються тренди, як фіксуються та аналізуються масиви текстів і повідомлень.[44]

---

[40] Андрієнко С. С. Психологічна підготовка та підтримка співробітників правоохоронних органів в умовах гібридної війни. Економіка, управління та адміністрування.2025. URL: https://doi.org/10.26642/ema-2024-4(110)-103-108 (дата звернення 06.03.2026).

[41] Тиравський В. Росія майже на чверть збільшила повітряні атаки на українські заклади охорони здоров'я. 19 березня 2026. URL: https://foreignukraines.com/2026/03/19/russia-has-increased-air-attacks-on-ukrainian-healthcare-facilities-by-almost-a-quarter/ (дата звернення: 21.03.2026).

[42] Наторіна А.О. Синкретичність менеджменту цифрових ризиків та інформаційної безпеки. 27 листопада 2019. URL: https://ema.ztu.edu.ua/article/view/185089 (дата звернення 06.03.2026).

[43] Сумін, П. Інформаційні технології як інструмент забезпечення національної безпеки на сучасному етапі розвитку: проблеми та перспективи. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2024-6(6)-37-43 (дата звернення: 06.03.2026).

[44] Ліпкан В.А. Національна безпека України : навч. посібник . К. : Кондор, 2008, 552 с.

Таким чином можна стверджувати, що пропаганда у війні є багаторівневим інструментом, який працює на безпекові ефекти, використовуючи психологічні тригери та цифрові можливості. Це створює основу наступного підрозділу, де ми розглядаємо, як демократична держава може протидіяти, не втрачаючи легітимності й довіри.

1.3. Контрпропаганда в демократичній державі під час війни. Принципи легітимності, межі дозволеного, ризики віддзеркалення та роль довіри

Контрпропаганда у російсько-українській війні є не «дзеркальною відповіддю» на ворожі меседжі, а комплексом контрзаходів держави й суспільства, спрямованих на збереження керованості, стійкості та здатності країни та нації до тривалого спротиву. У теоретичній рамках національної безпеки безпекові загрози мають багаторівневий характер[45], тобто вони можуть бути воєнними, політичними, соціальними, інформаційними, кібернетичними. При цьому також приймається до уваги, що інформаційна сфера є одночасно середовищем, інструментом і мішенню. Саме тому контрпропаганда має розглядатися не як PR-активність, а як елемент стратегічного управління інформаційною безпекою держави[46] з чіткими цілями, процедурами, процесами, розподілом ролей та критеріями ефективності.

Для демократичної держави під час війни ключовим викликом стає баланс між ефективністю, тобто швидкістю, масштабом, ефективною координацією контрзаходів, та легітимністю, тобто правомірністю, правдивістю, підзвітністю, недопущення внутрішньої маніпуляції[47] тощо. Якщо цей баланс порушено,

---

[45] Лисенко С.О. Стратегічне управління інформаційною безпекою держави : автореферат дисерт. на здобуття наук. ступ. д.н. з держ. упр. ; спец. 25.00.05 - державне управління у сфері державної безпеки та охорони громадського порядку. Житомирська політехніка. 2025. URL: https://ztu.edu.ua/site/files/1/docs/Університет/Спеціалізовані%20вчені%20ради/14.052.03/2025/ref_Лисенко_С.pdf . (дата звернення: 05.03.2026).

[46] Герасимюк К.Х. Механізми державного управління кібер- та інформаційною безпекою: проблеми та шляхи вирішення. Економіка, управління та адміністрування. Жовтень 2021. URL: https://www.researchgate.net/publication/356396763_Mehanizmi_derzavnogo_upravlinna_kiber-_ta_informacijnou_bezpekou_problemi_ta_slahi_virisenna (дата звернення: 07.03.2026).

[47] Ліпкан В.А. Національна безпека України : навч. посібник . К. : Кондор, 2008, 552 с.

держава може отримати короткострокові тактичні вигоди, але втратити стратегічний ресурс – довіру, що автоматично підриває керованість і національну стійкість.[48]

Принципи легітимності контрпропаганди. Легітимність у сфері контрпропаганди являє собою відповідність практик держави базовим засадам безпеки як суспільного блага, тобто захисту людини, її прав, суспільства і держави, збереження інституційної спроможності, підтримання внутрішньої стабільності та національних інтересів держави.[49] Тому легітимна контрпропаганда має працювати за принципами, які не руйнують демократичний порядок всередині країни, навіть коли держава перебуває в режимі жорсткої зовнішньої загрози. [50]

Принцип правдивості. У війні держава не зобов'язана розкривати всю інформацію, через існування режиму воєнної таємниці, але вона зобов'язана не підміняти реальність системною брехнею. У контексті національної безпеки правдивість є не моральною вимогою, а елементом стійкості, тому що, якщо офіційне джерело зруйнувало репутацію, воно втрачає здатність бути точкою опори у кризі, а суспільство переходить у тіньові канали, де домінують чутки й маніпуляції. В умовах інфодемії, тобто коли спостерігається надмірна кількість інформації, а здатність відрізняти істинне знижується, роль правдивої, структурної комунікації зростає, бо саме вона зменшує хаос і поляризацію.[51]

Принцип зменшення шкоди. Контрпропаганда повинна бути спрямована на зменшення шкоди від ворожих впливів, таких як паніки, деморалізації, недовіри, внутрішніх конфліктів тощо.[52] Це відповідає загальній лозіці системної безпеки, де управління спрямоване на збереження функцій держави і суспільства

---

[48] Лісовський П.М. Безпекознавство: особистість, держава, суспільство : навч. посібник. К. : Кондор, 2017, 368 с.
[49] Ліпкан В.А. Національна безпека України : навч. посібник . К. : Кондор, 2008, 552 с.
[50] Лісовський П.М. Безпекознавство: особистість, держава, суспільство : навч. посібник. К. : Кондор, 2017, 368 с.
[51] Гаращук, Д., Сергєєв, В. Інфодемія та популізм у цифрову епоху: загрози політичній стабільності та безпекові виклики. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2025-2(8)-61-71 (дата звернення: 06.03.2026).
[52] Лісовський П.М. Безпекознавство: особистість, держава, суспільство : навч. посібник. К. : Кондор, 2017, 368 с.

під тиском загроз. Психологічний компонент тут є критичним, через те, що тривала війна створює емоційні коливання, виснаження, які роблять аудиторії чутливими до інформаційних вкидів та проявів дезинформації. Саме тому держава має комунікувати так, щоб підтримувати психічну стійкість населення, не розганяючи страх і розпач.[53]

Принцип процедуральності й підзвітності. Легітимна контрпропаганда не являється спонтанним набором реакцій, а є процесом зі своїм набором правил, а саме хто проводить моніторинг загроз, хто проводить їх оцінку, хто ухвалює рішення, хто комунікує від лиця держави, як координуються повідомлення, як виправляються помилки тощо[54]. В сфері національної безпеки це означає інституційне управління, тобто наявністю механізмів державного управління кібер- та інформаційною безпекою, узгодженістю дій та протоколів тощо. [55] Відсутність процедур породжує суперечливі повідомлення, зниження довіри та відкриває простір для ворожих маніпуляцій.

Принцип пропорційності. Засоби протидії загрозам мають відповідати їх рівню. Надмірні обмеження й форсовані (силові) комунікаційні практики можуть створити вторинні ризики, а саме підсилити чутки, сприяти поляризації та популізму, знизити політичну стабільність, що у свою чергу вже являється прямим викликом національній безпеці.[56] Пропорційність означає, що там, де достатньо пояснення і превенції відбувається саме їх застосування. Там же, де

---

[53] Андрієнко С. С. Психологічна підготовка та підтримка співробітників правоохоронних органів в умовах гібридної війни. Економіка, управління та адміністрування.2025. URL: https://doi.org/10.26642/ema-2024-4(110)-103-108 (дата звернення 06.03.2026).

[54] Лисенко С.О. Стратегічне управління інформаційною безпекою держави : автореферат дисерт. на здобуття наук. ступ. д.н. з держ. упр. ; спец. 25.00.05 - державне управління у сфері державної безпеки та охорони громадського порядку. Житомирська політехніка. 2025. URL: https://ztu.edu.ua/site/files/1/docs/Університет/Спеціалізовані%20вчені%20ради/14.052.03/2025/ref_Лисенко_С.pdf . (дата звернення: 05.03.2026).

[55] Герасимюк К.Х. Механізми державного управління кібер- та інформаційною безпекою: проблеми та шляхи вирішення. Економіка, управління та адміністрування. Жовтень 2021. URL: https://www.researchgate.net/publication/356396763_Mehanizmi_derzavnogo_upravlinna_kiber-_ta_informacijnou_bezpekou_problemi_ta_slahi_virisenna (дата звернення: 07.03.2026).

[56] Лисенко С.О. Стратегічне управління інформаційною безпекою держави : автореферат дисерт. на здобуття наук. ступ. д.н. з держ. упр. ; спец. 25.00.05 - державне управління у сфері державної безпеки та охорони громадського порядку. Житомирська політехніка. 2025. URL: https://ztu.edu.ua/site/files/1/docs/Університет/Спеціалізовані%20вчені%20ради/14.052.03/2025/ref_Лисенко_С.pdf . (дата звернення: 05.03.2026).

потрібні правові заходи відбувається застосування їх відповідний у правовий спосіб.[57]

Принцип недискримінації і недопущення внутрішнього ворожнечі. Ворожі операції впливу часто націлені на розкол суспільства чи окремих груп (політичні, релігійні, соціальні тощо). Якщо держава починає комунікаційно стигматизувати «незручні» групи або запускати горизонтальну ворожнечу[58], вона фактично підсилює ціль противника. В контексті національної безпеки важливо дотримуватись розуміння, що внутрішня стабільність і згуртованість – це ресурс безпеки.[59]

Межі дозволеного. Де закінчується контрпропаганда і починається внутрішня маніпуляція. У демократичній державі під час війни межа допустимого визначається не лише законом, а й стратегічною доцільністю, тобто те, що руйнує довіру, у довгій перспективі шкодить безпеці держави. Тому важливо відрізняти законне обмеження інформації, з ціллю не нашкодити обороні (воєнна цензура, або цензура воєнного часу), від інформаційної маніпуляції власним суспільством для зручності управління або узурпації влади.

Внутрішня маніпуляція може давати короткий ефект, але довго не працює, особливо в цифровому середовищі. Вона провокує цинізм (наприклад, укорінення думки «усі брешуть»), а цинізм, в своє чергу, є ідеальним ґрунтом для ворожих інформаційних вкидів. У підсумку держава сама руйнує власні канали комунікації, які є інструментами безпеки.[60]

Окремо важливо дотримання правових меж. Дослідження іноземного досвіду кримінальної відповідальності за пропаганду агресивної війни показує,

---

[57] Лісовський П.М. Безпекознавство: особистість, держава, суспільство : навч. посібник. К. : Кондор, 2017, 368 с.

[58] Мосієнко О., Гордійчук О, Клименко І., Кондратюк Ю. Національна безпека; національні інтереси; глобалізація; глобалізаційні виклики. Society and security. 2024. URL: https://library.ztu.edu.ua/e-copies/sas/2-3(3)/98.pdf (дата звернення: 08.03.2026).

[59] Гаращук, Д., Сергєєв, В. Інфодемія та популізм у цифрову епоху: загрози політичній стабільності та безпекові виклики. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2025-2(8)-61-71 (дата звернення: 06.03.2026).

[60] Гаращук, Д., Сергєєв, В. Інфодемія та популізм у цифрову епоху: загрози політичній стабільності та безпекові виклики. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2025-2(8)-61-71 (дата звернення: 06.03.2026).

що держави розрізняють легітимну свободу слова і небезпечну діяльність, яка сприяє агресії.[61] Але з точки зору контрпропаганди також важливо, щоб правові інструменти не перетворилися на політичний тиск проти внутрішньої дискусії, інакше це вдарить по довірі та політичній стабільності всередині держави.

Ще одним прикладом межі дозволеного можна виділити мовну політику як складова інформаційної безпеки держави. Правовий режим державної мови у сфері забезпечення інформаційної безпеки може підтримувати стійкість інформаційного простору, але водночас він повинен залишатися правовим, прозорим і не дискримінаційним, щоб не продукувати конфліктність, яку противник легко використовує у своїх дистабілізаційних цілях.[62]

Ризик віддзеркалення, коли контрпропаганда копіює пропаганду ворога. Віддзеркаленням є ситуація, коли держава починає використовувати ті самі методи, що й агресор, тобто маніпуляцію, дегуманізацію, емоційний шантаж, перевантаження, створення міфів та альтернативної історії. У короткій дистанції це може здаватися ефективним, але для демократії це стратегічно ризиковано, бо руйнує головні переваги, а саме довіру до державних інститутів та їх легітимність.

Ризик віддзеркалення можна описати у трьох вимірах:

1. Дзеркальність методів.

Якщо держава системно керує суспільством через страх і маніпуляцію, вона створює внутрішній стрес і конфліктність суспільного середовища. У цифрову епоху це швидко конвертується в інфодемію та популістські коливання, що підривають політичну стабільність.[63]

2. Дзеркальність наративів.

---

[61] Канцір В, Олійник Х. Іноземний досвід регламентації кримінальної відповідальності за пропаганду, планування, підготовку, розв'язування та ведення агресивної війни. Вісник Національного університету "Львівська політехніка". 2020. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2020/may/21542/32.pdf (дата звернення: 17.03.2026)

[62] Яковлєв П. Правовий режим державної мови у сфері забезпечення інформаційної безпеки. ТОВ «Гарантія» // Підприємництво, господарство і право.№3. 2020. URL: https://pgp-journal.kiev.ua/archive/2020/3/33.pdf (дата звернення 17.03.2026)

[63] Гаращук, Д., Сергєєв, В. Інфодемія та популізм у цифрову епоху: загрози політичній стабільності та безпекові виклики. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2025-2(8)-61-71 (дата звернення: 06.03.2026).

Контрпропаганда не повинна будувати «контрміфи», що відірвані від реальності та фактів. Будь-яка розбіжність між офіційною рамкою і реальними подіями стає точкою атаки противника. У результаті це призводить до ситуації, коли навіть правдиві повідомлення знецінюються та не сприймаються суспільством або цільовою групою.

3. Дзеркальність інституцій.

Коли контрпропаганда стає закритою вертикаллю без підзвітності, вона деградує в механізм контролю інформаційного простору. З точки зору національної безпеки це створює нові уразливості, такі як падіння довіри до державних інституцій, появі тіньових інформаційних ринків (характерний приклад – анонімні Телеграм-канали, націлені на внутрішню аудиторію і маючі на меті дискредитацію опозиції), радикалізації суспільства, появи конфлікти, саме того чого і добивається противник.

Звідси випливає практичний висновок, що демократична держава має протидіяти не «брехнею на брехню», а процедурами, координацією[64], швидким поясненням, превенцією і верифікованими даними. [65]

Довіра як стратегічний ресурс. Чому контрпропаганда без довіри не працює. Довіра в умовах війни являється операційним ресурсом, який визначає здатність держави управляти кризою, що склалася. Якщо суспільство довіряє інститутам, то воно виконує рекомендації, підтримує мобілізаційні рішення, витримує обмеження, менше піддається паніці від кожного інформаційного вкиду, менше піддається маніпуляціям тощо. Психологічні дослідження, у тому числі про підтримку правоохоронного та військового персоналу в гібридній війні, підкреслюють, що тривалий стрес змінює поведінку і збільшує потребу в

---

[64] Лисенко С.О. Стратегічне управління інформаційною безпекою держави : автореферат дисерт. на здобуття наук. ступ. д.н. з держ. упр. ; спец. 25.00.05 - державне управління у сфері державної безпеки та охорони громадського порядку. Житомирська політехніка. 2025. URL: https://ztu.edu.ua/site/files/1/docs/Університет/Спеціалізовані%20вчені%20ради/14.052.03/2025/ref_Лисенко_С.pdf . (дата звернення: 05.03.2026).

[65] Герасимюк К.Х. Механізми державного управління кібер- та інформаційною безпекою: проблеми та шляхи вирішення. Економіка, управління та адміністрування. Жовтень 2021. URL: https://www.researchgate.net/publication/356396763_Mehanizmi_derzavnogo_upravlinna_kiber-_ta_informacijnou_bezpekou_problemi_ta_slahi_virisenna (дата звернення: 07.03.2026).

зрозумілих орієнтирах. Паралельно психотерапевтична оптика війни підкреслює «емоційні гойдалки» як нормальний ефект тривалого насильства і невизначеності. Це означає, що контрпропаганда має враховувати психологічну реальність суспільства, усвідомлюючи, що у кризі люди або шукають опори, або тікають у чутки/псевдоекспертів/радикальні пояснення та теорії змов.

Інфодемія, як феномен цифрової епохи показує, що надлишок інформації та популістські механіки уваги можуть створювати загрози політичній стабільності. Тому офіційна комунікація має зменшувати «інформаційний шум», а не збільшувати його. Це прямо пов'язано з довірою, коли офіційні канали говорять просто, послідовно, не суперечачи один одному та раніше викладеним фактам, вони стають маяком у кризі, на який суспільство може орієнтуватись в моменти невизначеності. Практично довіра формується трьома компонентами, а саме стабільністю повідомлень та координації, верифікованістю даних і здатністю визнавати обмеження, та повагою до цільової аудиторії.

Стабільність повідомлень і координація досягається, коли інституції держави узгоджені, вони не конфліктують між собою в публічному полі, що знижує простір для маніпуляцій.[66] І навпаки, суперечливі повідомлення створюють простір для ворожих інформаційних вкидів. Верифікованість даних і здатність визнавати обмеження проявляється тоді, коли держава може відмовитись від публічних коментарів з причин безпеки і це буде легітимно. Але вона не може системно підмінювати невідоме вигадкою, бо це руйнує репутацію самого джерела.

Повага до аудиторії. «Номенклатурна» комунікація «згори вниз» до цільової аудиторії, як до об'єкта управління, створює опір і цинізм. Водночас, комунікація як партнерство підтримує стійкість суспільства та груп. Дане

[66] Герасимюк К.Х. Механізми державного управління кібер- та інформаційною безпекою: проблеми та шляхи вирішення. Економіка, управління та адміністрування. Жовтень 2021. URL: https://www.researchgate.net/publication/356396763_Mehanizmi_derzavnogo_upravlinna_kiber-_ta_informacijnou_bezpekou_problemi_ta_slahi_virisenna (дата звернення: 07.03.2026).

твердження можна та необхідно сприймати не як риторику, а як безпековий механізм.

Інституційна логіка контрпропаганди. Від реакції до системи. Однією з ключових слабкостей протидії являється її реактивність, а саме відповіді лише після атаки. Але для національної безпеки держави потрібна система, яка включає в себе моніторинг і раннє виявлення загроз, ризик менеджмент, координацію суб'єктів, превентивність і підвищення стійкості, а також політику щодо використання і зберігання даних, та приватності. Нижче розглянемо кожен з цих компонентів.

Моніторинг і раннє виявлення загроз. В даному контексті мається на увазі не лише популярні фейки, а картографування тем, тез, наративів, каналів та повторюваних конструкцій. Лінгвістичний аналіз масивів інтернет-медіа і соцмереж є одним із підходів до оцінювання суспільних процесів і може бути корисним як методологічна база для моніторингу.[67]

Ризик-менеджмент в контексті планування контрпропаганди. Контрпропаганда має плануватися через системний ризик-підхід, де активи (такі як довіра, керованість, міжнародна підтримка), загрози (операції впливу), вразливості (інфодемія, поляризація суспільства, цифрові ризики тощо), наслідки та пріоритети реагування аналізуються системно, одночасно та комплексно. Методики оцінки й управління ризиками кібер- і інформаційної безпеки дають тут простір для побудови системи.[68]

Координація суб'єктів. Інформаційна безпека держави потребує узгодженості між різними органами влади, інакше протидія стає

[67] Потій О.В., Горбенко Ю.І., Замула О.А., Ісірова К.В. «Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки». 2021. URL: https://duikt.edu.ua/uploads/l_1066_72351971.pdf (дата звернення: 05.03.2026).

[68] Герасимюк К.Х. Механізми державного управління кібер- та інформаційною безпекою: проблеми та шляхи вирішення. Економіка, управління та адміністрування. Жовтень 2021. URL: https://www.researchgate.net/publication/356396763_Mehanizmi_derzavnogo_upravlinna_kiber-_ta_informacijnou_bezpekou_problemi_ta_slahi_virisenna (дата звернення: 07.03.2026).

фрагментованою. Механізми державного управління кібер- та інформаційною безпекою якраз і описують проблему координації та шляхи її вирішення.[69]

Превенція і підвищення стійкості. Окрім спростування, потрібні дії, що зменшують сприйнятливість аудиторій до ворожих впливів, такі як просвіта, інформаційна гігієна, робота з психологічною витривалістю, а також підтримка ключових груп.

Політика використання та обробки даних і забезпечення приватності. У цифрову епоху контрзаходи легко перетинаються з персональними даними. Безпекові рішення мають враховувати режим захисту персональних даних і не створювати нових вразливостей (витоки даних, делегітимізація державних інституцій-зберігачів даних, виникнення конфліктів між групами або всередині суспільства в наслідок оприлюднення даних тощо).[70]

Міжнародний і компаративний вимір. Порівняльний аналіз. Порівняльний аналіз на прикладі інформаційної політики Чехії під впливом війни показує, що демократії знаходяться у пошуку інституційних форматів протидії дезінформації, таких як координаційні механізми, політики, комунікаційні практики, роботу з суспільством.[71] Для України це є важливим з точки зору джерела потенційних моделей для імплементації[72], але з урахуванням в процесі адаптації норм воєнного стану та власні інституційні спроможності.[73]

Внутрішні вразливості як поле боротьби. Політична свідомість, цифрові ризики, соціальні конфлікти. Ворожа пропаганда найкраще працює

---

[69] Фасій, Б. Національна безпека та захист персональних даних в епоху цифрових технологій. Society and Security. URL: https://doi.org/10.26642/sas-2024-6(6)-76-82 (дата звернення 18.03.2026)
[70] Фасій, Б. Національна безпека та захист персональних даних в епоху цифрових технологій. Society and Security. URL: https://doi.org/10.26642/sas-2024-6(6)-76-82 (дата звернення 18.03.2026)
[71] Корнійчук, Л., Матвійчук, Н. Інформаційна політика Чеської Республіки як інструмент забезпечення інформаційної безпеки під впливом російсько-української війни. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2025-5(11)-19-25 (дата звернення 19.03.2026)
[72] Ліпкан В.А. Національна безпека України : навч. посібник . К. : Кондор, 2008, 552 с.
[73] Лисенко С.О. Стратегічне управління інформаційною безпекою держави : автореферат дисерт. на здобуття наук. ступ. д.н. з держ. упр. ; спец. 25.00.05 - державне управління у сфері державної безпеки та охорони громадського порядку. Житомирська політехніка. 2025. URL: https://ztu.edu.ua/site/files/1/docs/Університет/Спеціалізовані%20вчені%20ради/14.052.03/2025/ref_Лисенко_С.pdf . (дата звернення: 05.03.2026).

там, де є внутрішні тріщини або протиріччя[74], такі як недовіра, поляризація суспільства, соціальні, етнічні, релігійні конфлікти тощо. Трансформації політичної свідомості українців у війні мають транзитивний характер і створюють змінне поле вразливостей, що потребує системної уваги. Паралельно глобалізаційні виклики та національні інтереси формують контекст, у якому інформаційні загрози накладаються на ширші процеси.[75] Цифрові ризики також є системними, тому менеджмент цифрових ризиків і інформаційної безпеки потребує синкретичного підходу, бо загроза може виникати на стику технологій, економіки, політики й взаємовідносин.[76]

Критерії ефективності контрпропаганди. У національній безпеці ефективність не повинна зводитись до кількісного показника, як, наприклад, кількість спростувань. Доцільно оцінювати контрпропаганду через критерії:

- швидкість реагування (тобто час до першого пояснення, стабілізації ситуації, спростування);
- узгодженість повідомлень (відсутність взаємних суперечностей між фактами, джерелами та каналами комунікації);
- зменшення шкоди (зниження паніки, виникнення конфлікту, зменшення конфліктної обстановки, конфлікності між групами, зниження ризикової поведінки);
- динаміка довіри (вимірювання зміни довіри до державних інституцій та офіційних джерел);
- стійкість аудиторій (зменшення сприйнятливості до повторюваних маніпуляцій, наративів або методів);

---

[74] Загурська-Антонюк, В., Загурський, В. Транзитивність політичної свідомості українців в умовах російсько-української війни. Society and Security. 2024. URL: https://doi.org/10.26642/sas-2024-1(2)-40-45 (дата звернення: 18.03.2026)

[75] Наторіна А.О. Синкретичність менеджменту цифрових ризиків та інформаційної безпеки. 27 листопада 2019. URL: https://ema.ztu.edu.ua/article/view/185089 (дата звернення 06.03.2026).

[76] Сумін, П. Інформаційні технології як інструмент забезпечення національної безпеки на сучасному етапі розвитку: проблеми та перспективи. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2024-6(6)-37-43 (дата звернення: 06.03.2026).

- стабільність міжнародної підтримки (у випадках, коли кампанія націлена на зовнішню аудиторію).

Ризик-підхід до кібер- та інформаційної безпеки дозволяє прив'язати ці критерії до активів і наслідків та зробити оцінювання управлінським, а не декларативним.[77]

Отже, з контексту розглянутих у підрозділі тез можливо зробити проміжні висновки, що демократична контрпропаганда під час війни є легітимною лише тоді, коли вона підсилює стійкість і керованість суспільства та не перетворюється на внутрішню маніпуляцію. Межі дозволеного визначаються, в свою чергу, цілями й методами, таким як концентрація сил та засобів на протидію ворожим впливам, але відкиданням використання методів системної брехні власному суспільству та «виробництво правди» з залученням адмінресурсу. Відповідні праці у сфері національної безпеки підтверджують, що ризик віддзеркалення стратегічно небезпечний, бо копіювання маніпулятивних методів руйнує довіру і робить суспільство вразливішим. Довіра, в свою чергу, являється головним ресурсом контрпропаганди, тому що без довіри держава втрачає здатність стабілізувати кризу.

Контрпропаганда має бути інституційною системою з комплексною підходом, що включає моніторинг, ризик-менеджмент, координацію державних органів, превентивністю дій і вимірюванням ефективності засобів.

1.4. Методологія дослідження. Аналітичні рамки, методи, критерії оцінювання ефективності

Теоретико-методологічна основа дослідження. Теоретичною основою дослідження виступає системний підхід, який дозволяє розглядати пропаганду і контрпропаганду як частини цілісної системи інформаційного протистояння. [78] У

[77] Потій О.В., Горбенко Ю.І., Замула О.А., Ісірова К.В. «Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки». 2021. URL: https://duikt.edu.ua/uploads/l_1066_72351971.pdf (дата звернення: 05.03.2026).
[78] Ліпкан В.А. Національна безпека України : навч. посібник . К. : Кондор, 2008, 552 с.

межах цього підходу кожне інформаційне явище аналізується не саме по собі, а через його зв’язки з іншими елементами, такими як державні інституції, канали комунікації, аудиторії розповсюдження, психологічні ефекти, цифрові ризики, міжнародний контекст та політичними процесами, що відбуваються у період часу. Системний підхід є методологічно виправданим, оскільки дозволяє уникнути редукціонізму - тобто спрощеного зведення складних інформаційних процесів до “боротьби меседжів”. Для нашої роботи це є принциповим, так як безпекова аналітика вимагає бачити не лише контент, а й функціонування системи вцілому. [79]

Другим базовим елементом методології можна виділити інституційний підхід. Його застосування обумовлене тим, що контрпропаганда у демократичній державі є не спонтанною реакцією на ворожі інформаційні вкиди, а діяльністю, яка реалізується через певні суб’єкти, компетенції, процедури, механізми координації та правові режими. [80] Саме інституційний підхід дає можливість дослідити, як формуються та функціонують механізми державного управління кібер- та інформаційною безпекою, як розподіляються ролі між різними органами, які існують процедурні обмеження, де виникають вузькі місця координації та яким чином ці фактори впливають на ефективність контрзаходів.[81]

Третім компонентом виступає комунікаційно-наративний підхід, який дозволяє аналізувати пропаганду як процес конструювання сенсів, а не лише як

---

[79] Лисенко С.О. Стратегічне управління інформаційною безпекою держави : автореферат дисерт. на здобуття наук. ступ. д.н. з держ. упр. ; спец. 25.00.05 - державне управління у сфері державної безпеки та охорони громадського порядку. Житомирська політехніка. 2025. URL: https://ztu.edu.ua/site/files/1/docs/Університет/Спеціалізовані%20вчені%20ради/14.052.03/2025/ref_Лисенко_С.pdf . (дата звернення: 05.03.2026).

[80] Лисенко С.О. Стратегічне управління інформаційною безпекою держави : автореферат дисерт. на здобуття наук. ступ. д.н. з держ. упр. ; спец. 25.00.05 - державне управління у сфері державної безпеки та охорони громадського порядку. Житомирська політехніка. 2025. URL: https://ztu.edu.ua/site/files/1/docs/Університет/Спеціалізовані%20вчені%20ради/14.052.03/2025/ref_Лисенко_С.pdf . (дата звернення: 05.03.2026).

[81] Герасимюк К.Х. Механізми державного управління кібер- та інформаційною безпекою: проблеми та шляхи вирішення. Економіка, управління та адміністрування. Жовтень 2021. URL: https://www.researchgate.net/publication/356396763_Mehanizmi_derzavnogo_upravlinna_kiber-_ta_informacijnou_bezpekou_problemi_ta_slahi_virisenna (дата звернення: 07.03.2026).

набір повідомлень.[82] У даному підході важливими стають категорії наративу, фрейму, образу ворога, символічного протиставлення, емоційної мобілізації, інформаційного шуму та маніпуляцій. Саме через цю методологічну призму можна дослідити, як пропаганда впливає на політичну свідомість, колективні уявлення та поведінкові установки. Для цього корисними є напрацювання з політології, геополітики та робіт, присвячених інфодемії, популізму, маніпулятивним технологіям, політичній стабільності та іншим.[83]

Четвертим елементом виступає ризик-орієнтований підхід, який є необхідним не тільки для оцінювання змісту впливів, а також їхньої потенційної шкоди для системи національної безпеки. Пропагандистський вплив має оцінюватися не лише за його «гучністю» чи аудиторним охопленням, а й за тим, якими є його наслідки в контексті довіри, стійкості, політичної стабільності, функціонування державних інституцій, цифрової безпеки та міжнародної підтримки. Саме тому доречним є застосування підходів, які використовуються у сфері аналізу й управління ризиками кібер- та інформаційної безпеки, серед яких можна навести виділення активів, загроз, вразливостей, ймовірностей, сценаріїв наслідків і способів реагування на загрози.[84]

Основні принципи методології. Для забезпечення внутрішньої цілісності дослідження методологія повинна спиратися на низку принципів. Нижче наведено основні принципи, використані у рамках підготовки даної роботи.

Принцип міждисциплінарності означає, що жодна з площин, таких як безпекова, політична, психологічна, правова або технологічна не може бути проігнорована.[85] Пропаганда є одночасно комунікаційним, політичним і

---

[82] Скрипникова Л.В., Політологія: навчальний посібник. К.: Центр учбової літератури, 2014, 272 с. URL: https://dduvs.edu.ua/biblioteka/biblioteka-studenta-dduvs/pidruchniki-posibniki/politologiya/ (дата звернення: 06.03.2026).

[83] Гаращук, Д., Сергєєв, В. Інфодемія та популізм у цифрову епоху: загрози політичній стабільності та безпекові виклики. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2025-2(8)-61-71 (дата звернення: 06.03.2026).

[84] Потій О.В., Горбенко Ю.І., Замула О.А., Ісірова К.В. «Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки». 2021. URL: https://duikt.edu.ua/uploads/l_1066_72351971.pdf (дата звернення: 05.03.2026).

[85] Сумін, П. Інформаційні технології як інструмент забезпечення національної безпеки на сучасному етапі розвитку: проблеми та перспективи. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2024-6(6)-37-43 (дата звернення: 06.03.2026).

психологічним явищем. Контрпропаганда, в свою чергу, являється одночасно комунікаційною практикою, інституційною функцією і механізмом управління ризиками.[86]

Принцип системності передбачає, що кожне явище має аналізуватися в його зв'язках з іншими елементами середовища. Наприклад, окремий ворожий наратив має сенс не сам по собі, а в контексті більш широкої кампанії, цільової аудиторії, цифрового каналу, політичної ситуації та психологічного стану суспільства.[87]

Принцип верифікованості означає, що висновки мають ґрунтуватися на ідентифікованих поняттях, чітких критеріях і доказовій лозіці, а не на інтуїтивних суб'єктивних оцінках. Для теми пропаганди це особливо важливо, оскільки сам предмет дослідження насичений маніпуляціями, спотворенням фактів, емоційними інтерпретаціями і спокусою до перебільшень.

Принцип прикладної релевантності передбачає, що методологія повинна бути придатною не лише для опису явища, а й для формулювання практичних висновків щодо контрзаходів.[88] Саме тому дана робота не може акцентуватися виключно на теоретичному рівні, вона має давати інструментарій для оцінювання вразливостей, ефективності та пріоритетів реагування.[89]

Методи дослідження. У межах зазначеної методології доцільним є використання сукупності взаємодоповнювальних методів, наведених нижче.

Контент-аналіз. Контент-аналіз застосовується для виявлення повторюваних тем, повідомлень, образів, формулювань і смислових конструкцій

---

[86] Ліпкан В.А. Національна безпека України : навч. посібник . К. : Кондор, 2008, 552 с..

[87] Мосієнко О., Гордійчук О, Клименко І., Кондратюк Ю. Національна безпека; національні інтереси; глобалізація; глобалізаційні виклики. Society and security. 2024. URL: https://library.ztu.edu.ua/e-copies/sas/2-3(3)/98.pdf (дата звернення: 08.03.2026).

[88] Лисенко С.О. Стратегічне управління інформаційною безпекою держави : автореферат дисерт. на здобуття наук. ступ. д.н. з держ. упр. ; спец. 25.00.05 - державне управління у сфері державної безпеки та охорони громадського порядку. Житомирська політехніка. 2025. URL: https://ztu.edu.ua/site/files/1/docs/Університет/Спеціалізовані%20вчені%20ради/14.052.03/2025/ref_Лисенко_С.pdf . (дата звернення: 05.03.2026).

[89] Герасимюк К.Х. Механізми державного управління кібер- та інформаційною безпекою: проблеми та шляхи вирішення. Економіка, управління та адміністрування. Жовтень 2021. URL: https://www.researchgate.net/publication/356396763_Mehanizmi_derzavnogo_upravlinna_kiber-_ta_informacijnou_bezpekou_problemi_ta_slahi_virisenna (дата звернення: 07.03.2026).

у пропагандистських матеріалах. Його використання дозволяє не обмежуватися інтуїтивним враженням від інформаційного потоку, а фіксувати сталі елементи комунікації. Для даної теми це важливо, оскільки російська пропаганда працює не через хаотичний набір повідомлень, а через системне повторення певних тез, сенсів, образів та інтерпретацій. Контент-аналіз у поєднанні з аналізом цифрових масивів даних може давати змогу виявляти закономірності, що неочевидні на рівні поодиноких прикладів.[90]

Наративний аналіз

Наративний аналіз є ключовим методом для вивчення пропаганди, оскільки вона працює через «великі історії», які задають аудиторії межі розуміння подій. [91] Наративний аналіз дозволяє виявити, як окремі повідомлення вбудовуються у ширшу історію, тобто хто є жертвою, хто ворогом, хто винен, що є загрозою, що є порятунком тощо. Для роботи про російсько-українську війну цей метод особливо важливий, оскільки саме через наративи агресор легітимує насильство, виправдовує окупацію, перекладає відповідальність і намагається делегітимізувати українську державність.[92]

Дискурс-аналіз

Дискурс-аналіз дає змогу досліджувати не лише зміст повідомлень, а й способи, в які мовлення формує політичну реальність. Через дискурс-аналіз можна простежити, як будуються категорії «свій-чужий», «норма-загроза», «захист-агресія», як легітимізується насильство, яким чином відбувається дегуманізація противника, як формуються уявлення про політичну неминучість певних рішень тощо. Для даної роботи це метод є важливим, оскільки дозволяє

---

[90] Згуровський М. З., Ланде Д. В., Болдак А. О., Єфремов К. В., Перестюк М. М. Лінгвістичний аналіз даних інтернет-медіа та соціальних мереж у задачах оцінювання суспільних перетворень. *Кібернетика та системний аналіз*. 2021. URL: http://jnas.nbuv.gov.ua/article/UJRN-0001221023 (дата звернення 18.03.2026)

[91] Гаращук, Д., Сергєєв, В. Інфодемія та популізм у цифрову епоху: загрози політичній стабільності та безпекові виклики. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2025-2(8)-61-71 (дата звернення: 06.03.2026).

[92] Гольцов А.Г. Геополітика та політична географія : підручник. К. : ЦУЛ, 2021, 416 с. (дата звернення: 13.03.2026).

аналізувати пропаганду не лише як передачу інформації, а як виробництво політичних сенсів.[93]

Порівняльний аналіз

Порівняльний аналіз використовується для зіставлення підходів України та інших держав до інформаційної безпеки, дезінформації та контрпропаганди. Його функція полягає не в механічному копіюванні іноземного досвіду, а у виявленні моделей, які можуть бути адаптовані до українських умов. Компаративний вимір також дозволяє побачити, які практики є універсальними для демократичних держав, а які прив'язані до конкретного політичного чи правового контексту. Для цього корисними є праці, що досліджують інформаційну політику інших країн у відповідь на інформаційні загрози, зокрема під впливом російсько-української війни.[94]

Кейс-стаді

Метод кейс-стаді дозволяє перейти від загальних положень до аналізу конкретних кампаній, подій, хвиль дезінформації або кризових інформаційних епізодів. Його перевага полягає в тому, що він дозволяє простежити динаміку, а саме як формувався наратив, через які канали він поширювався, які цільові аудиторії були мішенями, якою була реакція держави чи суспільства, які наслідки можна зафіксувати тощо. В контексті праці, присвяченій пропаганді у російсько-українській війні, кейс-стаді доцільно застосовувати для демонстрації того, що пропаганда і контрпропаганда мають не абстрактний, а прикладний, керований характер.[95]

Аналіз нормативно-правових і концептуальних документів

---

[93] Ліпкан В.А. Національна безпека України : навч. посібник . К. : Кондор, 2008, 552 с.

[94] Корнійчук, Л., Матвійчук, Н. Інформаційна політика Чеської Республіки як інструмент забезпечення інформаційної безпеки під впливом російсько-української війни. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2025-5(11)-19-25 (дата звернення 19.03.2026).

[95] Герасимюк К.Х. Механізми державного управління кібер- та інформаційною безпекою: проблеми та шляхи вирішення. Економіка, управління та адміністрування. Жовтень 2021. URL: https://www.researchgate.net/publication/356396763_Mehanizmi_derzavnogo_upravlinna_kiber-_ta_informacijnou_bezpekou_problemi_ta_slahi_virisenna (дата звернення: 07.03.2026).

Оскільки дослідження виконується в межах спеціальності Національна безпека, обов'язковим є аналіз документів і концепцій, які формують інституційне бачення інформаційної безпеки. Такий аналіз дозволяє виявити, як держава визначає загрози, цілі, принципи реагування, інструменти та механізми координації. У поєднанні з теоретичними працями він формує базу для оцінки того, наскільки практичні рішення узгоджені з принципами безпеки, легітимності та ефективності.[96]

Емпірична база і логіка відбору матеріалу. Емпірична база дослідження має формуватися так, щоб забезпечити репрезентативність різних аспектів проблеми. З одного боку, це теоретичні праці з безпекознавства, національної безпеки, політології, геополітики, психології війни та цифрової безпеки. З іншого боку, спеціалізовані статті про інфодемію, цифрові ризики, мовний режим інформаційної безпеки, інформаційні політики інших держав, методи протидії ІПСО та ризик-орієнтовані підходи до кібер- й інформаційної безпеки.[97]

Логіка відбору матеріалу ґрунтується на трьох основних критеріях. По-перше, джерела мають бути релевантними темі, тобто містити поняття, тези або методологічні положення, які безпосередньо стосуються пропаганди, контрпропаганди, інформаційної безпеки, цифрових ризиків, політичної стабільності чи психологічних ефектів війни. По-друге, джерела мають бути функціонально придатним, щоб давати теоретичну базу, методи аналізу та прикладний чи компаративний матеріал для аналізу. По-третє, джерела мають бути вбудованими у логіку розділу через поняття, аналітичні межі, інституційні механізми, критерії оцінки ефективності.

Критерії оцінювання ефективності контрпропаганди. Окреме місце у методології займає питання оцінювання ефективності. Це принципово важливо, оскільки без критеріїв оцінювання контрпропаганда залишається сферою

---

[96] Лисенко С.О. Стратегічне управління інформаційною безпекою держави : автореферат дисерт. на здобуття наук. ступ. д.н. з держ. упр. ; спец. 25.00.05 - державне управління у сфері державної безпеки та охорони громадського порядку. Житомирська політехніка. 2025. URL: https://ztu.edu.ua/site/files/1/docs/Університет/Спеціалізовані%20вчені%20ради/14.052.03/2025/ref_Лисенко_С.pdf . (дата звернення: 05.03.2026).

[97] Ліпкан В.А. Національна безпека України : навч. посібник . К. : Кондор, 2008, 552 с..

декларацій, тобто відреагувати, спростувати, пояснити. Проте це не дає розуміння, чи це реально зменшило шкоду та підвищило стійкість суспільства чи групи, чи ні.

Для даного дослідження доцільно використовувати такі критерії ефективності:

1. Швидкість реагування.

Оцінюється не лише факт відповіді, а і те, наскільки швидко держава чи інші суб'єкти контрзаходів формують первинне пояснення, здатне стабілізувати інформаційне поле. У кризових комунікаціях затримка часто працює на користь противника.

2. Узгодженість повідомлень.

Якщо різні інституції подають різні трактування подій, це створює простір для маніпуляцій. Координація є ключем до довіри й ефективності. [98]

3. Зменшення шкоди.

Оцінювання повинно фокусуватися на тому, чи зменшилася паніка, чи знизилася конфліктність, чи було попереджена ризикова поведінка, чи не посилилися наявні вразливості і чи не створились нові. Цей критерій прямо пов'язаний із ризик-орієнтованим підходом до безпеки.[99]

4. Динаміка довіри.

Ефективна контрпропаганда має підтримувати або підвищувати довіру до державних інституцій і офіційних каналів комунікації. Якщо після здійснення контрзаходів ступінь довіри падає, це може означати, що інструмент є контрпродуктивним, тобто працює проти власної мети.[100]

5. Стійкість цільових аудиторій.

---

[98] Герасимюк К.Х. Механізми державного управління кібер- та інформаційною безпекою: проблеми та шляхи вирішення. Економіка, управління та адміністрування. Жовтень 2021. URL: https://www.researchgate.net/publication/356396763_Mehanizmi_derzavnogo_upravlinna_kiber-_ta_informacijnou_bezpekou_problemi_ta_slahi_virisenna (дата звернення: 07.03.2026).

[99] Потій О.В., Горбенко Ю.І., Замула О.А., Ісірова К.В. «Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки». 2021. URL: https://duikt.edu.ua/uploads/l_1066_72351971.pdf (дата звернення: 05.03.2026).

[100] Андрієнко С. С. Психологічна підготовка та підтримка співробітників правоохоронних органів в умовах гібридної війни. Економіка, управління та адміністрування.2025. URL: https://doi.org/10.26642/ema-2024-4(110)-103-108 (дата звернення 06.03.2026).

Стійкість цільових аудиторій є здатність цільових груп краще розпізнавати повторювані маніпулятивні прийоми, бути менш вразливими до інфодемії, паніки, емоційного шантажу та «гойдалок». Це один з найважливіших стратегічних критеріїв, оскільки він показує не реакцію на окремий інформаційний вкид, а довготривалий контрпропагандиський ефект.[101]

6. Інституційна відтворюваність.

Ефективна контрпропаганда не повинна залежати від випадкових успішних рішень окремих осіб. Вона має бути процедурно відтворюваною, тобто такою, яку можна повторити в іншій кризовій ситуації без втрати якості.

Обмеження методології. Будь-яка методологія має свої обмеження, які потрібно фіксувати, щоб уникнути ілюзії «всеохоплюваності». По-перше, пропаганда і контрпропаганда є динамічними процесами, які змінюються швидше, ніж встигає стабілізуватися академічний опис процесів. По-друге, далеко не всі ефекти можна виміряти прямо, бо, наприклад, падіння чи зростання ступеню довіри часто мають багатофакторну природу. По-третє, інформаційні процеси нерідко накладаються на психологічні, соціальні, економічні та політичні фактори, що ускладнює чисте виділення їх причинно-наслідкових зв’язків. Саме тому при виконанні аналітичного дослідження необхідно уникати категоричних висновків там, обережна аналітична оцінка буде більш доречною.

Водночас, ці обмеження не скасовують цінності дослідження, а, навпаки, підкреслюють необхідність комбінованої методології, яка поєднує різні методи і дозволяє будувати не спрощену, а багатовимірну картину інформаційного протистояння.

Отже, в якості проміжних висновків даного підрозділу можна виділити наступні твердження.

---

[101] Гаращук, Д., Сергєєв, В. Інфодемія та популізм у цифрову епоху: загрози політичній стабільності та безпекові виклики. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2025-2(8)-61-71 (дата звернення: 06.03.2026).

Методологія дослідження пропаганди та контрпропаганди в російсько-українській війні повинна бути міждисциплінарною, системною, ризик-орієнтованою, прикладною та релевантною.

Базовими для цього дослідження є системний, інституційний, комунікаційно-наративний і ризик-орієнтований підходи, що в сукупності дозволяють аналізувати пропаганду не лише як контент, а як частину комплексу безпекових впливів.

Основними методами дослідження вибрані контент-аналіз, наративний аналіз, дискурс-аналіз, порівняльний аналіз, кейс-стаді та аналіз нормативно-правових і концептуальних документів.

Ефективність контрпропаганди доцільно вимірювати через швидкість реагування, узгодженість повідомлень, зменшення шкоди, динаміку довіри, стійкість цільових аудиторій та інституційну відтворюваність.

Комбінована методологія дозволяє перейти від опису інформаційних явищ до формування аналітично обґрунтованих висновків і практичних рекомендацій у сфері національної безпеки.

Висновки до Розділу 1

У даному розділі було визначено теоретико-методологічні засади аналізу пропаганди та контрпропаганди як складових інформаційного протиборства у системі національної безпеки. Було уточнено понятійно-категоріальний апарат дослідження, так як саме чітке розмежування базових понять дає змогу уникнути підміни явищ і коректно оцінювати їхню роль у сучасній війні. У рамках розділу розкрито співвідношення понять «пропаганда», «дезінформація», «маніпуляція», «інформаційно-психологічний вплив», «інформаційно-психологічна спеціальна операція», «стратегічні комунікації» та «контрпропаганда». Було обґрунтовано не тотожність даних категорій, попри їх взаємодію між собою, яка утворює єдину систему впливу на цільові аудиторії, в реальних інформаційних кампаніях.

У розділі доведено, що пропаганда у війні не може розглядатися лише як форма комунікації або засіб поширення певних повідомлень. У безпековому вимірі вона виступає інструментом досягнення воєнно-політичних цілей, оскільки спрямована на зміну сприйняття реальності та вплив на поведінку різних аудиторій. Окрему увагу приділено контрпропаганді демократичної держави під час війни. Було встановлено, що ефективна контрпропаганда не повинна бути дзеркальним копіюванням методів держави-агресора. Її завдання полягає у зменшенні шкоди від ворожого впливу, підтриманні суспільної стійкості, зміцненні довіри до державних інституцій та забезпеченні здатності держави пояснювати свої дії в умовах кризи. У цьому контексті особливого значення набувають принципи правдивості, легітимності, процесуальності, пропорційності, недискримінації та підзвітності.

Даний розділ формує теоретичну й методологічну базу всієї роботи. У ньому показано, що аналіз пропаганди та контрпропаганди потребує не лише опису окремих повідомлень чи фейків, а комплексного дослідження інформаційних впливів як елементів національної безпеки. Це створює необхідну аналітичну основу для подальшого вивчення російських пропагандистських кампаній, їхніх наративів, інструментів, каналів поширення та цільових аудиторій, а також для розробки практичних критеріїв оцінювання ефективності українських контрзаходів.

РОЗДІЛ 2. РОСІЙСЬКА ПРОПАГАНДА У ВІЙНІ ПРОТИ УКРАЇНИ. СИСТЕМНИЙ АНАЛІЗ НАРАТИВІВ, ІНСТРУМЕНТІВ, КАНАЛІВ ТА АУДИТОРІЙ

2.1. Еволюція російської пропаганди у війні проти України

Еволюція російської пропаганди у війні проти України не може бути пояснена як сукупність окремих інформаційних кампаній або реакцій на події. В даному випадку йдеться більше про послідовну трансформацію інструментів впливу, що відбувається у тісному зв'язку зі зміною стратегічних цілей російської федерації, характеру воєнних дій, міжнародного контексту та внутрішнього стану цільових аудиторій. Як зазначає С.О. Лисенко у своїй праці, інформаційна складова сучасних конфліктів є керованим процесом, що інтегрується у загальну систему стратегічного управління державою і використовується для досягнення політичних і безпекових цілей.[102]

У цьому контексті пропаганда виступає не допоміжним елементом, а повноцінним інструментом ведення війни, здатним змінювати сприйняття реальності, впливати на політичні процеси та формувати поведінкові моделі як на внутрішньому, так і на зовнішньому рівнях.[103] Саме тому аналіз її еволюції дозволяє не лише реконструювати логіку інформаційного впливу, але й частково прогнозувати подальші дії держави-агресора.

Вдаючись до аналізу пропаганди рф в російсько-українській війні, першим етапом її еволюції можна визначити як підготовчо-гібридний, на якому ключовим завданням було формування когнітивного середовища, сприятливого для подальшої агресії. У цей період Україна системно зображувалася як нестабільна держава, неспроможна до самостійного розвитку (failed state), а її політичний

---

[102] Лисенко С.О. Стратегічне управління інформаційною безпекою держави : автореферат дисерт. на здобуття наук. ступ. д.н. з держ. упр. ; спец. 25.00.05 - державне управління у сфері державної безпеки та охорони громадського порядку. Житомирська політехніка. 2025. URL: https://ztu.edu.ua/site/files/1/docs/Університет/Спеціалізовані%20вчені%20ради/14.052.03/2025/ref_Лисенко_С.pdf . (дата звернення: 04.04.2026).

[103] Ліпкан В.А. Національна безпека України : навч. посібник . К. : Кондор, 2008, 552 с.

курс подавався як похідний від зовнішніх впливів (так зване «зовнішнє управління»). Як підкреслює А. Гольцов у своєму підручнику з геополітики та політичної географії, у геополітичному дискурсі делегітимізація суб'єктності держави є типовим інструментом підготовки до ревізії існуючого міжнародного порядку.[104]

Це означає, що пропаганда діяла не лише на рівні окремих повідомлень, а на рівні глибинних уявлень про політичну реальність. Вона поступово формувала рамку, в якій Україна переставала сприйматися як повноцінний суб'єкт міжнародних відносин. Як зазначено у праці Лісовського та Лісовської, подібні інформаційні впливи здатні підривати національну стійкість через трансформацію довіри до державних інституцій та зміни у сприйнятті загроз.[105]

Перехід до відкритої форми агресії супроводжувався зміною функції пропаганди. Якщо на попередньому етапі вона формувала передумови для сприйняття агресії, то тепер її завданням стало безпосередньо легітимізація насильства. Агресія почала подаватися як вимушена реакція, як захисний захід чи історична необхідність. Як зазначено у своєму дослідженні Канцір та Олійник, інформаційне забезпечення агресивних дій є ключовим фактором їхньої легітимації у політичному та правовому вимірах.[106]

Ключовим механізмом цього етапу стало зміщення причинно-наслідкових зв'язків. Тобто, у межах інформаційної війни стало важливим не стільки спотворити факти, а скільки змінити їх інтерпретацію. У результаті агресор перестає сприйматися як джерело загрози, а сам конфлікт подається як складний і неоднозначний процес, що не має чіткої відповідальності.

Після початку повномасштабного вторгнення пропаганда переходить у нову фазу, пов'язану з управлінням сприйняттям реальності в умовах затяжного

---

[104] Гольцов А.Г. Геополітика та політична географія : підручник. К. : ЦУЛ, 2021,416 с.
[105] Лісовський П.М. Безпекознавство: особистість, держава, суспільство : навч. посібник. К. : Кондор, 2017, 368 с.
[106] Канцір В, Олійник Х. Іноземний досвід регламентації кримінальної відповідальності за пропаганду, планування, підготовку, розв'язування та ведення агресивної війни. Вісник Національного університету "Львівська політехніка". 2020. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2020/may/21542/32.pdf (дата звернення: 04.04.2026)

конфлікту. Особливо важливим стає контроль над розривом між очікуваннями та реальними результатами. Якщо початково війна подавалася як швидка і контрольована, то з часом виникає необхідність пояснити її затягування, втрати та відсутність швидкого результату.

Як зазначає у своїй праці В. Станчишин, тривалий стрес і невизначеність формують стан емоційної нестабільності, що робить суспільство більш вразливим до інформаційного впливу.[107] У цьому контексті пропаганда починає виконувати функцію психологічної стабілізації, яка досягається через раціоналізацію втрат і перевизначення цілей війни.

Подальша еволюція пов’язана з переходом до стратегії виснаження. На цьому етапі пропаганда спрямована не стільки на переконання, скільки на зниження здатності аудиторій чинити спротив. Це досягається через постійне наголошення на втраті ресурсів, тривалості конфлікту та необхідності компромісів. У цифрову епоху інфодемія стає фактором політичної дестабілізації, оскільки перевантаження інформацією знижує здатність до критичного мислення.[108]

Окремої уваги заслуговує технологічна трансформація пропаганди. Сучасний етап характеризується переходом від централізованих інформаційних моделей до мережевих систем, де важливу роль відіграють алгоритми поширення контенту, соціальні мережі та цифрові платформи. В даному контексті цифрові ризики суттєво змінюють характер інформаційного впливу, перетворюючи його на складну систему взаємодії технологій і поведінкових моделей.[109] У результаті цього пропаганда перестає бути лише інструментом комунікації і стає елементом інформаційної інфраструктури.

---

[107] Станчишин В. Емоційні гойдалки війни : роздуми психотерапевта про війну. Вид. 2-ге, допов. Київ : Віхола, 2024, 309 с.

[108] Гаращук, Д., Сергєєв, В. Інфодемія та популізм у цифрову епоху: загрози політичній стабільності та безпекові виклики. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2025-2(8)-61-71 (дата звернення: 04.04.2026).

[109] Наторіна А.О. Синкретичність менеджменту цифрових ризиків та інформаційної безпеки. 27 листопада 2019. URL: https://ema.ztu.edu.ua/article/view/185089 (дата звернення 04.04.2026).

З огляду на вищесказане, можливо зробити проміжний висновок, що еволюція російської пропаганди демонструє її глибоку інтегрованість у систему ведення війни. Вона змінюється разом із цілями держави-агресора, адаптується до середовища та виконує різні функції залежно від етапу конфлікту. Це підтверджує, що пропаганда є не допоміжним, а являється ключовим інструментом гібридної війни, а її аналіз має важливе значення для розуміння логіки дій противника та розробки ефективних заходів протидії.

2.2. Ключові наративи російської пропаганди щодо України

Російська пропаганда у війні проти України реалізується не через окремі повідомлення, а через систему взаємопов'язаних наративів, які формують цілісну картину реальності для різних аудиторій. Як зазначено у підручнику Політологія під редакцією Л. Скрипникової, наративи у політичній комунікації виконують функцію рамок, через які аудиторія інтерпретує події та визначає їх значення.[110] Саме тому аналіз пропаганди без урахування її наративної структури є неповним, оскільки дозволяє побачити лише поверхневий рівень впливу.

Центральним наративом російської пропаганди є делегітимізація української державності, який пронизує всі інші інформаційні конструкції, що використовуються агресором. Його сутність полягає у системному підриві уявлення про Україну як самостійну політичну одиницю, здатну здійснювати незалежну внутрішню та зовнішню політику. Українська держава подається як нестабільна, внутрішньо розколота і залежна від зовнішніх сил. Такий підхід відповідає геополітичній логіці, у якій заперечення суб'єктності іншої держави є передумовою для легітимації втручання у її справи.[111] У безпековому контексті це означає, що підрив довіри до держави трансформується у підрив її стійкості[112],

---

[110] Скрипникова Л.В., Політологія: навчальний посібник. К.: Центр учбової літератури, 2014, 272 с. URL: https://dduvs.edu.ua/biblioteka/biblioteka-studenta-dduvs/pidruchniki-posibniki/politologiya/ (дата звернення: 04.04.2026).
[111] Гольцов А.Г. Геополітика та політична географія : підручник. К. : ЦУЛ, 2021, 416 с.
[112] Ліпкан В.А. Національна безпека України : навч. посібник . К. : Кондор, 2008, 552 с.

підкреслюючи залежність національної безпеки від рівня легітимності державних інститутів.

Паралельно формується наратив виправдання агресії, який функціонує як логічне продовження делегітимізації. Якщо держава зображується як неспроможна або «неправильна», то будь-яке втручання може бути представлене як необхідне. Агресія в такому випадку інтерпретується як захист, стабілізація або навіть позиціонується як гуманітарна місія. Як зазначено у праці Канціра та Олійника, пропаганда агресивної війни часто базується на перекручуванні правових категорій та зсуненні меж між агресією і самообороною. [113] Така риторика дозволяє формувати уявлення про війну як про вимушений крок, а не як про акт порушення міжнародного права.

Важливим елементом можливо також виділити наратив “зовнішнього управління”, який підсилює делегітимізацію України, позбавляючи її суб’єктності в очах своєї спільноти громадян. У межах цього наративу Україна подається як інструмент впливу та дій західних держав, що дозволяє росії перенести відповідальність за війну на зовнішніх дійових суб’єктів. У праці Носенка та Яковлєва щодо трансформації стримування, подібні інформаційні конструкції спрямовані на зміну сприйняття ролі України у міжнародній системі, що впливає на рівень її підтримки з боку держав-партнерів та їхнього суспільства.[114]

Особливе місце тут займає наратив деморалізації, спрямований на українське суспільство. Він базується на експлуатації емоційних станів – страху, тривоги, втоми та розчарування. Тривалий стрес у воєнних умовах призводить до емоційного виснаження, що знижує здатність до раціонального аналізу і

[113] Канцір В, Олійник Х. Іноземний досвід регламентації кримінальної відповідальності за пропаганду, планування, підготовку, розв’язування та ведення агресивної війни. Вісник Національного університету “Львівська політехніка”. 2020. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2020/may/21542/32.pdf (дата звернення: 05.04.2026)

[114] Носенко С., Яковлєв М., Трансформація стримування в контексті російсько-української війни: концептуалізація поняття крізь призму становлення України як середньої держави. Society and security. 2025. URL: https://sas.ztu.edu.ua/article/view/323957/314626 (дата звернення: 05.04.2026).

підвищує сприйнятливість до маніпуляцій.[115] Таким чином, пропаганда не лише інформує, а й активно впливає на психологічний стан, що має безпосередній вплив на поведінку.

Не менш важливим також можна виділити наратив поляризації, що спрямований на посилення внутрішніх суперечностей у суспільстві. Він використовує соціальні, політичні та культурні відмінності, підсилюючи конфлікти і знижуючи рівень соціальної згуртованості. Згідно дослідженням Гаращука і Сергєєва, у цифрову епоху інформаційні процеси можуть підсилювати політичну поляризацію, створюючи середовище нестабільності.[116] Це особливо небезпечно в умовах війни, коли згуртованість є одним із ключових факторів стійкості.

Окремим рядом є наративи, спрямовані на міжнародну аудиторію. Вони орієнтовані на формування сумнівів щодо доцільності підтримки України, акцентуючи увагу на економічних витратах, ризиках ескалації та тривалості конфлікту. У цьому випадку пропаганда працює не проти позиції як такої, а проти її довготривалого утримання, що є принципово важливим у контексті міжнародної політики.

Завершальним елементом системи є стратегія інформаційного шуму, яка полягає у створенні великої кількості взаємосуперечливих повідомлень. Так, у цифровому середовищі надлишок інформації знижує здатність до критичного аналізу, що робить аудиторію більш вразливою до маніпуляцій.[117] У результаті формується стан невизначеності, в якому істина втрачає всіляке значення.

З огляду наративів, що використовує росія у своїй пропаганді підтримки та виправдання збройної агресії проти нашої держави, можна зробити проміжний висновок, що система наративів російської пропаганди є складною і

---

[115] Станчишин В. Емоційні гойдалки війни : роздуми психотерапевта про війну. Вид. 2-ге, допов. Київ : Віхола, 2024, 309 с.
[116] Гаращук, Д., Сергєєв, В. Інфодемія та популізм у цифрову епоху: загрози політичній стабільності та безпекові виклики. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2025-2(8)-61-71 (дата звернення: 05.04.2026).
[117] Наторіна А.О. Синкретичність менеджменту цифрових ризиків та інформаційної безпеки. 27 листопада 2019. URL: https://ema.ztu.edu.ua/article/view/185089 (дата звернення 05.04.2026).

багаторівневою структурою, яка забезпечує досягнення стратегічних цілей через вплив на сприйняття реальності. Вона поєднує делегітимізацію, виправдання агресії, деморалізацію та поляризацію в єдину систему, що діє одночасно на різні аудиторії. Це дозволяє пропаганді не лише формувати уявлення, але й визначати поведінку об'єктів впливу, що робить її одним із ключових інструментів сучасної гібридної війни.

2.3. Інструменти та технології пропагандистського впливу. Канали та екосистеми поширення. Цільові аудиторії пропаганди рф

Інструментальний вимір російської пропаганди визначає її практичну ефективність, оскільки саме через конкретні технології відбувається реалізація наративів. Як зазначено у праці С.О. Лисенка, інформаційні операції у сучасних конфліктах характеризуються комплексністю та поєднанням різних методів впливу в єдину систему. [118]

Одним із базових інструментів пропаганди завжди є дезінформація, яка полягає у навмисному поширенні неправдивих або перекручених відомостей. Проте її ефективність визначається не самою неправдивістю, а здатністю інтегруватися у вже існуючі переконання аудиторії. Це означає, що дезінформація працює через резонанс із попередніми уявленнями, а не через їх повне заміщення.

Не менш важливим є маніпулятивний вплив, який часто використовує правдиві факти, але подає їх у викривленому контексті. Маніпуляція є більш ефективною, ніж пряма дезінформація, оскільки вона менш помітна і викликає менший рівень спротиву.

Особливе значення має інформаційно-психологічний вплив, спрямований на зміну емоційного стану аудиторії. У цьому випадку інформація

---

[118] Лисенко С.О. Стратегічне управління інформаційною безпекою держави : автореферат дисерт. на здобуття наук. ступ. д.н. з держ. упр. ; спец. 25.00.05 - державне управління у сфері державної безпеки та охорони громадського порядку. Житомирська політехніка. 2025. URL: https://ztu.edu.ua/site/files/1/docs/Університет/Спеціалізовані%20вчені%20ради/14.052.03/2025/ref_Лисенко_С.pdf . (дата звернення: 05.04.2026).

використовується не як джерело знань, а як тригер емоційних реакцій. Як зазначає у своїй праці В. Станчишин, у стані війни емоційна нестабільність значно підвищує ефективність таких впливів.[119]

Важливим сучасним інструментом є інфодемія, яка створює інформаційне перевантаження. У праці Гаращука та Сергєєва зазначається, що надлишок інформації призводить до когнітивного виснаження і зниження здатності до аналізу.[120] У такому середовищі пропаганда не переконує напряму, а створює умови, в яких будь-яка інформація втрачає довіру.

Цифрові технології відіграють ключову роль у сучасній пропаганді. Інформаційні технології стають інструментом забезпечення безпеки і водночас створюють нові загрози.[121] Алгоритмічне поширення контенту дозволяє масштабувати вплив і адаптувати його до конкретних аудиторій, що значно підвищує ефективність пропаганди.

З вищезазначеного можна припустити, що інструменти російської пропаганди формують комплексну систему впливу, яка охоплює когнітивний, емоційний та поведінковий рівні. Їхня ефективність забезпечується взаємодією та технологічною підтримкою, що перетворює пропаганду на інструмент управління соціальною реальністю.

Канали поширення російської пропаганди та їхня специфіка. Ефективність пропагандистського впливу визначається не лише змістом повідомлень, а й каналами їхнього поширення, оскільки саме канали формують швидкість, масштаб і характер сприйняття інформації. Як зазначається у роботі С. Лисенка, контроль інформаційних потоків є одним із ключових елементів

---

[119] Станчишин В. Емоційні гойдалки війни : роздуми психотерапевта про війну. Вид. 2-ге, допов. Київ : Віхола, 2024, 309 с.

[120] Гаращук, Д., Сергєєв, В. Інфодемія та популізм у цифрову епоху: загрози політичній стабільності та безпекові виклики. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2025-2(8)-61-71 (дата звернення: 07.04.2026).

[121] Сумін, П. Інформаційні технології як інструмент забезпечення національної безпеки на сучасному етапі розвитку: проблеми та перспективи. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2024-6(6)-37-43 (дата звернення: 07.04.2026).

забезпечення інформаційної безпеки, оскільки він дозволяє не лише поширювати повідомлення, а й визначати структуру інформаційного середовища.[122]

У сучасних умовах російська пропаганда функціонує через багаторівневу систему каналів, яка поєднує традиційні медіа, цифрові платформи та альтернативні інтернет-мережі. Така система дозволяє забезпечити одночасний вплив на різні аудиторії, використовуючи як офіційні, так і неформальні джерела інформації.

Традиційні медіа залишаються важливим інструментом формування базових наративів, оскільки вони забезпечують офіційне оформлення інформаційної позиції держави. Саме через традиційні медіа відбувається формування політичної картини світу, яка сприймається як «офіційна реальність».[123] У російській практиці це означає централізоване поширення ключових наративів, які потім масштабуються через інші канали.

Водночас, вирішальну роль у сучасній пропаганді відіграють цифрові платформи, які забезпечують швидкість поширення інформації та можливість її адаптації до різних аудиторій. Так, інформаційні технології значно розширюють можливості впливу, дозволяючи поєднувати масовість і персоналізацію[124]. Вони створюють умови, в яких пропаганда може одночасно діяти як на широкі маси, так і на окремі соціальні групи.

Особливе місце у системі каналів займають соціальні мережі, які забезпечують ефект віральності та створюють ілюзію спонтанності інформаційних процесів. За даними компанії Meta[125], у 2023 році було видалено десятки координаційних мереж, пов’язаних з російськими інформаційними

---

[122] Лисенко С.О. Стратегічне управління інформаційною безпекою держави : автореферат дисерт. на здобуття наук. ступ. д.н. з держ. упр. ; спец. 25.00.05 - державне управління у сфері державної безпеки та охорони громадського порядку. Житомирська політехніка. 2025. URL: https://ztu.edu.ua/site/files/1/docs/Університет/Спеціалізовані%20вчені%20ради/14.052.03/2025/ref_Лисенко_С.pdf . (дата звернення: 08.04.2026).

[123] Гольцов А.Г. Геополітика та політична географія : підручник / А. Г. Гольцов. – К. : ЦУЛ, 2021. – 416 с. (дата звернення: 08.04.2026).

[124] Сумін, П. Інформаційні технології як інструмент забезпечення національної безпеки на сучасному етапі розвитку: проблеми та перспективи. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2024-6(6)-37-43 (дата звернення: 08.04.2026).

[125] Nimmo B., Torrey M. Adversarial Threat Report. Meta Quarterly Adversarial Threat Report Q2 2023. 2023. URL: https://transparency.meta.com/sr/Q2-2023-Adversarial-threat-report/ (дата звернення: 09.04.2025).

операціями, які охоплювали мільйони користувачів, що свідчить про масштаб і організованість такого впливу. У цьому контексті соціальні мережі виступають не лише каналом поширення інформації, а й середовищем, яке саме підсилює її вплив через алгоритмічні механізми.

Окрему роль відіграє платформа Telegram, яка стала одним із ключових інструментів поширення пропаганди у війні проти України. За даними Digital Forensic Research Lab[126], саме Telegram активно використовується для поширення проросійських наративів через канали, які маскуються під незалежні джерела інформації та соціальні медіа. Високий рівень довіри до таких каналів пояснюється їхньою неформальністю та відсутністю жорсткої модерації, що створює ілюзію «альтернативної правди» та «інсайдів».

Крім того, важливим елементом є використання проксі-ресурсів, які дозволяють поширювати пропаганду без прямої асоціації з державою. Подібні ресурси підвищують довіру до інформації, оскільки сприймаються як незалежні джерела, про що вказується у сучасних посібниках та пам’ятках. У результаті формується багаторівнева система поширення, у якій складно визначити первинне джерело інформації та верифікувати його.

У міжнародному інформаційному просторі російська пропаганда використовує глобальні інформаційні платформи для впливу на громадську думку в інших країнах. Як зазначають Носенко та Яковлєв, інформаційний вплив є важливою складовою міжнародного протистояння, оскільки дозволяє змінювати політичні позиції держав.[127] Це особливо важливо у контексті підтримки України, оскільки пропаганда спрямована на її зниження.

Отже, канали поширення російської пропаганди формують складну інфраструктуру інформаційного впливу, яка забезпечує її ефективність.

---

[126] Buziashvili E., Châtelet V.. Another battlefield: Telegram as a digital front in Russia’s war against Ukraine. ISBN-13: 978-1-61977-335-6. 2024. URL: https://dfrlab.org/wp-content/uploads/sites/3/2024/06/DFRLab_Russian_Telegram_2024.pdf (дата звернення: 08.04.2026).

[127] Носенко С., Яковлєв М., Трансформація стримування в контексті російсько-української війни: концептуалізація поняття крізь призму становлення України як середньої держави. Society and security. 2025. URL: https://sas.ztu.edu.ua/article/view/323957/314626 (дата звернення: 05.04.2026).

Поєднання традиційних і цифрових медіа дозволяє одночасно формувати базові наративи та масштабувати їх через різні середовища. Особливу роль відіграють соціальні мережі та альтернативні платформи, які створюють ілюзію незалежності та підсилюють довіру до інформації. У результаті формується цілісна система, здатна впливати на різні аудиторії та адаптуватися до змін інформаційного середовища.

Цільові аудиторії російської пропаганди

Ефективність пропагандистського впливу значною мірою залежить від точності визначення цільових аудиторій, оскільки різні соціальні групи мають відмінні інформаційні потреби, рівень критичного мислення та психологічні особливості. У своїй роботі В. Ліпкан зазначає, національна безпека держави значною мірою залежить від стану її суспільства, що включає рівень довіри, згуртованість і здатність протидіяти інформаційним впливам.[128]

Внутрішня аудиторія росії є ключовою з точки зору легітимації війни. Пропаганда у цьому випадку спрямована на формування підтримки дій влади та створення образу справедливої війни. Це досягається через поєднання наративів загрози, історичної місії та необхідності захисту. Такий підхід дозволяє забезпечити стабільність політичного режиму навіть у умовах тривалого конфлікту.

Українська аудиторія розглядається як об’єкт деморалізації та дестабілізації. Пропаганда активно використовує емоційні фактори, такі як страх, втома і розчарування. Водночас, тривалий стрес знижує здатність до критичного мислення, що робить аудиторію більш вразливою до маніпуляцій та інформаційних вкидів.[129] У цьому випадку пропаганда спрямована не на переконання, а на зниження стійкості населення в умовах повномасштабного вторгнення.

---

[128] Ліпкан В.А. Національна безпека України : навч. посібник . К. : Кондор, 2008, 552 с..

[129] Станчишин В. Емоційні гойдалки війни : роздуми психотерапевта про війну / Володимир Станчишин. – Вид. 2-ге, допов. – Київ : Віхола, 2024. – 309 с.

Міжнародна аудиторія є окремим об’єктом впливу, оскільки від її позиції залежить рівень підтримки України. За даними European Council on Foreign Relations[130], у низці європейських країн ще з 2022 року спостерігається зростання підтримки переговорів як альтернативи військовій допомозі, що частково пов’язано з інформаційним впливом. Все це свідчить про ефективність пропаганди у формуванні довготривалих політичних тенденцій.

Сегментація аудиторій дозволяє російській пропаганді досягати високого рівня ефективності, оскільки вона враховує специфіку різних соціальних груп. Вплив на внутрішню аудиторію забезпечує стабільність режиму, на українську – спрямований на деморалізацію, а на міжнародну – на зміну політичних позицій. Такий підхід підтверджує стратегічний характер пропаганди як інструменту впливу на різні рівні соціальної та політичної системи.

2.4. Безпекові наслідки російської пропаганди

Російська пропаганда має безпосередній вплив на національну безпеку України, оскільки вона впливає не лише на інформаційне середовище, а й на політичні, соціальні та психологічні процеси. Згідно з працею В. Ліпкана, інформаційна безпека є складовою загальної системи національної безпеки і визначає здатність держави протидіяти зовнішнім впливам.[131]

Одним із ключових наслідків є підрив довіри до державних інституцій, що створює умови для внутрішньої дестабілізації. Крім того, пропаганда впливає на соціальну згуртованість, посилюючи конфлікти та поляризацію. В такому контексті інформаційні процеси можуть бути одним із факторів політичної нестабільності.[132]

---

[130] Krastev I., Leonard M. Peace versus Justice: The coming European split over the war in Ukraine. 2022. URL: https://ecfr.eu/publication/peace-versus-justice-the-coming-european-split-over-the-war-in-ukraine/ (дата звернення: 08.04.2026).

[131] Ліпкан В.А. Національна безпека України : навч. посібник . К. : Кондор, 2008, 552 с..

[132] Гаращук, Д., Сергєєв, В. Інфодемія та популізм у цифрову епоху: загрози політичній стабільності та безпекові виклики. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2025-2(8)-61-71 (дата звернення: 08.04.2026).

Психологічний вплив також є критично важливим, оскільки він безпосередньо визначає поведінку населення, а емоційний стан суспільства впливає на його здатність до опору.[133]

У міжнародному вимірі пропаганда спрямована на зниження підтримки України. За даними Pew Research Center, рівень підтримки України у світі варіюється залежно від інформаційного середовища, що підтверджує вплив пропаганди.

Кейс-аналіз дозволяє розглянути російську пропаганду як практичний процес реалізації інформаційного впливу, де інформаційно-психологічні операції включають етапи формування наративу, його поширення, впливу на аудиторію та досягнення результату.

Показовим прикладом є інформаційна кампанія щодо подій у м. Буча, Київська область, Україна, де після оприлюднення фактів масових вбивств цивільного населення було запущено наратив про «постановку київського режиму». За даними Human Rights Watch[134], задокументовано численні випадки воєнних злочинів, що спростовує пропагандистські твердження.

Іншим прикладом є кампанія щодо «біолабораторій»[135], яка активно поширювалася у міжнародному середовищі. Як зазначено у звітах United Nations, такі твердження не мають фактичного підтвердження.

У випадку зернової угоди пропаганда використовувала маніпуляцію статистикою, стверджуючи, що українське зерно постачається лише до багатих країн, хоча дані United Nations свідчать про значні обсяги експорту до країн, що розвиваються.

Даний кейс-аналіз демонструє, що російська пропаганда функціонує як керована система, яка включає чіткі етапи реалізації. Вона використовує різні

---

[133] Станчишин В. Емоційні гойдалки війни : роздуми психотерапевта про війну. Вид. 2-ге, допов. Київ : Віхола, 2024, 309 с.
[134] Report. Ukraine: Russian Forces' Trail of Death in Bucha. 2022. URL:https://www.hrw.org/news/2022/04/21/ukraine-russian-forces-trail-death-bucha (дата звернення: 10.04.2026).
[135] United Nations Not Aware of Any Biological Weapons Programmes, Disarmament Chief Affirms as Security Council Meets to Address Related Concerns in Ukraine. SC/14827. 2022. URL: https://press.un.org/en/2022/sc14827.doc.htm (дата звернення: 10.04.2026).

інструменти та канали для досягнення конкретних цілей, що підтверджує її системний характер. Аналіз практичних прикладів дозволяє глибше зрозуміти механізми інформаційного впливу та визначити можливі шляхи протидії.

Отже, з вищенаведеного можна винести проміжні висновки про те, що безпекові наслідки російської пропаганди мають комплексний характер і охоплюють всі рівні функціонування держави. Вона впливає на довіру, стабільність, психологічний стан і міжнародну підтримку, що робить її одним із ключових інструментів гібридної війни. Це підтверджує необхідність системної протидії інформаційним загрозам.

Висновки до Розділу 2

У даному розділі було здійснено системний аналіз російської пропаганди у війні проти України через розгляд її еволюції, ключових наративів, інструментів, каналів поширення, цільових аудиторій та безпекових наслідків. У межах розділу доведено, що російська пропаганда не є випадковим набором інформаційних вкидів або окремих дезінформаційних кампаній. Вона функціонує як цілісна система інформаційно-психологічного впливу, інтегрована у загальну стратегію ведення війни проти України. Було показано, що еволюція російської пропаганди безпосередньо пов’язана зі зміною етапів російсько-української війни. На початкових етапах особливе значення мали підготовчі наративи, спрямовані на делегітимізацію української державності, формування образу України як «неспроможної держави» та заперечення її суб’єктності. У подальшому ці наративи були використані для виправдання агресії, окупації частини територій та спроби представити насильницькі дії російської федерації як нібито вимушені або такі, що носять виключно оборонний характер. Після початку повномасштабного вторгнення пропагандистська система адаптувалася до умов затяжної війни, змістивши акценти на деморалізацію українського суспільства, розпалювання внутрішніх конфліктів, нав’язування втоми від війни та зниження довіри до інституцій.

Окремо було встановлено, що ключові наративи російської пропаганди мають взаємопов’язаний характер. Делегітимізація української державності, наратив наявності «зовнішнього управління», виправдання агресії, демонізація української влади та Сил Оборони України, деморалізація населення, поляризація суспільства та дискредитація міжнародної підтримки України діють не ізольовано, а як елементи єдиної наративної системи пропаганди росії. Обґрунтовано, що ефективність російської пропаганди значною мірою забезпечується поєднанням традиційних і цифрових каналів поширення, такі як державні медіа, проксі-ресурси, соціальні мережі, анонімні Telegram-канали, ботоферми, псевдоекспертні майданчики та алгоритмічне просування контенту, утворюючи розгалужену екосистему впливу на різні цільову аудиторії, як внутрішні, так і зовнішні.

У рамках розділу було доведено, що російська пропаганда є одним із ключових інструментів гібридної війни проти України. Її небезпека полягає не лише в поширенні неправдивої інформації, а у здатності впливати на довіру, політичну стабільність, соціальну згуртованість, психологічну стійкість і міжнародну підтримку України. Саме тому протидія російській пропаганді потребує не ситуативного спростування окремих фейків, а системного аналізу її наративів, каналів, аудиторій і наслідків.

РОЗДІЛ 3. КОНТРПРОПАГАНДА УКРАЇНИ ТА ПАРТНЕРІВ. ПІДХОДИ, ІНСТРУМЕНТИ, ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ, РЕКОМЕНДАЦІЇ

3.1. Українська інституційна архітектура контрзаходів. Політики, документи, ролі суб'єктів, координація, інформаційна гігієна держави

Українська інституційна архітектура протидії пропаганді сформувалася як відповідь на тривалу, системну й багаторівневу інформаційну агресію російської федерації. Її особливість полягає в тому, що вона не була створена в умовах спокійного адміністративного планування, а розбудовувалася паралельно з ескалацією війни у режимі постійного реагування на нові загрози. Саме тому українська модель поєднує стратегічні документи, державні органи, безпекові інституції, медійні платформи, громадські ініціативи та міжнародну підтримку.

У цьому сенсі контрпропаганда в Україні є не окремою комунікаційною практикою, а частиною ширшої системи національної безпеки, де інформаційна сфера розглядається як простір прямого протиборства. Стратегія інформаційної безпеки України прямо визначає актуальні виклики та загрози національній безпеці в інформаційній сфері, а також цілі й завдання щодо протидії таким загрозам.[136]

У попередніх розділах нами було показано, що російська пропаганда функціонує як цілісна система впливу, яка поєднує наративи, канали, інструменти та цільові аудиторії. Відповідно до цього, інституційна відповідь України не може зводитися до ситуативних спростувань окремих фейків. Вона має охоплювати стратегічне планування, аналітичний моніторинг, кризові комунікації, роботу з платформами, міжнародну взаємодію, медіаграмотність і правове регулювання. Як зазначає у своїй роботі С.О. Лисенко[137], інформаційна

---

[136] Указ Президента України № 685/2021, Про рішення Ради національної безпеки і оборони України "Про Стратегію інформаційної безпеки", 2021. URL: https://zakon.rada.gov.ua/laws/main/685/2021 (дата звернення: 21.04.2026).

[137] Лисенко С.О. Стратегічне управління інформаційною безпекою держави : автореферат дисерт. на здобуття наук. ступ. д.н. з держ. упр. ; спец. 25.00.05 - державне управління у сфері державної безпеки та охорони

безпека держави потребує стратегічного управління, що має мати за мету узгодження цілей, ресурсів, інструментів і суб'єктів у єдиній логіці. Саме ця теза є методологічно важливою для розуміння української моделі, де протидія пропаганді має працювати не як набір окремих реакцій, а як система взаємопов'язаних контрзаходів.

На нормативному рівні базовим документом є Стратегія інформаційної безпеки України, затверджена Указом Президента № 685/2021.[138] Вона визначає інформаційну безпеку як складову національної безпеки і фіксує необхідність протидії дезінформації, інформаційним операціям та іншим формам ворожого впливу. Особливо важливо те, що цей документ закладає не лише оборонну, а й правозахисну логіку. В ньому йдеться не тільки про захист держави від інформаційних атак, а й про захист прав людини на інформацію, захист персональних даних і формування стійкого інформаційного середовища. Такий підхід є принциповим, оскільки дозволяє поєднати безпекову необхідність із демократичними обмеженнями. Це прямо перегукується з нашими висновками, наведеними у розділі 1, де контрпропаганда розглядалася як легітимна лише за умови, де вона не перетворюється на внутрішню маніпуляцію.

Інституційна архітектура української протидії пропаганді має кілька рівнів. Перший рівень - стратегічно-політичний, пов'язаний із формуванням державної політики, визначенням загроз, ухваленням стратегічних документів і встановленням рамок міжвідомчої координації.

Другим рівнем є аналітично-комунікаційний, де здійснюється моніторинг дезінформації, аналіз наративів противника, підготовка спростувань і формування контрнаративів.

Третій рівень - це оперативний, який охоплює кризові комунікації, реагування на конкретні інформаційні атаки, роботу з медіа й платформами.

громадського порядку. Житомирська політехніка. 2025. URL: https://ztu.edu.ua/site/files/1/docs/Університет/Спеціалізовані%20вчені%20ради/14.052.03/2025/ref_Лисенко_С.pdf . (дата звернення: 21.04.2026).

[138] Указ Президента України № 685/2021, Про рішення Ради національної безпеки і оборони України "Про Стратегію інформаційної безпеки", 2021. URL: https://zakon.rada.gov.ua/laws/main/685/2021 (дата звернення: 21.04.2026).

Четвертим рівнем іде суспільний, пов’язаний із медіаграмотністю населення, культурою громадського фактчекінгу, незалежними медіа та залученням громадянського суспільства до контрпропаганди через соціальні мережі. Така багаторівнева структура має перевагу в гнучкості, але водночас створює ризик фрагментації, де різні суб’єкти можуть діяти ефективно у своїй сфері, але без достатньої координації загальний ефект буде слабшим.

У межах цієї системи важливу роль відіграє Центр протидії дезінформації при РНБО України. Його офіційна місія пов’язана із захистом від інформаційного тероризму та протидією дезінформації.[139] Важливість Центру полягає не лише у публічному спростуванні фейків, а й у формуванні аналітичної рамки для розуміння інформаційних загроз. Це важливо, оскільки дезінформація рф часто працює не як окремий фейк, а як частина довшого наративного ланцюга або інформаційно-психологічній спеціальній операції. Як приклад можна навести, повідомлення про «втому Заходу», «зовнішнє управління Україною» або «неминучість переговорів на умовах росії», що можуть з’являтися у різних формах, але виконувати одну й ту саму функцію, а саме послаблювати стійкість українського суспільства та міжнародну підтримку нашої держави. Тому завдання аналітичної інституції полягає не тільки в тому, щоб зафіксувати неправдиве твердження, а й у тому, щоб визначити, до якого наративу воно належить, на яку аудиторію спрямоване і який безпековий ефект має створити.

Окремим елементом інституційної архітектури є Центр стратегічних комунікацій та інформаційної безпеки, який працює у сфері комунікаційної протидії зовнішнім загрозам, зокрема інформаційним атакам російської федерації.[140] Його портал SPRAVDI.ORG (Додаток Б) розміщує власні матеріали, антифейки, аналітику, дослідження, моніторинг та навчальні.[141] Якщо Центр протидії дезінформації більше асоціюється з безпековим профілем РНБО, то

---

[139] Веб-сайт Центру протидії дезінформації при РНБО України. 2026. URL: https://cpd.gov.ua/category/events/# (дата звернення: 21.04.2026).
[140] Веб-сайт Центру стратегічних комунікацій та інформаційної безпеки. 2026. URL: https://spravdi.org/ (дата звернення: 21.04.2026).
[141] Веб-сайт Центру стратегічних комунікацій та інформаційної безпеки. Розділ «Антифейк». 2026. URL: https://spravdi.org/sprostuvannya-fejkiv/ (дата звернення: 21.04.2026).

Центр стратегічних комунікацій посідає проміжне місце між державною комунікацією, аналітикою, публічною просвітою та медійним реагуванням. Такий розподіл функцій вважається корисним, бо дозволяє не концентрувати весь інструментарій в одному органі протидії чи управління. Водночас він підвищує вимоги до координації, щоб різні інституції не дублювали повноваження одна одної та не створювали розбіжностей у повідомленнях\комунікації.

Саме координація є одним із ключових викликів української системи пропаганди та контрпропаганди. У сфері контрпропаганди недостатньо, щоб кожен суб'єкт робив лише свою частину роботи. Необхідно, аби ці частини складалися в єдину комунікаційну або наративну логіку. Якщо один орган говорить мовою безпекових загроз, інший - мовою публічної комунікації, а третій - мовою політичних заяв, а четвертий оперує мовою технічної модерації, то аудиторія може отримати фрагментовану, неконсистентну або викривлену картину. Російська пропаганда активно використовує саме такі розриви, де будь-яка неузгодженість між інституціями може подаватися як «хаос», «некомпетентність», «приховування правди» або «боротьба внутрішніх владних груп». Саме тому українська інституційна архітектура потребує не лише формальних каналів взаємодії, а й спільної мови опису загроз.

Тут варто було б повернутися до логіки розділу 1, де контрпропаганда визначалася як система контрзаходів, спрямованих на нейтралізацію ворожого інформаційного впливу й посилення національної стійкості[142]. Тобто, якщо прийняти це визначення, то інституційна архітектура має будуватися не навколо окремого фейку, а безпосередньо навколо циклу управління загрозою. Такий цикл включає виявлення інформаційної атаки, класифікацію її наративу, оцінку цільової аудиторії, визначення ймовірної шкоди, підготовку контрповідомлення, вибір каналів реагування, моніторинг ефекту й корекцію подальших дій. Саме так контрпропаганда переходить від режиму реакції до режиму управління.

---

[142] Лісовський П.М. Безпекознавство: особистість, держава, суспільство : навч. посібник. К. : Кондор, 2017, 368 с.

Роль силового й безпекового сектору в цій системі полягає не лише в блокуванні каналів або викритті мереж ворожого впливу. Вона також включає аналітичне розуміння інформаційно-психологічних спеціальних операцій. Під цим мається на увазі, що протидія ІПСО потребує комплексного підходу, який поєднує аналіз джерел, змісту, каналів поширення і психологічних. Це особливо важливо для України, оскільки російська пропаганда часто поєднує інформаційний, кібернетичний і психологічний компоненти. Наприклад, кібератака на державний ресурс може супроводжуватися інформаційним вкидом про «некерованість держави», «дезорганізацію та хаос у владі», а військовий удар по цивільній інфраструктурі супроводжується хвилею повідомлень про «безсилля влади», «дефіцит засобів ППО» або «неминучість капітуляції». Тому відповідь має бути міжсекторальною, тобто де технічна ліквідація наслідків атаки повинна супроводжуватися швидкою, зрозумілою і психологічно грамотною комунікацією.

Важливим інституційним компонентом є державна інформаційна гігієна. У вузькому сенсі її можна розуміти як здатність держави не продукувати інформаційний хаос власними діями. Це означає, що державні органи мають уникати неперевірених заяв, суперечливих повідомлень, надмірної емоційності, непродуманої публікації чутливої інформації та комунікації, яка створює простір для маніпуляцій. У широкому сенсі інформаційна гігієна означає формування таких правил, практик і звичок, які зменшують сприйнятливість суспільства до дезінформації. Як зазначає Сумін у своїй праці, інформаційні технології можуть бути як інструментом забезпечення національної безпеки, так і джерелом нових ризиків.[143] Саме тому інформаційна гігієна не є лише освітньою темою, а частиною системи управління ризиками.

Окремим питанням постає баланс між державним регулюванням і демократичною легітимністю. Контрпропаганда в умовах війни не може бути

[143] Сумін, П. Інформаційні технології як інструмент забезпечення національної безпеки на сучасному етапі розвитку: проблеми та перспективи. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2024-6(6)-37-43 (дата звернення: 21.04.2026).

повністю «м’якою», адже очевидно, частина загроз потребує обмежувальних правових або технічних рішень. Водночас надмірно жорстке втручання в інформаційний простір може створити протилежний ефект через зниження довіри населення до держави. Саме тому принцип легітимності, сформульований у першому розділі, має практичне значення для інституційної архітектури. Держава повинна не тільки боротися з дезінформацією, а й пояснювати логіку своїх дій. Якщо обмежується доступ до певного ресурсу, спростовується певний наратив, вводяться інформаційні застереження, то суспільство має розуміти підстави таких дій, інакше будь-який контрзахід може бути перевизначений противником як «цензура», «приховування правди», «політичний контроль» або «авторитаризм».

Важливо, що українська система не може бути копією західних моделей. У ЄС і НАТО багато механізмів протидії дезінформації формувалися в умовах стабільних інституцій і відносно низької інтенсивності прямої воєнної загрози. Україна ж працює в умовах повномасштабної війни. Це суттєво скорочує часовий горизонт реагування, ризики є значно вищими, а наслідки помилок можуть бути безпосередньо пов’язані з життям людей. Саме тому українська інституційна архітектура має поєднувати західні принципи прозорості, підзвітності й доказовості з воєнною швидкістю реагування через характер сучасної війни.

Роль громадянського суспільства в Україні є однією з переваг цієї моделі. Незалежні медіа, OSINT-спільноти, фактчекінгові організації, волонтерські ініціативи та експертні середовища часто реагують та діють швидше за державні структури. Вони можуть першими помічати фейки, картографувати мережі поширення, пояснювати аудиторії маніпуляції та передавати інформацію далі. Це створює ефект «розподіленої стійкості», де протидія пропаганді не залежить від одного центру чи органу влади. Але цей самий фактор створює ризик неузгодженості дій і, як наслідок, послаблення ефекту, про що ми говорили вище. Якщо громадський сектор і держава діють у різних логіках процесів та комунікацій, це може зменшувати загальний ефект від протидії, а то і зовсім

нівелювати його у довгостроковій перспективі. Тому оптимальною є модель партнерства, де держава не поглинає громадянське суспільство та волонтерські ініціативи, а системно взаємодіє з ними.

До сильних сторін української інституційної архітектури можна віднести високу адаптивність, реальний досвід протидії російським операціям впливу, активність громадянського суспільства, наявність спеціалізованих інституцій та широку міжнародну підтримку. Слабкими ж сторонами можна визначити нерівномірність координації, залежність від персонального чинника, фрагментарність стратегічного планування, обмеженість ресурсів, ризик реактивності та вразливість до внутрішньої політичної поляризації. У межах даної кваліфікаційної роботи важливо не ідеалізувати українську модель, а показати її як живу, складну й таку, що розвивається під тиском війни.

Отже можна зробити проміжний висновок, що українська інституційна архітектура контрзаходів має мережевий, адаптивний і багаторівневий характер. Її головна перевага полягає у здатності швидко реагувати та залучати широкий спектр суб'єктів, а головна проблема полягає у потребі більшої стратегічної узгодженості. Подальший розвиток має бути спрямований на створення стабільного циклу управління інформаційними загрозами, від моніторингу й аналізу до реагування, оцінювання ефективності та превентивних дій. Саме така модель дозволить перейти від ситуативного реагування до системної контрпропаганди як повноцінного елементу національної безпеки.

3.2. Інструменти контрпропаганди. Стратегічні наративи, фактчекінг, кризові комунікації, робота з платформами, медіаграмотність, взаємодія з громадянським суспільством

Інструментальний рівень контрпропаганди визначає практичну спроможність держави не лише реагувати на окремі інформаційні атаки, а й формувати стійке інформаційне середовище, у якому ворожі наративи втрачають частину своєї ефективності. У попередньому розділі було показано, що російська

пропаганда діє як багаторівнева система, тобто вона поєднує стратегічні наративи, дезінформацію, маніпуляцію, інформаційно-психологічний вплив, цифрові платформи та роботу з різними аудиторіями. Через це контрпропаганда не може бути зведена до окремого факту спростування. Вона має бути симетрично складною, але не дзеркальною за методами: тобто поєднувати швидкість, доказовість, легітимність, психологічну чутливість і стратегічну послідовність.

У цьому сенсі контрпропаганда є не «спростуванням» у вузькому розумінні, а системою комунікаційних, аналітичних, освітніх, технологічних і координаційних інструментів. Її завдання полягає не лише у тому, щоб довести хибність ворожого повідомлення, а в тому, щоб зменшити його шкоду, не допустити закріплення маніпулятивної рамки і посилити здатність аудиторії самостійно розпізнавати подібні впливи в майбутньому. Саме така логіка відповідає підходу, запропонований С.О. Лисенком, який розглядає інформаційну безпеку як сферу стратегічного управління, де важливими є не лише окремі заходи, а їхня інтеграція в єдину систему.[144]

Першим та базовим інструментом контрпропаганди є стратегічні наративи. Вони виконують роль смислового каркасу, через який суспільство, партнери та зовнішні аудиторії інтерпретують події. Якщо російська пропаганда намагається нав’язати рамки «зовнішнього управління», «втоми населення\партнерів від війни», «безперспективності опору» або «неминучості компромісу», то українська контрпропаганда має формувати альтернативну рамку, у якій Україна постає суб’єктом, що захищає власну незалежність, міжнародне право і ширшу європейську безпеку. Така рамка не має бути лише риторикою. Вона має виконувати мобілізаційну, пояснювальну і легітимаційну функції. Тобто, можна

[144] Лисенко С.О. Стратегічне управління інформаційною безпекою держави : автореферат дисерт. на здобуття наук. ступ. д.н. з держ. упр. ; спец. 25.00.05 - державне управління у сфері державної безпеки та охорони громадського порядку. Житомирська політехніка. 2025. URL: https://ztu.edu.ua/site/files/1/docs/Університет/Спеціалізовані%20вчені%20ради/14.052.03/2025/ref_Лисенко_С.pdf . (дата звернення: 22.04.2026).

стверджувати, що політична комунікація має працювати через смислові конструкції, які задають спосіб сприйняття політичної реальності.[145]

Особливість стратегічного наративу полягає в тому, що він не може бути ефективним, якщо суперечить практиці та дійсності. Якщо держава говорить про відкритість, але комунікує закрито і суперечливо, то наратив, відповідно, втрачає свою переконливість. Якщо держава говорить про суб'єктність, але її комунікація виглядає залежною або реактивною, це послаблює контрпропагандиський ефект або і зовсім може нівелювати його. Тому стратегічний наратив має спиратися на реальні дії, інституційну послідовність і зрозумілу логіку пояснення. У цьому полягає принципова різниця між пропагандою авторитарного типу і демократичною контрпропагандою, де перша може тривалий час функціонувати через примус, ізоляцію та брехню, тоді як друга тримається на довірі, доказовості та повторюваній відповідності між словами і діями.

Другим інструментом є фактчекінг. Його значення полягає у встановленні фактичної істини там, де пропаганда намагається створити сумнів або альтернативну реальність. Український досвід показує, що фактчекінг є особливо важливим у випадках, коли ворог просуває конкретні фейки про нібито «біолабораторії США та НАТО», про «постановочність» воєнних злочинів у Бучі та Ірпені, Херсоні та Маріуполі, про «масову втому партнерів» або «нелегітимність української влади». Однак сам по собі фактчекінг не є достатнім. Його слабкість полягає у часовій асиметрії, де фейк поширюється швидше, ніж спростування, а перше емоційне враження часто закріплюється сильніше, ніж подальше раціональне пояснення. Це означає, що фактчекінг має бути вбудований у ширшу систему превенції, дебанкінгу (debunking) і пребанкінгу (prebunking).

Цінність такого підходу полягає не тільки у спростуванні конкретних повідомлень, а також в накопиченні масиву випадків, який дозволяє бачити та

---

[145] Скрипникова Л.В., Політологія: навчальний посібник. К.: Центр учбової літератури, 2014, 272 с. URL: https://dduvs.edu.ua/biblioteka/biblioteka-studenta-dduvs/pidruchniki-posibniki/politologiya/ (дата звернення: 22.04.2026).

класифікувати повторювані наративи. Це важливо для нашої держави, оскільки російська інформаційна політика рідко вигадує повністю нові смислові конструкції. Частіше вона повертає старі наративи в оновленій формі, як от «Україна керована Заходом», «українська влада нелегітимна», «Європа втомилася від підтримки України», «Україна становить загрозу росії та російськомовному населенню», «росія лише обороняється» та інші. Отже, фактчекінг має працювати не лише на рівні «правда/неправда», а й на рівні виявлення повторюваної структури впливу.

Дебанкінгом (debunking), як третім методом, визначається процес зменшення впливу дезінформації шляхом її спростування та пояснення механізмів маніпуляції, що лежать в її основі.[146] У практиці стратегічних комунікацій ЄС і НАТО дебанкінг розглядається як елемент реагування на інформаційні загрози, спрямований на викриття та корекцію неправдивих наративів. Веб-портал EUvsDisinfo.EU (Додаток В) є прикладом інституціалізованого підходу до документування й спростування прокремлівської дезінформації, а саме база EUvsDisinfo описує себе як відкритий пошуковий репозиторій прикладів прокремлівської дезінформації, який оновлюється щотижня.[147]

Ефективність дебанкінга залежить від кількох факторів. По-перше, від швидкості, де чим раніше з’являється пояснення, тим менше часу має фейк для закріплення. По-друге, від доступності, де спростування має бути зрозумілим не лише експертам, а й широкій аудиторії. По-третє, від каналу поширення, тобто, якщо фейк поширився в Telegram, спростування тільки на офіційному сайті може не досягти потрібної аудиторії. По-четверте, від форми спростування, де сухе заперечення часто менш ефективне, ніж пояснення механізму маніпуляції. Саме

[146] Lewandowsky, S., Cook, J., Ecker, U. K. H., Albarracín, D., Amazeen, M. A., Kendeou, P., Lombardi, D., Newman, E. J., Pennycook, G., Porter, E. Rand, D. G., Rapp, D. N., Reifler, J., Roozenbeek, J., Schmid, P., Seifert, C. M., Sinatra, G. M., Swire-Thompson, B., van der Linden, S., Vraga, E. K., Wood, T. J., Zaragoza, M. S. (2020). The Debunking Handbook 2020, 19 pages, PDF. 2020. URL: https://skepticalscience.com/docs/DebunkingHandbook2020-Ukranian.pdf (дата звернення: 22.04.2026).

[147] Веб-портал EUvsDisInfo. 2026. URL: https://euvsdisinfo.eu/disinformation-cases/ (дата звернення: 22.04.2026).

тому сучасний дебанкінг має включати не лише твердження «це неправда», а й показ того, як саме була сконструйована маніпуляція.

Прикладом може бути російська кампанія про «біолабораторії США в Україні». Її сила була не в одному фейку, а у поєднанні страху, псевдонаукової достовірності, антизахідних настроїв і недовіри до міжнародних інституцій загалом. Просте спростування «біологічної зброї немає» є необхідним, але також було недостатнім. Ефективний дебанкінг має пояснювати, чому така тема емоційно працює, як використовуються наукові терміни для створення псевдодоказовості, чому подібні наративи поширюються на міжнародні аудиторії, і який політичний ефект вони мають створити. Саме тут дебанкінг переходить від фактологічного спростування до навчання аудиторії розпізнавати методи маніпуляції.

Водночас, сам дебанкінг має бути якісним. Неефективний дебанкінг характеризується низьким охопленням, запізненням реагування та слабкою інтеграцією у дискусійне середовище. Як показало дослідження, проведеного у 2024 році, медіанний час появи фактчекінгу становив чотири дні після виникнення дезінформаційного наративу, тоді як самі фактчек-матеріали становили менш ніж 1,2% усіх інформаційних взаємодій навколо теми спростування.[148]

Четвертим інструментом є пребанкінг, або попереджувальна обробка аудиторії проти маніпуляцій. Його логіка полягає у тому, що людям заздалегідь пояснюють типові прийоми дезінформації, ще до того, як вони зіткнуться з конкретним фейком, ІПСО або наративом. Для нас це особливо важливо, тому що російські операції впливу часто мають циклічний характер. Перед важливими міжнародними рішеннями активізуються повідомлення про «втому Заходу». Після ударів по цивільній інфраструктурі з’являються спроби перекласти відповідальність. Під час мобілізаційних дискусій просуваються наративи про

[148] Wack M., Duskin K., Hodel D. Political Fact-Checking Efforts are Constrained by Deficiencies in Coverage, Speed, and Reach. Dec 19th 2024. URL: https://arxiv.org/pdf/2412.13280 (дата звернення: 23.04.2026).

«несправедливість мобілізації стосовно груп\регіонів\верств населення», «хаос в державному управлінні\владі», «беззахисність населення» і «зраду національних інтересів\національної боротьби». Якщо аудиторія заздалегідь знає, що такі теми будуть експлуатуватися, вона менш схильна реагувати на них імпульсивно.

П’ятий інструмент – це кризові комунікації. У воєнних умовах вони мають не просто інформаційну, а й психологічну функцію. Коли відбувається масований обстріл, техногенна аварія, кібератака або резонансний інформаційний інцидент, перші години є критичними. Якщо держава мовчить, інформаційний вакуум заповнюється чутками, припущеннями й ворожими інтерпретаціями. Як зазначає у своїй книзі В. Станчишин, війна створює стан тривалого емоційного напруження, у якому аудиторія гостро потребує зрозумілих орієнтирів і пояснень.[149] Тому кризова комунікація має відповідати трьом вимогам: бути швидкою, правдивою і психологічно стабілізуючою.

Швидкість, в даному контексті, не означає поспішність. Якщо інформація неперевірена, офіційний комунікатор має чесно зазначити, що дані уточнюються. Правдивість також не означає розкриття всієї інформації, особливо якщо йдеться про військові деталі. Психологічна стабілізація тут теж не означає заспокоєння будь-якою ціною. Вона означає, що аудиторія отримує зрозуміле пояснення, де вказується що сталося, що відомо, що робить держава, чого не варто робити громадянам, де шукати оновлення інформації тощо. Така структура повідомлення зменшує простір для паніки і маніпуляцій. У цьому сенсі кризові комунікації є формою контрпропаганди навіть тоді, коли вони прямо не спростовують фейків, бо вони не дають ворожій стороні монополізувати перше пояснення події.

Шостим інструментом є робота з цифровими платформами. У другому розділі було показано, що російська пропаганда активно використовує соціальні мережі, Telegram, проксі-ресурси та мережеві розгони. Відповідно до цього,

---

[149] Станчишин В. Емоційні гойдалки війни : роздуми психотерапевта про війну. Вид. 2-ге, допов. Київ : Віхола, 2024, 309 с.

контрпропаганда має діяти не лише на рівні контенту, а й на рівні інфраструктури його поширення. Йдеться про виявлення координованих мереж ботів, фейкових сторінок, каналів, що системно розганяють дезінформацію, та про співпрацю з платформами щодо їхнього обмеження. Meta у своїх звітах про adversarial threats у 2024 році продовжувала публікувати дані про виявлення й видалення мереж, пов'язаних із координованою неавтентичною поведінкою, а Freedom House, посилаючись на Meta, зазначав, що російські суб'єкти, пов'язані з урядом, "особливо агресивно і наполегливо" таргетували Україну дезінформаційними наративами. У Q2 2024 Meta видалила мережу з 12 акаунтів Facebook, 32 сторінок, 5 груп і 3 Instagram-акаунтів, що походила з росії, але управлялася фірмою зі Шрі-Ланки і критикувала український уряд.[150]

Цей приклад важливий не стільки кількісно, скільки якісно. Він показує, що сучасні інформаційні операції можуть бути багатошаровими, де країна походження, технічний оператор, контентна рамка і цільова аудиторія можуть бути рознесені між різними юрисдикціями та навіть країнами. Це ускладнює реагування, тому що національна держава не завжди має прямий доступ до інфраструктури, через яку поширюється вплив. Саме тому робота з платформами має бути постійною, інституційною і міжнародно координованою.

Сьомим інструментом є медіаграмотність. Вона відрізняється від фактчекінгу тим, що працює не з конкретним повідомленням, а зі здатністю аудиторії самостійно оцінювати інформацію. Її значення особливо зростає в умовах інфодемії, коли проблема полягає не лише в наявності неправдивої інформації, а в перенасиченні інформаційного простору. Як зазначають Гаращук і Сергєєв, інфодемія у цифрову епоху створює загрози політичній стабільності саме через перевантаження аудиторії та спрощення сприйняття складних

[150] Веб-портал https://freedomhouse.org/. Key Developments, June 1, 2023 – May 31, 2024. 2024. URL:https://freedomhouse.org/country/ukraine/freedom-net/2024 (дата звернення 23.04.2026)

процесів.[151] Тому медіаграмотність має бути не факультативною освітньою темою, а обов'язковою складовою комплексу національного спротиву.

Українська медіаграмотність у контексті війни має специфіку. Її завданням є не лише навчити перевіряти джерела, а й сформувати розуміння того, як працюють ворожі операції впливу. Людина має розпізнавати не тільки очевидний фейк, а й маніпулятивний фрейм, емоційну провокацію, а також псевдоекспертність, «злив», анонімне джерело, штучний розгін і підміну причинно-наслідкових зв'язків. Це зближує медіаграмотність із пребанкінгом, коли аудиторія отримує не лише знання, а й психологічну готовність до зіткнення з маніпуляцією.

Восьмим інструментом є взаємодія з громадянським суспільством. В Україні цей компонент має особливо велике значення, тому що громадянське суспільство часто діє швидше, гнучкіше і ближче до конкретних аудиторій, ніж державні інституції. Фактчекінгові ініціативи, незалежні медіа, волонтерські OSINT-спільноти, експертні групи, освітні проєкти і локальні комунікатори, як от лідери суспільної думки, створюють розподілену систему стійкості. Вона не замінює державу, але підсилює її там, де офіційна комунікація має обмежену довіру або меншу швидкість.

Перевага громадянського суспільства полягає у довірі й гнучкості. Але тут є і ризик, бо якщо громадські ініціативи діють повністю розрізнено, без обміну даними й узгодження базових принципів, ефект може бути фрагментарним, а то і подеколи нівельованим. Тому оптимальною є модель партнерства, у якій держава забезпечує стратегічну рамку, доступ до важливої інформації та міжнародну взаємодію, а громадянське суспільство підтримує моніторинг, пояснення, локалізацію і довіру.

Дев'ятим інструментом є міжнародна комунікація. Українська контрпропаганда має працювати не лише з внутрішньою аудиторією, а також із

---

[151] Гаращук, Д., Сергєєв, В. Інфодемія та популізм у цифрову епоху: загрози політичній стабільності та безпекові виклики. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2025-2(8)-61-71 (дата звернення: 04.04.2026).

міжнародними партнерами. Це пов’язано з тим, що російська пропаганда активно намагається знизити міжнародну підтримку України. EEAS (Додаток Г) у звіті про діяльність із протидії FIMI за 2024 рік зазначив, що Україна залишалася головною мішенню російських FIMI-операцій, спрямованих на підрив її легітимності та міжнародної підтримки уряду й народу.[152] У свою чергу це означає, що українська контрпропаганда має пояснювати війну зовнішнім аудиторіям не менш системно, ніж внутрішнім. Вона має підтримувати міжнародну рамку, що це не «криза в Україні», а війна агресії РФ проти суверенної держави. Що це не локальний конфлікт, а загроза міжнародному порядку. Що допомога Україні - це не благодійність, а інвестиція у європейську безпеку.

Десятим інструментом є робота з новими технологіями, зокрема штучним інтелектом. Генеративні інструменти можуть спрощувати створення фейкового контенту, автоматизувати виробництво текстів, зображень, відео, коментарів і псевдоаналітики. Аналітичне видання Reuters у 2024 році повідомляло, що OpenAI заявила про припинення п’яти спроб використання її інструментів для «операцій обману» (deceptive activity) в інформаційно-психологічних операціях впливу, зокрема пов’язаних з росією, Китаєм, Іраном та Ізраїлем. Дані кампанії створювали коментарі, статті й профілі у соцмережах, але не отримали значного охоплення.[153] Для нашої країни це має слугувати приводом для усвідомлення того, що технологічна контрпропаганда має включати не лише класичний фактчекінг, а й виявлення синтетичного контенту, аналіз поведінкових шаблонів та співпрацю з технологічними компаніями.

Усі ці інструменти мають різний часовий горизонт. Фактчекінг і кризові комунікації працюють швидко, але мають обмежений довгостроковий ефект. Стратегічні наративи й медіаграмотність працюють повільніше, але формують

---

[152] 3rd EEAS Report on Foreign Information Manipulation and Interference Threats. March 2025. URL: https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf (дата звернення: 23.04.2026).

[153]. OpenAI has stopped five attempts to misuse its AI for 'deceptive activity'. May 30, 2024. URL: https://www.reuters.com/technology/cybersecurity/openai-has-stopped-five-attempts-misuse-its-ai-deceptive-activity-2024-05-30 (дата звернення: 23.04.2026)

стійкість. Робота з платформами може швидко зменшити охоплення конкретної мережі, але не усуває саму причину вразливості. Взаємодія з громадянським суспільством підвищує довіру, але потребує координації. Саме тому інструменти контрпропаганди не можна ранжувати за принципом «головний\другорядний», тому що вони мають працювати як єдина система.

Так, з огляду на аналіз інструментів контрпропаганди можна сказати, що ефективна контрпропаганда України має поєднувати стратегічні наративи, ефективний фактчекінг, дебанкінг, пребанкінг, кризові комунікації, платформну взаємодію, медіаграмотність, міжнародну комунікацію і партнерство з громадянським суспільством. Її головна мета має бути не лише спростовування неправди, а також і зменшення шкоди від ворожого впливу, зміцнення довіри, підвищення стійкості разом із збереженням легітимності демократичної держави в умовах повномасштабної війни. Такий підхід прямо узгоджується з висновками, які були наведені у рамках першого розділу, що контрпропаганда має бути не «дзеркалом» ворожої пропаганди, а легітимною системою захисту інформаційного простору від ворожих впливів.

3.3. Західні підходи та їх адаптація. EEAS/FIMI, NATO StratCom, Hybrid CoE, RAND. Межі та можливості адаптивності

Західні підходи до протидії пропаганді та дезінформації сформувалися в умовах поступового усвідомлення того, що інформаційні загрози не є другорядним супроводом політичних конфліктів, а становлять окремий безпековий вимір. Для України цей досвід є важливим, але, з огляду на реалії російсько-української війни, не може бути механічно перенесений, оскільки українська ситуація відрізняється від більшості західних моделей рівнем інтенсивності загроз, попереднього спільного нав’язаного культурного та інформаційного простору, прямою залежністю інформаційного простору від бойових дій і високою швидкістю зміни інформаційного середовища. Якщо для багатьох країн ЄС або НАТО протидія дезінформації переважно є питанням

демократичної стійкості, захисту виборчих процесів, медіасистеми та довіри до інституцій, то для України вона одночасно є питанням виживання держави, підтримання обороноздатності та збереження міжнародної підтримки.

Саме тому західний досвід у цій сфері слід розглядати не як готову модель, а як набір методів, підходів, інструментів та принципів, які можуть бути адаптовані до українського контексту. Така адаптація має відбуватися вибірково, тому що Україна може використовувати західні методики моніторингу, атрибуції, стратегічних комунікацій, міжсекторальної координації та оцінювання ефективності, але повинна враховувати власні умови, тобто воєнний стан, обмеженість ресурсів, високу динаміку загроз, активну роль громадянського суспільства і потребу у оперативномк реагуванні та рішеннях. У цьому сенсі західні підходи виконують для України не роль шаблону, а роль методологічної опори.

Одним із найбільш розвинених підходів у Європейському Союзі є концепція FIMI (Foreign Information Manipulation and Interference , «Іноземна інформаційна маніпуляція та вплив», англ.). Її перевага полягає в тому, що вона не зводить проблему до «фейкових новин», а розглядає інформаційний вплив як комплексну поведінку ворожого суб’єкта. Це особливо важливо для теми роботи, тому що російська пропаганда, як було показано у розділі 2, діє не лише через неправдиві твердження, а через наративи, їх повторюваність, маніпулятивне оформлення, проксі-канали, цифрові мережі та вплив на різні цільові аудиторії. У звіті EEAS про діяльність із протидії FIMI за 2024 рік Україна прямо визначається як головна мішень FIMI-операцій, спрямованих на підтримку й виправдання російських воєнних зусиль та підрив боротьби України за суверенітет і незалежність.[154]

[154] 3rd EEAS Report on Foreign Information Manipulation and Interference Threats. March 2025. URL: https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf (дата звернення: 25.04.2026).

Цей підхід важливий тим, що переводить аналіз з рівня окремого повідомлення на рівень поведінкових патернів, тобто шаблонів. Якщо класичний фактчекінг запитує «це правда чи неправда?», то FIMI-підхід ставить ширші питання, а саме хто є актором впливу, яку поведінку він демонструє, які канали використовує, які цільові аудиторії охоплює, які теми повторює, які ефекти прагне створити тощо. Для України така рамка є особливо корисною, бо вона дозволяє виявляти не лише фейки, а й цілі інформаційні кампанії, що їх створюють та поширюють. Наприклад, повідомлення про «втому Заходу від України», чи «нелегітимність української влади», чи «неефективність допомоги» або «неминучість російської перемоги» можуть поширюватися різними каналами і в різних мовних формах, але належати до одного операційного задуму чи інформаційно-психологічному впливу або спеціальній операції. Саме FIMI-логіка дозволяє побачити цю системність.

Важливо також зазначити, що ЄС розглядає FIMI не лише як інформаційну проблему, а і як елемент зовнішньої та безпекової політики. Це наближає європейський підхід до українського контексту, де інформаційна агресія прямо пов’язана з воєнними діями. Водночас європейська модель має власні обмеження для імплементації в Україні. Вона часто побудована на процедурах, міжінституційних консультаціях і тривалому документуванні та узгодженні. В умовах нашої країни частина таких процедур може бути занадто повільною. Якщо, наприклад, інформаційна атака супроводжує ракетний удар, кібератаку або кризу на фронті, держава не може чекати повного аналітичного циклу. Тому FIMI-підхід варто адаптувати як аналітичну рамку для класифікації та документування, але не як єдину модель оперативного реагування.

Іншим важливим європейським інструментом є EUvsDisinfo, який створив відкриту базу прикладів прокремлівської дезінформації. Його цінність полягає в накопиченні емпіричного матеріалу, що дозволяє виявляти повторювані теми, структури та наративи. Для нас це важливо не лише як джерело спростувань, а як приклад побудови пам’яті інформаційних операцій. Російська пропаганда

часто працює циклічно. Старі наративи повертаються у нових формах, адаптуючись до поточного контексту. Тому база таких випадків дозволяє не починати аналіз з початку щоразу, а бачити спадковість дезінформаційних кампаній. У цьому сенсі EUvsDisinfo є не лише фактчекінговим проєктом, а й інструментом стратегічного моніторингу.

Паралельно з європейським напрямом важливе значення має досвід НАТО у сфері стратегічних комунікацій. NATO Strategic Communications Centre of Excellence (CoE або ще в українському сегменті визначається як «Центр передового досвіду НАТО зі стратегічних комунікацій») розглядає стратегічні комунікації як інтеграцію інформаційних, дипломатичних, військових і політичних компонентів. Для України цей підхід особливо важливий, тому що він дозволяє поєднати цивільну комунікацію, оборонну логіку й міжнародну підтримку. У спільному звіті NATO StratCom COE та українського Центру стратегічних комунікацій, присвяченому атрибуції російських інформаційно-психологічний спеціальних операцій, зазначено, що досліджуються російські операції впливу проти аудиторій в Україні та сусідніх регіонах, включно з українськими цивільними, Силами оборони, цивільними у сусідніх державах та європейськими прокремлівськими групами.[155]

Дана теза є важливою для української контрпропаганди, бо вона підтверджує багатовекторність російського впливу. Російські інформаційно-психологічні спеціальні операції не спрямовані лише на «українське населення» як абстрактну масу, вони також таргетують конкретні групи цивільних, військових, родини військових, жителів прикордонних регіонів, аудиторії сусідніх держав, західних виборців, проросійські середовища в Європі тощо. Відповідно, українська контрпропаганда має також бути сегментованою. Один і той самий меседж не може однаково ефективно працювати для українського

[155] Dikhtiarenko, S., Heap, B., Pamment, J., Smith, V. Attributing Russian Information Influence Operations: Testing the Information Influence Attribution Framework with real-world case studies. Riga: NATO Strategic Communications Centre of Excellence. 12th February 2026. URL: https://stratcomcoe.org/publications/attributing-russian-information-influence-operations-testing-the-information-influence-attribution-framework-with-real-world-case-studies/340 (дата звернення:25.04.2026).

суспільства, європейських партнерів, військових союзників і громадян країн Глобального Півдня. NATO StratCom-підхід корисний тим, що змушує мислити не лише повідомленнями, а аудиторіями, цілями, каналами і ефектами.

Однак у використанні підходів НАТО також є свої обмеження. НАТО є міждержавною безпековою організацією, яка діє в межах складної системи погоджень, політичного консенсусу та інституційних процедур. Україна ж у воєнних умовах потребує швидших і часто більш гнучких рішень. Тому з НАТО-підходу доцільно переносити не бюрократичну модель, а саме принципи узгодженісті повідомлень, зв'язку комунікації з діями, сегментацію аудиторій, оцінювання ефектів з інтеграцією цивільного і безпекового вимірів. Саме ці принципи можуть бути адаптовані до українського середовища без втрати оперативності.

Окремий пласт становить досвід Hybrid CoE – Європейського центру передового досвіду з протидії гібридним загрозам. Для України особливо важливим є дослідження «How Ukraine fights Russian disinformation: Beehive vs mammoth», за редакцією Якуба Каленського та Романа Осадчука. [156] У ньому Україна описується через метафору «вулик проти мамонта», де російська система є великою, важкою і ресурсною, тоді як українська протидія значною мірою тримається на мережевості, розгалудженості, швидкості, гнучкості й взаємодії численних її суб'єктів.

Дана метафора дуже точно описує українську модель. Її сила не в абсолютній централізації, а в багатоточковій активності, де державні інституції, журналісти, OSINT-розслідувачі, волонтери, аналітики, громадські організації, міжнародні партнери та активні громадяни створюють розподілену систему протидії. У тексті Hybrid CoE також акцентовано потребу повторення повідомлень, тобто, що не достатньо один раз опублікувати список фейкових

[156] Kalenský J. & Osadchuk R. How Ukraine fights Russian disinformation: Beehive vs mammoth. Hybrid CoE Research Report 11. January 2024. URL: https://www.hybridcoe.fi/wp-content/uploads/2024/01/20240124-Hybrid-CoE-Research-Report-11-How-UKR-fights-RUS-disinfo-WEB.pdf (дата звернення: 25.04.2026).

каналів, повідомлення потрібно повторювати щоденно, бо саме повторюваність є одним із механізмів російського впливу. Для нашої країни це важлива практична теза, тому що контрпропаганда має бути ритмічною. Одноразове спростування рідко перемагає системну пропаганду. Їй потрібно протиставляти не тільки правду, а й стабільну присутність правдивого пояснення у інформаційному середовищі з таргетованими повідомленнями цільовим групам впливу.

Hybrid CoE-підхід також корисний тим, що розглядає дезінформацію не ізольовано, а як частину ширших гібридних загроз. Це дозволяє пов'язати інформаційний вплив із кібератаками, економічним тиском, дипломатичними діями, саботажем, енергетичним шантажем та безпосередньо воєнними операціями. Для нашої держави така рамка є необхідною, бо російська пропаганда часто супроводжує фізичні дії, де удар по енергетичній інфраструктурі супроводжується повідомленнями про «нездатність держави захистити своїх громадян», атаки на мобілізаційні об'єкти супроводжуються наративами про «хаос мобілізації», дипломатичні дискусії про допомогу Україні супроводжуються хвилями повідомлень про «втому партнерів від конфлікту в Україні» тощо. Якщо ці процеси аналізувати окремо, втрачається системність.

Аналітичний досвід RAND (Research And Development Corporation)[157] також є важливим для України. RAND у 2024 році опублікував дослідження про українську протидію російській дезінформаційній війні, де було зазначено, що після повномасштабного вторгнення росія веде масштабну, багатоканальну дезінформаційну кампанію, спрямовану не лише на підрив української стійкості, а й на підтримку російської підтримки війни та виснаження міжнародної підтримки України.[158] Дана оцінка напряму узгоджується з висновками з розділу 2, де визначається, що російська пропаганда має три головні контури – внутрішній російський, український і міжнародний. Відповідно,

[157] Веб-сайт RAND Corporation. 2026. URL: https://www.rand.org/about.html (дата звернення: 25.04.2026).
[158] Helmus T.C., Holynska K. Ukrainian Resistance to Russian Disinformation.
Lessons for Future Conflict. 2024. URL: https://www.rand.org/pubs/research_reports/RRA2771-1.html (дата звернення: 25.04.2026).

контрпропаганда України також має працювати у трьох контурах, а саме зміцнення внутрішньої стійкості, нейтралізація впливу на українське суспільство і підтримання міжнародної коаліції.

RAND може бути корисним ще й тим, що розглядає український досвід як джерело уроків для США та союзників. Це змінює звичну оптику, де Україна не лише запозичує західні підходи, а і сама стає джерелом практичних знань. У сфері протидії російській дезінформації український досвід часто є більш практичним і перевіреним ніж досвід держав, які не живуть в умовах повномасштабної війни. Це означає, що адаптація має бути двосторонньою. Україна бере методики, стандарти та інституційні рамки Заходу, але і Захід також може брати українські практики швидкої реакції, мережевої взаємодії та громадянської мобілізації.

Західні підходи мають кілька сильних сторін, які є релевантними для України. Перша – інституційність. Європейські та євроатлантичні структури створюють сталі механізми, які не залежать лише від окремих людей. Для України це важливо, бо частина системи контрпропаганди ще і досі залежить від персональної активності окремих команд, лідерів суспільної думки або організацій. Інституційність дозволяє зберегти сталість у довгостроковій перспективі.

Друга сильна сторона – доказовість. Західні підходи дедалі більше орієнтуються на документування поведінки суб’єктів(акторів), атрибуцію інформаційно-психологічних спеціальних операцій, опис їх тактик, технік і процедур. Це важливо, тому що дозволяє уникати абстрактних звинувачень і будувати комунікацію на фактах. Для України це має значення не лише всередині країни, а й у міжнародному середовищі, де партнери охочіше реагують на доказово оформлені звіти, ніж на загальні твердження про «інформаційну війну проти України».

Третя сильна сторона – міжсекторальність. У західних підходах протидія дезінформації поступово перестає бути завданням лише медіа або державної

комунікації. Вона включає кібербезпеку, дипломатію, освіту, регулювання інформаційних платформ та соціальних мереж, роботу з виборчими процесами, підтримку незалежних медіа, дослідження суспільної думки та інше. Для України така міжсекторальність також є необхідною, бо російська пропаганда не поважає адміністративних меж. Вона одночасно цілить по обороні, політиці, економіці, соціальній психології та міжнародних відносинах.

Четвертою сильною стороною є оцінювання ефективності. Західні підходи все більше уваги приділяють тому, як вимірювати вплив FIMI та контрзаходів. Це важливо, бо без метрик контрпропаганда ризикує перетворитися на набір інтуїтивних дій. Для нашої держав це особливо актуально, тому що у воєнних умовах ресурси обмежені, тому потрібно розуміти, які інструменти працюють, а які лише створюють видимість активності чи які можуть мати побічні ефекти чи навіть негативний вплив.

Водночас західні підходи мають і обмеження. По-перше, це темп. Європейські інституції часто працюють у логіці звітів, погоджень і процедур, що можуть займати дні та тижні, тоді як інформаційна атака розгортається за години. Україна не може повністю покладатися на повільні механізми, коли йдеться про кризові ситуації. По-друге, це ресурсна асиметрія. Частина західних моделей передбачає значні аналітичні, технологічні й фінансові ресурси, які Україна не завжди може забезпечити. По-третє, відмінність правового контексту. У воєнний час Україна має інші обмеження і пріоритети, ніж країни, що функціонують у звичайному правовому режимі. Четверте – це різниця в аудиторіях. Те, що працює для західного виборця, не завжди працює для українського суспільства або для аудиторій Глобального Півдня.

Особливо складним є питання балансу між безпекою і свободою слова. У західних демократіях протидія дезінформації часто супроводжується гострими дебатами про межі регулювання. Для України ця дилема ще складніша, бо російська пропаганда прямо пов’язана з воєнною агресією. Однак навіть у воєнних умовах надмірне або непрозоре втручання в інформаційний простір

може підірвати довіру. Тому адаптація західних підходів має спиратися на принцип легітимності, в якому будь-які обмеження мають бути обґрунтованими, пропорційними, поясненими й спрямованими саме проти ворожого впливу, а не проти внутрішньої дискусії.

Для України доцільно переносити з західного досвіду насамперед чотири елементи. Першим можна визначити FIMI-рамку як спосіб класифікації операцій впливу. Вона дозволяє бачити не лише фейки, а поведінку акторів, їхні тактики, канали та цілі. Другий – це стандарти стратегічних комунікацій НАТО, які наголошують на узгодженості повідомлень, зв'язку комунікації з діями й роботі з аудиторіями. Третім варто визначити міжсекторальний підхід Hybrid CoE, який показує, що інформаційні загрози потрібно аналізувати разом із кібернетичними, політичними й соціальними. Четвертим - аналітичну культуру RAND, орієнтовану на доказовість, попередні уроки та оцінювання ефективності заходів.

В свою чергу, не варто механічно переносити громіздкі бюрократичні структури, повільні процедури або моделі, розраховані на функціонування у мирний час. Україна потребує легших та більш швидших механізмів, які можуть працювати у режимі постійної кризи. Оптимальною є гібридна модель, де стратегічна рамка має бути стабільною й інституційною, а оперативне реагування – гнучким та мережевим. Така модель відповідає українському досвіду «вулик проти мамонта», про який ми згадували вище, де сила України полягає не лише в централізованих структурах, а й у здатності великої кількості акторів діяти синхронно, швидко й мотиваційно.

Отже, західні підходи до контрпропаганди становлять важливу методологічну й практичну базу для України, але їхня цінність залежить від правильної адаптації. Підхід EEAS/FIMI дає рамку аналізу іноземних маніпуляцій і втручань, в той час як підхід NATO StratCom – принципи стратегічної узгодженості, а Hybrid CoE дає розуміння гібридної природи загроз і мережевої стійкості. RAND, в свою чергу, являється доказовий і уроково-орієнтований підходом. Усі ці елементи можуть посилити українську систему

контрпропаганди, якщо будуть адаптовані до умов війни, української інституційної реальності й необхідності зберігати демократичну легітимність в рамках обмежень воєнного стану.

3.4. Оцінювання ефективності контрпропаганди. Метрики, збір даних, аналітичні підходи та обмеження

Оцінювання ефективності контрпропаганди є одним із найскладніших елементів інформаційної безпеки, оскільки її результат не завжди проявляється у прямій, швидкій і кількісно вимірюваній формі. На відміну від військової або економічної сфери, де результат часто можна зафіксувати через конкретні показники, контрпропаганда працює з довірою, сприйняттям, емоційними станами, поведінковими реакціями, стійкістю аудиторій і здатністю суспільства відрізняти факт від маніпуляції. Саме тому оцінювання не може зводитися до простого підрахунку кількості спростованих фейків, переглядів офіційних повідомлень або охоплення інформаційних кампаній. Такі показники можуть бути корисними, але вони не дають відповіді на головне питання, як от чи зменшила контрпропаганда шкоду від ворожого впливу та чи підвищила інформаційну стійкість суспільства.

У цьому контексті важливо застосовувати ризик-орієнтований підхід. Якщо російська пропаганда, як було показано у розділі 2, спрямована на підрив довіри, деморалізацію, поляризацію, послаблення міжнародної підтримки та зміну поведінки цільових аудиторій, то ефективність контрпропаганди має оцінюватися через здатність нейтралізувати саме ці ефекти. Як зазначають у своїй праці Потій, Горбенко та ін, аналіз кібер- й інформаційної безпеки потребує оцінювання ризиків, вразливостей та їх наслідків, а не лише формальної фіксації подій.[159] Для теми даної кваліфікаційної роботи це означає, що контрпропаганда

[159] Потій О.В., Горбенко Ю.І., Замула О.А., Ісірова К.В. «Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки». 2021. URL: https://duikt.edu.ua/uploads/l_1066_72351971.pdf (дата звернення: 26.04.2026).

має оцінюватися не за кількістю комунікаційних активностей, а за тим, наскільки вона знижує вразливість інформаційного середовища перед впливом противника.

Першою ключовою метрикою є довіра. Вона має розглядатися не як абстрактна соціологічна категорія, а як практичний ресурс національної безпеки. Якщо аудиторія не довіряє державним інституціям, офіційним джерелам, незалежним медіа або експертному середовищу, навіть точна і швидка інформація може бути відкинута як «провладна пропаганда», «маніпуляція» або «приховування правди». Ліпкан у своїй роботі прямо пов'язує національну безпеку зі станом суспільства та здатністю інститутів підтримувати легітимність і керованість.[160]

Отже, довіра є не лише результатом ефективної контрпропаганди, а й передумовою її ефективної роботи. Довіру можна вимірювати через регулярні соціологічні опитування, фокус-групи, аналіз динаміки ставлення до офіційних джерел, медіа та конкретних інституцій. Але важливо не обмежуватися загальним питанням «чи довіряєте ви державі\владі\адміністрації?».

Таким прикладом виміру ефекту довіри можна побачити у статті The Financial Times від 23 березня 2025 року, де відзначалось збільшення довіри до президента України Володимира Зеленського після перепалки з очільником Білого дому, Дональдом Трампом у лютому 2025 року.[161] Тоді, за даними КМІС, рейтинг довіри до президента України піднявся до 67% через тиждень після події.

Для оцінювання контрпропаганди потрібні більш точні індикатори, як довіра до повідомлень у кризових ситуаціях, довіра до джерел, які спростовують фейки, готовність перевіряти інформацію через офіційні канали, частота звернення до перевірених джерел, сприйняття державної комунікації як правдивої, своєчасної та зрозумілої та інші. Pew Research Center на прикладі США показує, що довіра до інформації від національних новинних організацій і

---

[160] Ліпкан В.А. Національна безпека України : навч. посібник . К. : Кондор, 2008, 552 с..
[161] Deprez F. Ukrainians rally around Zelenskyy after bruising Trump encounter. Mar 23rd 2025. URL: https://www.ft.com/content/8649ba24-9801-4063-bcf1-6364c1185c46 (дата звернення: 05.05.2026).

соціальних платформ змінюється в часі, а отже має розглядатися як динамічний показник, який потребує регулярного моніторингу, а не одноразового заміру.[162]

Другою метрикою можна визначити швидкість реагування. У цифровому середовищі час між появою дезінформації та першою якісною відповіддю має критичне значення. Якщо неправдиве повідомлення встигає сформувати перше емоційне враження, подальше спростування працює дедалі слабше. Це особливо важливо в умовах війни, коли російські інформаційні вкиди часто прив'язуються до чутливих тем, наприклад, обстрілів, втрат, політичних рішень, мобілізаційних тем або міжнародних переговорів. Як зазначає С.О. Лисенко, стратегічне управління інформаційною безпекою передбачає не лише наявність правильних повідомлень, а й здатність системи діяти своєчасно.[163]

Швидкість реагування можна вимірювати через кілька показників, наприклад, час від появи вкиду до його виявлення, час від виявлення до внутрішньої класифікації, час від класифікації до публічного повідомлення, час до поширення контрповідомлення у тих самих або релевантних каналах розповсюдження вкиду, час до зниження активності фейкового наративу. При цьому важливо не плутати швидкість із поспішністю. Оперативна відповідь не повинна бути неперевіреною. Якщо держава реагує швидко, але неточно, вона може завдати шкоди власній довірі. Тому реальна метрика має поєднувати два параметри – швидкість і достовірність.

Третьою метрикою є охоплення контрповідомлень, хоч її і потрібно трактувати обережно. Кількість переглядів, репостів або згадок сама по собі не є ознакою ефективності. Високе охоплення може свідчити як про успішну комунікацію, так і про скандал, поляризацію або негативну реакцію. Саме тому охоплення має аналізуватися разом із тональністю, структурою аудиторії,

---

[162] Report. Trust in Media. Feb 11th 2026. URL: https://www.pewresearch.org/topic/news-habits-media/media-society/media-attitudes/trust-in-media/ (дата звернення: 25.04.2026).

[163] Лисенко С.О. Стратегічне управління інформаційною безпекою держави : автореферат дисерт. на здобуття наук. ступ. д.н. з держ. упр. ; спец. 25.00.05 - державне управління у сфері державної безпеки та охорони громадського порядку. Житомирська політехніка. 2025. URL: https://ztu.edu.ua/site/files/1/docs/Університет/Спеціалізовані%20вчені%20ради/14.052.03/2025/ref_Лисенко_С.pdf . (дата звернення: 26.04.2026).

каналами поширення та поведінковим ефектом. Якщо спростування побачили переважно ті, хто й так не вірив фейку, ефект буде обмеженим. Якщо ж воно дійшло до групи, на яку був спрямований ворожий вплив, його цінність значно вища.

Четвертою метрикою можна визначити зміну наративного середовища. Це складніший, але більш змістовний показник. У розділі 2 було показано, що російська пропаганда працює не лише через окремі фейки, а через довготривалі наративи, як от «Україна не є суб'єктом», «Захід втомився», «опір безперспективний», «допомога марна», «переговори неминучі на умовах рф» тощо. Відповідно, ефективність контрпропаганди має оцінюватися через те, чи вдається зменшити присутність цих наративів, послабити їхню переконливість або замінити їх альтернативними смисловими рамками. Політичні наративи визначають спосіб інтерпретації подій, а тому вплив на наративне середовище є впливом на політичне сприйняття реальності, як це зазначено у праці Скрипникової, Тутік та ін.[164]

Для вимірювання наративного середовища можна використовувати контент-аналіз медіа, аналіз соціальних мереж, лінгвістичний аналіз великих масивів текстів, відстеження ключових слів, фреймів і повторюваних конструкцій. Так лінгвістичний аналіз даних інтернет-медіа та соціальних мереж може застосовуватися для оцінювання суспільних процесів.[165] У межах даної роботи такий підхід можна використати для відстеження того, як змінюється частотність і контекст ворожих наративів після вживаних контрзаходів.

П'ятою метрикою можна виділити зменшення шкоди. Це одна з найважливіших категорій, бо контрпропаганда не завжди здатна повністю зупинити дезінформацію, але може зменшити її наслідки. Якщо інформаційна

---

[164] Скрипникова Л.В., Політологія: навчальний посібник. К.: Центр учбової літератури, 2014, 272 с. URL: https://dduvs.edu.ua/biblioteka/biblioteka-studenta-dduvs/pidruchniki-posibniki/politologiya/ (дата звернення: 25.04.2026).

[165] Згуровський М. З., Ланде Д. В., Болдак А. О., Єфремов К. В., Перестюк М. М. Лінгвістичний аналіз даних інтернет-медіа та соціальних мереж у задачах оцінювання суспільних перетворень. *Кібернетика та системний аналіз*. 2021. URL: http://jnas.nbuv.gov.ua/article/UJRN-0001221023 (дата звернення 25.04.2026)

атака була спрямована на паніку, критерієм ефективності буде не повна відсутність фейку, а відсутність масової панічної поведінки. Якщо атака була спрямована на підрив довіри до інституції, критерієм буде те, чи вдалося запобігти різкому падінню довіри. Якщо атака була спрямована на міжнародну аудиторію, критерієм буде збереження підтримки, нейтралізація шкідливого фрейму або поява коректного пояснення у медіапросторі партнерів.

Саме категорія «зменшення шкоди» дозволяє уникнути завищених очікувань. У реальному інформаційному середовищі неможливо повністю зупинити всі фейки або гарантувати, що кожна аудиторія сприйме правдиву інформацію. Але можна скоротити життєвий цикл фейку, зменшити його охоплення, нейтралізувати найбільш небезпечний емоційний ефект, знизити ймовірність паніки або не допустити політичного рішення, вигідного агресору. Така логіка відповідає ризик-орієнтованому підходу, де ключовим є не абсолютне усунення загрози, а управління ризиком і наслідками.[166]

Шоста метрика визначається як стійкість аудиторії. Вона відображає здатність суспільства не лише реагувати на конкретне спростування, а самостійно протидіяти маніпуляціям. До цієї метрики входять рівень медіаграмотності, здатність перевіряти джерела, розпізнавання типових маніпулятивних прийомів, прояв емоційної стабільності у кризових ситуаціях, готовність не поширювати неперевірену інформацію тощо. Як зазначає В. Станчишин, війна створює стан емоційних коливань і виснаження, що підвищує вразливість до впливу.[167] Тому стійкість не можна вимірювати лише знаннями про дезинформацію, вона має включати і психологічний вимір.

Прикладом одновимірного оцінювання можна навести ланцюжок «джерело отримання інформації\розповсюдження наративу -> стійкість аудиторії». Так, за даними інформаційного агенства Reuters, 75% українців

---

[166] Потій О.В., Горбенко Ю.І., Замула О.А., Ісірова К.В. «Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки». 2021. URL: https://duikt.edu.ua/uploads/l_1066_72351971.pdf (дата звернення: 25.04.2026).

[167] Станчишин В. Емоційні гойдалки війни : роздуми психотерапевта про війну. Вид. 2-ге, допов. Київ : Віхола, 2024, 309 с.

отримають новини через соціальні мережі[168], що, як зазначається у статті, може свідчити про високу піддатливість населення до дизінформації. Проте, без виміру психологічної стійкості до сприйняття цих наративів, оцінка може бути неповна, а то і спотворена, хоча все ж дана метрика і дає можливість робити деякі висновки в контексті ефективних каналів контрпропаганди.

Сьомою метрикою є стабільність міжнародної підтримки. Для України це окрема стратегічна категорія, бо російська пропаганда активно працює не лише всередині України, а й проти західних суспільств, урядів і виборців. EEAS у звіті про діяльність із протидії FIMI за 2024 рік зазначає, що Україна залишалася головною мішенню російських FIMI-операцій, спрямованих на підрив її легітимності і міжнародної підтримки. У 3-му звіті FIMI Threat Report EEAS за 2025 рік також ідеться, що Україна була головною ціллю російських FIMI-атак у вибірці, з 257 зафіксованими інцидентами, тобто майже половиною записаних випадків.[169] З даного звіту випливає, що зовнішній контур контрпропаганди має оцінюватися не менш уважно, ніж внутрішній.

Для оцінювання міжнародної підтримки можна використовувати кілька груп показників, як от соціологічні дані в країнах-партнерах, тональність медійного висвітлення, частоту й контекст згадок про Україну, політичні рішення щодо військової, фінансової та гуманітарної допомоги, наявність або відсутність у публічному дискурсі російських фреймів тощо. Важливо, що стабільність підтримки не залежить лише від інформаційної політики України, але контрпропаганда може впливати на те, як партнери розуміють ціну війни, логіку допомоги і ризики поступок агресору.

Восьмою метрикою можна виділити атрибуцію інформаційних операцій. Вона показує, наскільки система здатна не лише виявити фейк, а й аргументовано пов’язати його з певним суб’єктом, мережею або патерном поведінки. NATO

---

[168] Hunder M. Russia vs Ukraine: the biggest war of the fake news era. Aug 1st 2024. URL: https://www.reuters.com/world/europe/russia-vs-ukraine-biggest-war-fake-news-era-2024-07-31/ (дата звернення: 25.04.2026).

[169] Звіт про діяльність EEAS з протидії іноземним інформаційним маніпуляціям та втручанню – 2024. (FIMI). 22 серпня 2025. URL: https://www.eeas.europa.eu/eeas/2024-report-eeas-activities-counter-foreign-information-manipulation-and-interference-fimi_en?etrans=uk. (дата звернення: 25.04.2026).

StratCom COE у 2026 році опублікував дослідження про застосування Information Influence Attribution Framework[170] до реальних російських кампаній, наголошуючи, що FIMI-рамка, санкції ЄС і Digital Services Act[171] підвищують стандарти доказовості. Для України це принципово важливо, тому що чим краще доказовість, тим легше будувати міжнародну реакцію, санкції, платформні обмеження і публічне пояснення загрози.

Дев'ятою метрикою доцільно виділити інституційну відтворюваність реагування. Ефективність контрпропаганди не повинна залежати лише від таланту окремих комунікаторів або випадкового успіху конкретної команди. Система має працювати повторювано: виявлення -> оцінка -> реакція -> поширення -> моніторинг -> корекція. Якщо кожна інформаційна атака щоразу проходить в ручному режимі без стандартизованого процесу, то система буде перевантажуватися. Інституційна відтворюваність означає наявність протоколів, відповідальних суб'єктів взаємодії, каналів взаємодії, баз даних наративів та шаблонів кризової комунікації, та механізмів навчання на попередніх кейсах.

Окремо потрібно враховувати якість даних, на яких ґрунтується оцінювання. Дані можуть надходити з відкритих джерел, соціальних мереж, моніторингу медіа-простору, соціології, платформних звітів, OSINT-розслідувань, урядових повідомлень і міжнародних аналітичних звітів. Кожне джерело має переваги й обмеження. Соціальні мережі дають швидкі дані, але вони не завжди бувають репрезентативні. Опитування дають репрезентативність, але повільніші й дорожчі. Платформенні звіти дають дані про видалені мережі\аккаунти, але не завжди розкривають повну методологію. OSINT може бути швидким і гнучким, але потребує перевірки та часу на формування звітів.

---

[170] Dikhtiarenko, S., Heap, B., Pamment, J., Smith, V. Attributing Russian Information Influence Operations: Testing the Information Influence Attribution Framework with real-world case studies. Riga: NATO Strategic Communications Centre of Excellence. 12th February 2026. URL: https://stratcomcoe.org/publications/attributing-russian-information-influence-operations-testing-the-information-influence-attribution-framework-with-real-world-case-studies/340 (дата звернення:25.04.2026).

[171] The Digital Services Act. 2026. URL: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act (дата звернення: 25.05.2026)

Тому оцінювання має спиратися на триангуляцію, тобто зіставлення інформації з кількох джерел.

RAND у 2024 році описав російську кампанію проти України як «wide-reaching, high-volume and multichannel disinformation campaign» («широкоспрямовану, високоємнісну та мультиканальну дезінформаційну кампанію», англ), спрямовану на підрив української стійкості, підтримку російської війни та виснаження міжнародної підтримки України.[172] Дана характеристика важлива для методології оцінювання, тому що якщо загроза є широкою, багатоканальною і високочастотною, то й оцінювання не може бути вузьким та однонаправленим. Не можна оцінювати ефективність контрпропаганди лише за кількістю спростувань на одному сайті або переглядів одного відео. Потрібна система, що бачить усі три контури: український (зовнішній), російський (внутрішній) та міжнародний.

Складність оцінювання полягає також у проблемі причинності. Якщо після комунікаційної кампанії рівень довіри зріс, не завжди очевидно, чи це результат кампанії, чи наслідок військових успіхів, міжнародних рішень, економічних змін або інших факторів. Якщо після інформаційної атаки не сталося паніки, це може бути результатом якісної комунікації, а може бути наслідком загальної звички суспільства до криз. Тому оцінювання мають бути обережними. Вони мають показувати не абсолютну причинність, а ймовірнісний внесок контрзаходів у зміну ситуації.

Ще однією проблемою являються відкладені ефекти. Деякі результати контрпропаганди помітні швидко, як от зменшення поширення фейку, поява офіційного пояснення, зниження панічних реакцій. Інші проявляються повільно: зростання медіаграмотності населення країни, зміцнення довіри до джерел контрпропаганди, формування стійкого наративу, зменшення сприйнятливості до повторюваних маніпуляцій. Тому система оцінювання має включати коротко-,

[172] Helmus T. C., Holynska K. Ukrainian Resistance to Russian Disinformation: Lessons for Future Conflict. Santa Monica, CA: RAND Corporation, 2024. URL: https://www.rand.org/pubs/research_reports/RRA2771-1.html (дата звернення: 25.04.2026).

середньо- і довгострокові показники. Короткострокові відповідають на питання «чи вдалося мінімізувати шкоду зараз?», середньострокові – «чи змінилася структура дискусії?», а довгострокові – «чи стала аудиторія стійкішою?».

В даному контексті також потрібно оцінювати побічні ефекти контрпропаганди. Спростування може ненавмисно повторити фейк і посилити його впізнаваність або навпаки, викликати «ефект Барбари Стрейзанд». Жорстке обмеження контенту може бути використане ворогом як доказ «цензури». Надмірна емоційність державної комунікації може знизити довіру до повідомлень. Непрозорі рішення можуть спровокувати підозру у приховуванні фактів або їх підміну. Тому ефективність має включати не тільки позитивні результати, а й аналіз ризиків. Це напряму пов’язано з принципом легітимності, сформульованим у розділі 1, про те, що контрпропаганда в демократичній державі не повинна копіювати методи ворожої пропаганди.

Практично систему оцінювання можна побудувати як цикл. На першому етапі фіксується загроза, тобто виникнення наративу, канал поширення, суб’єкти, цільова аудиторія, потенційна шкода. На другому визначається ціль реагування, тобто чи необхідно спростувати, пояснити, знизити паніку, не допустити поширення, мобілізувати довіру чи підтримати міжнародну аудиторію. На третьому обираються інструменти, як, наприклад, офіційна заява, фактчекінг, спростування, кризова комунікація, робота з платформою розповсюдження, міжнародне пояснення, виготовлення матеріалів для медіа. На четвертому етапі вимірюється результат, де оцінюється швидкість, охоплення, тональність, зміна наративу, поведінкова реакція, довіра. На п’ятому – робиться корекція і фіксуються висновки\курси дій для майбутніх кейсів.

Для української системи це означає потребу у створенні єдиного аналітичного контуру, де дані від державних органів, громадських ініціатив, платформ, соціологів і міжнародних партнерів не існують окремо, а збираються в спільну картину. Без цього кожен суб’єкт бачить лише власний фрагмент: держава – офіційні загрози, платформи соціальних мереж – поведінку акаунтів,

фактчекери – окремі фейки, соціологи – суспільні настрої, а медіа аналітики – соціальний дискурс. Ефективне оцінювання можливе лише тоді, коли ці фрагменти з’єднуються в єдину аналітику даних.

Отже, оцінювання ефективності контрпропаганди має бути багатовимірним. Воно повинно включати довіру, швидкість реагування, охоплення, зміну наративного середовища, мінімізацію шкоди, стійкість цільових аудиторій, стабільність міжнародної підтримки, якість достовірності та інституційну відтворюваність. Такий підхід дозволяє уникнути поверхневого підрахунку активностей та перейти до реального управління ефективністю контрпропаганди. У контексті російсько-української війни це має особливе значення, тому що інформаційна боротьба є не короткостроковою кампанією, а являється тривалим процесом, від якого залежить стійкість держави, суспільства і міжнародної коаліції підтримки України.

3.5. Рекомендації. Управлінська модель контрпропаганди, процеси реагування, пріоритети та «червоні лінії» легітимності

Формування ефективної системи контрпропаганди в Україні потребує переходу від переважно реактивної моделі до цілісної управлінської архітектури, у межах якої інформаційна безпека розглядається як безперервний цикл – від виявлення загроз до оцінювання ефективності та корекції дій. Такий перехід обумовлений не лише масштабом російського інформаційного впливу, але й його системністю, тому що, як показано у попередніх підрозділах, пропаганда РФ працює через повторювані наративи, багатоканальне поширення та інтеграцію з іншими інструментами гібридної війни. Відповідно, контрпропаганда не може залишатися набором розрізнених дій, вона має стати керованою системою, де кожен елемент виконує функцію в загальній логіці.

Першою ключовою рекомендацією є інституціоналізація єдиного циклу управління інформаційними загрозами. Такий цикл має включати етапи виявлення, класифікації, оцінки ризику, формування відповіді, поширення контрповідомлення, моніторингу ефекту та накопичення уроків\курсів дій або

кейсів. Важливо, що цей цикл не має бути лінійним, він має працювати як замкнена система, де результати попередніх кейсів впливають на майбутні рішення. Як підкреслює Лисенко, стратегічне управління інформаційною безпекою передбачає узгодження всіх елементів системи, а не лише реагування на окремі загрози.[173] Для України це означає, що навіть у кризових умовах необхідно зберігати структурованість процесів, інакше система буде перевантажуватися й втрачати ефективність.

Другим ключовим напрямом є формування стійкої системи стратегічних наративів, яка не змінюється ситуативно, а адаптується до контексту, зберігаючи внутрішню логіку. У попередніх підрозділах було показано, що наративи визначають інтерпретацію подій, а отже їх стабільність є критично важливою. Якщо держава змінює комунікаційні рамки залежно від політичної кон'юнктури, це створює розрив, який може бути використаний противником. Як зазначають у своїй роботі Скрипникова, Тутік та Гринчак, політичні наративи формують когнітивні моделі сприйняття, і їхня нестабільність знижує ефективність комунікації.[174] Отже, рекомендація полягає у тому, щоб визначити обмежену кількість базових наративів, наприклад про суб'єктність України, оборонний характер війни, ціннісний вимір боротьби та міжнародну безпеку та забезпечити їх послідовне відтворення на всіх рівнях комунікації.

Третім елементом є посилення координації між суб'єктами контрпропаганди. Українська модель, як показано у розділі 3.1, є мережевою і включає державні інституції, силові структури, медіа, громадянське суспільство та міжнародних партнерів. Її сила у гнучкості, але слабкість у ризику фрагментації. Тому координація має будуватися не лише як адміністративна функція, а як узгодження смислів і пріоритетів. Це означає створення єдиного

---

[173] Лисенко С.О. Стратегічне управління інформаційною безпекою держави : автореферат дисерт. на здобуття наук. ступ. д.н. з держ. упр. ; спец. 25.00.05 - державне управління у сфері державної безпеки та охорони громадського порядку. Житомирська політехніка. 2025. URL: https://ztu.edu.ua/site/files/1/docs/Університет/Спеціалізовані%20вчені%20ради/14.052.03/2025/ref_Лисенко_С.pdf . (дата звернення: 27.04.2026).

[174] Скрипникова Л.В., Політологія: навчальний посібник. К.: Центр учбової літератури, 2014, 272 с. URL: https://dduvs.edu.ua/biblioteka/biblioteka-studenta-dduvs/pidruchniki-posibniki/politologiya/ (дата звернення: 26.04.2026).

«наративного ядра» або бази, у межах якого різні суб'єкти можуть діяти автономно, але не суперечити один одному. Водночас така координація не повинна перетворюватися на централізацію, що знижує гнучкість і швидкість реагування. Оптимальною є модель, у якій держава визначає рамку, а інші суб'єкти адаптують її до своїх цільових аудиторій.

Четвертим напрямом можна визначити розвиток превентивних інструментів, зокрема пребанкінгу та медіаграмотності. Як було зазначено у розділу 3.2, реактивні інструменти, такі як фактчекінг і дебанкінг, мають обмежену ефективність через часову асиметрію. Тому ключовим завданням є формування стійкості аудиторії до інформаційних впливів. Це включає системні освітні програми, пояснення механізмів маніпуляції, розвиток критичного мислення та формування інформаційної гігієни. Як було визначено раніше, у стані тривалого стресу аудиторія стає більш вразливою до маніпуляцій, що підвищує значення психологічного компоненту інформаційної безпеки.[175] Відповідно, медіаграмотність має включати не лише знання, а й емоційну стійкість. Це можна досягти через системну роботу психологів та фахівців з комунікацій у навчальних закладах в комплексі з впровадженням широких медійних кампаній з медіаграмотності.

П'ятим напрямом рекомендацій являється інтеграція роботи з цифровими платформами в загальну систему контрпропаганди. У сучасному середовищі значна частина дезінформації поширюється через соціальні мережі, месенджери та алгоритмічні новинні стрічки. Це означає, що боротьба з контентом має доповнюватися роботою з інфраструктурою поширення. Дані Meta та звіти Freedom House свідчать, що координаційні мережі можуть бути виявлені та обмежені, але повністю усунути проблему неможливо через її адаптивний характер. Відповідно, рекомендація полягає у створенні постійних каналів

[175] Станчишин В. Емоційні гойдалки війни : роздуми психотерапевта про війну. Вид. 2-ге, допов. Київ : Віхола, 2024, 309 с.

взаємодії з платформами, обміні даними, спільному виявленні загроз та використанні аналітичних інструментів.

Так, прикладом співпраці з цифровими платформами можна відмітити впровадження позначок «Disputed» або «Rated false» («Піддалось втручанню» або «Оцінено як неправдиве») у соціальних мережах Meta, зокрема Facebook, що дало змогу зменшити вплив неправдивого наративу на цільову аудиторію. Згідно з опублікованими результатами оцінки ефективності, після додавання таких позначок у пости, частка людей, як вірили у правдивість фейкового повідомлення зменшилась з 29% (Без втручання) до 19% (позначка «Disputed») та 16% (позначка «Rated false»).[176]

Шостим напрямом можна виділити розвиток аналітичної спроможності системи. Контрпропаганда має базуватися не лише на комунікації, а й на глибокому аналізі великих обсягів даних, тобто меседжів, наративів, трендів. Це включає моніторинг інформаційного простору, аналіз наративів, виявлення патернів поведінки, атрибуцію інформаційно-психологічних спеціальних операцій та, як наслідок, прогнозування їх розвитку. Досвід NATO Strategic Communications Centre of Excellence та RAND Corporation показує, що аналітичний компонент є критичним для ефективності контрпропаганди, оскільки дозволяє переходити від реакції до передбачення. Для нашої країни витікає в необхідність розвитку OSINT-спроможностей, аналітичних та розвідувально-інформаційних центрів, інтеграції даних з різних джерел та створення єдиного аналітичного контуру.

Сьомим напрямом можна охарактеризувати впровадження системи оцінювання ефективності, описаної у розділі 3.4. Без чітких метрик контрпропаганда ризикує залишатися інтуїтивною, а отже, не завжди ефективною та системною. Водночас оцінювання має враховувати складність інформаційного середовища і не зводитися до простих показників. Ключовими

[176] Bryanov, K., & Vziatysheva, V. Determinants of individuals' belief in fake news: A scoping review determinants of belief in fake news.2021. URL:https://doi.org/10.1371/journal.pone.0253717 (дата звернення 01.05.2026).

метриками мають бути довіра, швидкість реагування, зміна наративів, мінімізація шкоди, стійкість аудиторії та міжнародна підтримка. Як показують дослідження European External Action Service(EEAS)[177], інформаційні операції спрямовані на різні аудиторії, а отже і оцінювання їх ефективності має бути багатовимірним.

Окрему увагу слід приділити формуванню «червоних ліній» легітимності контрпропаганди, тобто меж дозволених прийомів та інструментів у арсеналі демократичної держави. У демократичній державі контрпропаганда не може використовувати ті самі методи, що й пропаганда авторитарного типу. Це означає відмову від системної дезінформації, маніпуляції власним населенням, приховування критично важливої інформації без обґрунтування причин, надмірного обмеження свободи слова, тиску на медіа тощо. Як підкреслює В. Ліпкан, національна безпека не може забезпечуватися за рахунок підриву довіри до держави.[178] Тому легітимність є не обмеженням, а умовою ефективності у демократичному суспільстві.

З іншого боку, у воєнних умовах допускається певне обмеження інформації, якщо це прямо пов’язано з національною безпекою. Наприклад, обмеження доступу до інформації про переміщення військ, критичну інфраструктуру або результати ударів є виправданим. Але такі обмеження мають бути пропорційними, тимчасовими і зрозумілими для суспільства через системні роз’яснення у необхідності таких дій. В іншому випадку вони можуть бути інтерпретовані як цензура і використані у пропагандистських цілях противником.

Важливим є також питання довгострокової стійкості системи. Контрпропаганда не може бути лише реакцією на поточну війну. Вона має формувати інституційну пам’ять, накопичувати досвід, розвивати кадри, створювати методології та інтегруватися у систему національної безпеки, і, як

---

[177] 2024 Звіт про діяльність EEAS з протидії іноземним інформаційним маніпуляціям та втручанню (FIMI). 22 серпня 2025. URL: https://www.eeas.europa.eu/eeas/2024-report-eeas-activities-counter-foreign-information-manipulation-and-interference-fimi_en?etrans=uk. (дата звернення: 19.02.2026).

[178] Ліпкан В.А. Національна безпека України : навч. посібник . К. : Кондор, 2008, 552 с.

наслідок, у систему колективної безпеки країн Заходу. Це означає, що навіть після завершення активної фази війни система має зберегти свою функціональність, оскільки інформаційні загрози не зникнуть, а лише трансформуються під впливом політичної кон'юктури.

Таким чином, можна сказати, що ефективна модель контрпропаганди для України має базуватися на поєднанні стратегічного управління, розгалуженої мережевої взаємодії, аналітичної спроможності держави, превентивних інструментів, роботи з цифровими та медіа-платформами, та чітких принципів легітимності. Вона має бути гнучкою, але узгодженою, швидкою, але доказовою, жорсткою до ворожого впливу, але обережною щодо власного суспільства. Саме така модель дозволяє не лише протидіяти російській пропаганді, а й формувати довгострокову стійкість держави та суспільства, забезпечуючи одну з найважливіших частин національної безпеки України.

Висновки до Розділу 3

У даному розділі нами було проаналізовано контрпропаганду України та її партнерів як систему інституційних, комунікаційних, аналітичних і практичних заходів, спрямованих на протидію російським інформаційним впливам. Зміст розділу показує, що ефективна контрпропаганда не може обмежуватися реактивним спростуванням фейків, а повинна функціонувати як комплексна управлінська система. Водночас було визначено, що основною проблемою залишається не сама відсутність інституцій, а питання координації, розподілу компетенцій, швидкості реагування, сталість процедур і здатність перетворювати окремі успішні практики на відтворювану систему, щоб покривати функції, покладені на неї як на елемент національної безпеки. Особливу увагу в даному розділі було приділено інструментам контрпропаганди, а також проаналізовано їх обмеження. У цьому розділі також обґрунтовано значення західних підходів, зокрема рамок EEAS/FIMI, NATO StratCom, Hybrid CoE та RAND. Водночас показано, що механічне перенесення цих підходів в український контекст є

недостатнім, оскільки Україна перебуває не лише в умовах інформаційного впливу, а в умовах повномасштабної війни, де інформаційна протидія безпосередньо пов’язана з виживанням держави.

Окремим результатом розділу стало визначення критеріїв оцінювання ефективності контрпропаганди. Було доведено, що її не можна вимірювати лише кількістю спростувань, публікацій або охопленням повідомлень. Доцільно враховувати швидкість реагування, узгодженість повідомлень, рівень довіри, зменшення шкоди, зміну наративного середовища, стійкість цільових аудиторій, якість координації, стабільність міжнародної підтримки та інституційну відтворюваність.

Отже, в рамках розділу було можна вважати доведеним, що ефективна система контрпропаганди України має будуватися на поєднанні інституційної координації, стратегічних комунікацій, аналітики даних, правових і етичних обмежень, співпраці з партнерами та постійного вимірювання результатів. Її головною метою має бути не лише нейтралізація окремих ворожих повідомлень, а збереження довіри, стійкості, керованості держави та здатності суспільства протистояти тривалому інформаційному тиску. Саме тому контрпропаганда повинна залишатися легітимною, правдивою, процедурною та орієнтованою на зменшення шкоди, а не на віддзеркалення методів держави-агресора.

ВИСНОВКИ

Проведене дослідження дозволяє зробити висновок, що в умовах сучасної російсько-української війни пропаганда та контрпропаганда остаточно трансформувалися з допоміжного інструменту політичного впливу у окремий стратегічний вимір ведення війни. Російсько-українська війна продемонструвала, що інформаційне середовище більше не виконує лише функцію супроводу воєнних дій або медійного відображення конфлікту. Натомість, інформаційний простір став окремим середовищем боротьби, у межах якого здійснюється вплив на політичні рішення, міжнародну підтримку, психологічний стан населення, рівень довіри до державних інституцій, мобілізаційні процеси та загальну стійкість суспільства. Саме тому сучасна війна має не лише військовий чи політичний, але й виразний когнітивний характер, оскільки боротьба ведеться за формування уявлень, інтерпретацій та моделей сприйняття реальності.

У ході даного дослідження було встановлено, що сучасна пропаганда суттєво відрізняється від класичних моделей інформаційного впливу XX століття. Якщо традиційна пропаганда функціонувала переважно через централізоване поширення ідеологічних повідомлень у межах контрольованих державою каналів комунікації, то сучасні інформаційні операції мають значно складнішу структуру. Вони поєднують цифрові технології, алгоритмічне просування контенту, мережеві моделі поширення інформації, психологічний вплив, маніпулятивні практики, використання емоційних тригерів та елементи когнітивного впливу. Це означає, що сучасна пропаганда повинна розглядатися не як окреме повідомлення або сукупність фейків, а як цілісна система формування необхідної противнику картини реальності.

Теоретичний аналіз дозволив уточнити та систематизувати понятійний апарат дослідження. Так, завдяки ньому було встановлено, що поняття «пропаганда», «дезінформація», «маніпуляція», «інформаційно-психологічна

операція», «стратегічні комунікації» та «контрпропаганда» перебувають у тісному взаємозв'язку, однак не є тотожними. Особливого значення набуває розмежування між контрпропагандою та дзеркальною пропагандою. У межах даного дослідження контрпропаганда розглядається як комплексна система захисту інформаційного простору держави та суспільства, спрямована на нейтралізацію деструктивного інформаційного впливу, зниження ефективності ворожих наративів та формування довгострокової стійкості аудиторії. Таким чином, контрпропаганда не повинна ототожнюватися з маніпулятивним інформаційним впливом, оскільки її ключовим завданням є захист інформаційної безпеки та підтримання стійкості демократичних інституцій.

У ході дослідження було доведено, що російська пропаганда у контексті війни проти України має системний характер та є складовою ширшої концепції гібридної війни. російська федерація використовує інформаційний вплив як інструмент досягнення стратегічних політичних і військових цілей. Основними напрямами такого впливу стали делегітимізація української державності, підрив довіри до української влади, деморалізація населення та військових, вплив на міжнародну підтримку України та створення атмосфери невизначеності й інформаційного хаосу. Аналіз кейсів, пов'язаних із кампаніями про «біолабораторії США в Україні», подіями у Бучі, інформаційними операціями навколо енергетичної інфраструктури України, а також наративами про «втому Заходу від війни» та маніпуляціями навколо зернової угоди, дозволив встановити, що російська пропаганда базується на багаторазовому повторенні емоційно навантажених повідомлень через велику кількість каналів поширення.

Важливим висновком дослідження можна виокремити визначення ключових особливостей російської інформаційної моделі. По-перше, вона характеризується високим рівнем адаптивності. Російські інформаційні операції швидко змінюють акценти залежно від ситуації на фронті, міжнародної реакції та змін інформаційного середовища. По-друге, російська пропаганда активно використовує емоційний компонент як основний механізм впливу. Страх,

тривога, невизначеність, паніка, недовіра та емоційна втома виступають основними психологічними тригерами, через які здійснюється маніпулятивний вплив на аудиторію. По-третє, важливою особливістю російської моделі є використання цифрової інфраструктури як механізму масштабування інформаційного впливу. Соціальні мережі, Telegram-канали, ботоферми, псевдо медіа-ресурси та алгоритмічне просування контенту дозволяють забезпечувати високу швидкість поширення дезінформації та суттєво ускладнюють протидію їй.

Дослідження показало, що окреме місце у російській інформаційній стратегії займають інформаційно-психологічні спеціальні операції, спрямовані на дестабілізацію внутрішньої ситуації в Україні. Особливу роль у цьому відіграють кампанії, пов’язані з темами мобілізації, втрат, економічної кризи, енергетичної безпеки та міжнародної підтримки України. Аналіз інформаційних атак показав, що російські ІПСО часто орієнтуються не на переконання аудиторії у конкретній тезі, а на створення атмосфери недовіри, хаосу та інформаційного перевантаження. Таким чином, головною метою сучасних інформаційних операцій дедалі частіше стає не формування чіткої політичної позиції, а руйнування здатності аудиторії адекватно оцінювати інформацію та приймати раціональні рішення.

В даній роботі увагу також було приділено аналізу української системи контрпропаганди. У ході дослідження було встановлено, що українська модель протидії інформаційним загрозам сформувалася як гібридна мережа, яка поєднує державні інституції, громадянське суспільство, незалежні медіа, міжнародних партнерів, волонтерські ініціативи та аналітичні спільноти. На відміну від жорстко централізованих моделей, українська система демонструє високий рівень розгалуженості та адаптивності. Саме ця гнучкість стала одним із ключових факторів ефективності української інформаційної протидії у перші місяці повномасштабного вторгнення.

Проведений аналіз дозволяє стверджувати, що важливу роль у системі української контрпропаганди відіграють стратегічні комунікації. Україна змогла сформувати низку ключових наративів, які забезпечили підтримку як всередині держави, так і на міжнародному рівні. До них належать наративи про боротьбу за свободу, оборонний характер війни, захист демократичних цінностей та право України на суб'єктність. Важливим фактором ефективності цих наративів стало те, що вони підкріплювалися реальними подіями, а отже мали високий рівень довіри та сприймалися як автентичні.

Дослідження також показує неможливість контрпропаганді існувати без кризових комунікацій. Приклади інформаційних кампаній навколо ударів по енергетичній інфраструктурі України продемонстрували, що регулярна, зрозуміла та послідовна комунікація здатна суттєво знижувати рівень паніки та підтримувати психологічну стійкість населення навіть в умовах масштабних криз. Аналогічно, швидка реакція України на російські інформаційні операції навколо подій у Бучі дозволила не лише нейтралізувати спроби дискредитації доказів воєнних злочинів, але й сформувати міжнародний дискурс про відповідальність Російської Федерації за порушення міжнародного гуманітарного права.

У межах дослідження було встановлено те, що важливим елементом сучасної контрпропаганди є також дебанкінг та пребанкінг. Просте спростування фейкової інформації виявляється недостатньо ефективним у ситуації, коли дезінформаційний наратив уже встиг поширитися та закріпитися у свідомості аудиторії. Ефективний дебанкінг повинен включати швидкість реагування, високий рівень довіри до джерела, пояснення механізмів маніпуляції, використання різних каналів комунікації та інтеграцію у ширшу систему стратегічних комунікацій. Водночас пребанкінг, тобто попереднє пояснення механізмів маніпулятивного впливу до початку інформаційної атаки, поступово набуває дедалі більшого значення як інструмент довгострокового формування стійкості аудиторії.

Проведене дослідження дозволило також визначити, що західні підходи до протидії дезінформації та інформаційним операціям зазнають поступової трансформації під впливом російсько-української війни. Особливе значення у цьому контексті має концепція FIMI (Foreign Information Manipulation and Interference), яка використовується у країнах Європейського Союзу. Її перевага полягає у тому, що вона дозволяє розглядати інформаційні операції не як ізольовані фейки, а як комплексні кампанії впливу, які поєднують цифрові платформи, інформаційні мережі, дипломатичні заяви, медійні ресурси та політичні наративи.

Ще одним показовим висновком даної роботи стало те, що український досвід суттєво вплинув на розвиток сучасних західних підходів до інформаційної безпеки. Практичні кейси російсько-української війни стали важливим джерелом для розвитку методик аналізу інформаційних операцій, кризових комунікацій та стратегічних комунікацій у структурах ЄС і НАТО. Водночас дослідження показало, що механічне перенесення західних моделей в українські умови є недостатньо ефективним. Україна функціонує в умовах значно вищої інтенсивності інформаційного протистояння, що потребує швидших, менш бюрократизованих та більш адаптивних моделей реагування.

Одним із ключових результатів дослідження можна вважати виявлення проблеми оцінювання ефективності контрпропаганди. Було встановлено, що традиційні кількісні показники, такі як кількість спростувань, кількість інформаційних повідомлень або загальне охоплення аудиторії, не дозволяють повноцінно оцінити реальний вплив контрпропагандистських заходів. У сучасних умовах значно важливішими стають якісні показники, а саме рівень суспільної довіри, психологічна стійкість аудиторії, зміни поведінкових реакцій, рівень адаптивності системи та здатність держави знижувати вплив ворожих наративів.

У процесі дослідження було встановлено, що проблема оцінювання ефективності контрпропаганди безпосередньо пов’язана з необхідністю створення нових методик збору та аналізу даних. Сучасна система інформаційної безпеки потребує використання міждисциплінарних підходів, які поєднуватимуть OSINT-аналітику, аналіз соціальних мереж, поведінкові моделі, когнітивну аналітику, цифровий моніторинг та інструменти аналізу інформаційних наративів. Саме комплексний аналіз поведінки аудиторій та змін інформаційного середовища дозволяє оцінювати не лише кількість інформаційних впливів, але і їх реальний психологічний та соціальний ефект.

В даному контексті особливого значення набуває проблема формування системи якісних KPI у сфері стратегічних комунікацій та інформаційної безпеки. У сучасних умовах недостатнім є використання виключно формальних кількісних показників інформаційної активності. Ефективність контрпропаганди повинна оцінюватися через комплекс якісних критеріїв, які включатимуть рівень довіри до державних інституцій, рівень стійкості суспільства до дезінформації, швидкість реагування на інформаційні атаки, рівень поширення деструктивних наративів, зміни поведінкових моделей аудиторії та стабільність інформаційного середовища держави. Саме такий підхід дозволяє перейти від формального оцінювання інформаційної активності до реального аналізу ефективності інформаційної безпеки.

Проведене дослідження дозволяє зробити висновок, що пропаганда та контрпропаганда в умовах сучасної російсько-української війни потребують формування комплексного підходу до інституціалізації відповідної діяльності. Йдеться не лише про створення окремих механізмів реагування на інформаційні загрози, але й про побудову цілісної системи стратегічних комунікацій, координації державних інституцій, громадянського суспільства, медійного сектору та міжнародних партнерів. Водночас особливого значення набуває створення системи якісного оцінювання ефективності контрпропагандистської діяльності через поєднання кількісних та якісних показників, використання

сучасних методик збору та аналітики даних, а також впровадження нових моделей аналізу поведінкових і когнітивних змін у суспільстві.

Отже, підсумовуючи викладені вище висновки, можна сказати, що результати проведеного дослідження підтверджують, що інформаційна стійкість суспільства є одним із ключових елементів сучасної національної безпеки. Російсько-українська війна продемонструвала, що боротьба за інформаційний простір є не менш важливою, ніж боротьба на полі бою. Саме тому ефективна система контрпропаганди повинна розглядатися як постійно діючий елемент державної безпекової політики, інтегрований у систему стратегічних комунікацій, національної стійкості та інформаційної безпеки держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ І ЛІТЕРАТУРИ

1. Андрієнко С. С. Психологічна підготовка та підтримка співробітників правоохоронних органів в умовах гібридної війни. Економіка, управління та адміністрування. 2025. URL: https://doi.org/10.26642/ema-

2. Гаращук Д., Сергєєв В. Інфодемія та популізм у цифрову епоху: загрози політичній стабільності та безпекові виклики. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2025-2(8)-61-71.

3. Герасимюк К. Х. Механізми державного управління кібер- та інформаційною безпекою: проблеми та шляхи вирішення. Економіка, управління та адміністрування. Жовтень 2021. URL: https://www.researchgate.net/publication/356396763_Mehanizmi_derzavnogo_upravlinna_kiber-_ta_informacijnou_bezpekou_problemi_ta_slahi_virisenna.

4. Гольцов А. Г. Геополітика та політична географія : підручник. Київ : ЦУЛ, 2021. 416 с.

5. Загурська-Антонюк В., Загурський В. Транзитивність політичної свідомості українців в умовах російсько-української війни. Society and Security. 2024. URL: https://doi.org/10.26642/sas-2024-1(2)-40-45.

6. Звіт Міністерства культури та інформаційної політики України за 2023 рік щодо виконання Плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року. Лютий 2026. URL: https://mincult.gov.ua/wp-content/uploads/2025/01/zvit-shhodo-vykonannya-planu-zahodiv-z-realizacziyi-strategiyi-informaczijnoyi-bezpeky-za-2023-rik.pdf.

7. Звіт про діяльність EEAS з протидії іноземним інформаційним маніпуляціям та втручанню – 2024 (FIMI). 22 серпня 2025. URL: https://www.eeas.europa.eu/eeas/2024-report-eeas-activities-counter-foreign-information-manipulation-and-interference-fimi_en?etrans=uk.

8. Згуровський М. З., Ланде Д. В., Болдак А. О., Єфремов К. В., Перестюк М. М. Лінгвістичний аналіз даних інтернет-медіа та соціальних мереж

у задачах оцінювання суспільних перетворень. Кібернетика та системний аналіз. 2021. URL: http://jnas.nbuv.gov.ua/article/UJRN-0001221023.

9. Канцір В., Олійник Х. Іноземний досвід регламентації кримінальної відповідальності за пропаганду, планування, підготовку, розв'язування та ведення агресивної війни. Вісник Національного університету «Львівська політехніка». 2020. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2020/may/21542/32.pdf.

10. Корнійчук Л., Матвійчук Н. Інформаційна політика Чеської Республіки як інструмент забезпечення інформаційної безпеки під впливом російсько-української війни. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2025-5(11)-19-25.

11. Ліпкан В. А. Національна безпека України : навч. посібник. Київ : Кондор, 2008. 552 с.

12. Лісовський П. М. Безпекознавство: особистість, держава, суспільство : навч. посібник. Київ : Кондор, 2017. 368 с.

13. Лисенко С. О. Стратегічне управління інформаційною безпекою держави : автореферат дисертації на здобуття наук. ступ. д-ра наук з держ. упр.; спец. 25.00.05 – державне управління у сфері державної безпеки та охорони громадського порядку. Житомирська політехніка. 2025. URL: https://ztu.edu.ua/site/files/1/docs/Університет/Спеціалізовані%20вчені%20ради/14.052.03/2025/ref_Лисенко_С.pdf.

14. Мосієнко О., Гордійчук О., Клименко І., Кондратюк Ю. Національна безпека; національні інтереси; глобалізація; глобалізаційні виклики. Society and Security. 2024. URL: https://library.ztu.edu.ua/e-copies/sas/2-3(3)/98.pdf.

15. Наторіна А. О. Синкретичність менеджменту цифрових ризиків та інформаційної безпеки. 27 листопада 2019. URL: https://ema.ztu.edu.ua/article/view/185089.

16. Носенко С., Яковлєв М. Трансформація стримування в контексті російсько-української війни: концептуалізація поняття крізь призму становлення

України як середньої держави. Society and Security. 2025. URL: https://sas.ztu.edu.ua/article/view/323957/314626.

17. Потій О. В., Горбенко Ю. І., Замула О. А., Ісірова К. В. Аналіз методів оцінки і управління ризиками кібер- і інформаційної безпеки. 2021. URL: https://duikt.edu.ua/uploads/l_1066_72351971.pdf.

18. Пропаганда та дезінформація: що найбільше впливає на український інфопростір. Національна спілка журналістів України. 25 грудня 2024. URL: https://nsju.org/novini/propaganda-ta-dezinformacziya-shho-najbilshe-vplyvaye-na-ukrayinskyj-infoprostir/.

19. Рустецький Л., Янковський В. (ред.). Російська дезінформація в добу технологічної революції: штучний інтелект, нові наративи та протидія. Чорне Небо; StopFake.org. 2025. URL: https://www.stopfake.org/content/uploads/2025/12/PDF_CNSF_Rosiyska_dezinformatsiya_v_dobu_tekhnolohichnoyi_revolyutsiyi.pdf.

20. Сащук Г. М. Еволюція стратегічних комунікацій сектору безпеки та оборони України як інструменту протидії інформаційним загрозам. Київський національний університет імені Тараса Шевченка. 2025. URL: https://jpl.donnu.edu.ua/article/view/17920/17812.

21. Скрипникова Л. В. Політологія : навчальний посібник. Київ : Центр учбової літератури, 2014. 272 с. URL: https://dduvs.edu.ua/biblioteka/biblioteka-studenta-dduvs/pidruchniki-posibniki/politologiya/.

22. Станчишин В. Емоційні гойдалки війни : роздуми психотерапевта про війну. Вид. 2-ге, допов. Київ : Віхола, 2024. 309 с.

23. Сумін П. Інформаційні технології як інструмент забезпечення національної безпеки на сучасному етапі розвитку: проблеми та перспективи. Society and Security. 2025. URL: https://doi.org/10.26642/sas-2024-6(6)-37-43.

24. Указ Президента України № 685/2021 «Про рішення Ради національної безпеки і оборони України “Про Стратегію інформаційної безпеки”». 2021. URL: https://zakon.rada.gov.ua/laws/main/685/2021.

25. Фасій Б. Національна безпека та захист персональних даних в епоху цифрових технологій. Society and Security. 2024. URL: https://doi.org/10.26642/sas-2024-6(6)-76-82.

26. Яковлєв П. Правовий режим державної мови у сфері забезпечення інформаційної безпеки. Підприємництво, господарство і право. 2020. № 3. URL: https://pgp-journal.kiev.ua/archive/2020/3/33.pdf.

27. 3rd EEAS Report on Foreign Information Manipulation and Interference Threats. March 2025. URL: https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf.

28. Bryanov K., Vziatysheva V. Determinants of individuals' belief in fake news: A scoping review. 2021. URL: https://doi.org/10.1371/journal.pone.0253717.

29. Buziashvili E., Châtelet V. Another battlefield: Telegram as a digital front in Russia's war against Ukraine. DFRLab. 2024. URL: https://dfrlab.org/wp-content/uploads/sites/3/2024/06/DFRLab_Russian_Telegram_2024.pdf.

30. Deprez F. Ukrainians rally around Zelenskyy after bruising Trump encounter. Financial Times. 23 March 2025. URL: https://www.ft.com/content/8649ba24-9801-4063-bcf1-6364c1185c46.

31. Dikhtiarenko S., Heap B., Pamment J., Smith V. Attributing Russian Information Influence Operations: Testing the Information Influence Attribution Framework with real-world case studies. Riga : NATO Strategic Communications Centre of Excellence, 12 February 2026. URL: https://stratcomcoe.org/publications/attributing-russian-information-influence-operations-testing-the-information-influence-attribution-framework-with-real-world-case-studies/340.

32. European Commission. The Digital Services Act. 2026. URL: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act.

33. Freedom House. Key Developments, June 1, 2023 – May 31, 2024. 2024. URL: https://freedomhouse.org/country/ukraine/freedom-net/2024.

34. Helmus T. C., Holynska K. Ukrainian Resistance to Russian Disinformation: Lessons for Future Conflict. Santa Monica, CA : RAND Corporation, 2024. URL: https://www.rand.org/pubs/research_reports/RRA2771-1.html.

35. Hunder M. Russia vs Ukraine: the biggest war of the fake news era. Reuters. 31 July 2024. URL: https://www.reuters.com/world/europe/russia-vs-ukraine-biggest-war-fake-news-era-2024-07-31/.

36. Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI). EEAS. 17 March 2026. URL: https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en.

37. Kalenský J., Hanhijärvi H. Countering disinformation in the Euro-Atlantic: Strengths and gaps. Hybrid CoE Research Report 15. September 2025. URL: https://www.hybridcoe.fi/wp-content/uploads/2025/10/Hybrid_CoE_Research_Report_15_Countering_disinformation_Euro_Atlantic.pdf.

38. Krastev I., Leonard M. Peace versus Justice: The coming European split over the war in Ukraine. European Council on Foreign Relations. 2022. URL: https://ecfr.eu/publication/peace-versus-justice-the-coming-european-split-over-the-war-in-ukraine/.

39. Lewandowsky S., Cook J., Ecker U. K. H., Albarracín D., Amazeen M. A., Kendeou P., Lombardi D., Newman E. J., Pennycook G., Porter E., Rand D. G., Rapp D. N., Reifler J., Roozenbeek J., Schmid P., Seifert C. M., Sinatra G. M., Swire-Thompson B., van der Linden S., Vraga E. K., Wood T. J., Zaragoza M. S. The Debunking Handbook 2020. 2020. URL: https://skepticalscience.com/docs/DebunkingHandbook2020-Ukranian.pdf.

40. Maristany de las Casas P. Investigation | Talking points: When chatbots surface Russian state media. ISD. 27 October 2025. URL: https://www.isdglobal.org/digital-dispatch/investigation-talking-points-when-chatbots-surface-russian-state-media/.

41. Nimmo B., Torrey M. Adversarial Threat Report. Meta Quarterly Adversarial Threat Report Q2 2023. 2023. URL: https://transparency.meta.com/sr/Q2-2023-Adversarial-threat-report/.

42. OpenAI has stopped five attempts to misuse its AI for "deceptive activity". 30 May 2024. URL: https://www.reuters.com/technology/cybersecurity/openai-has-stopped-five-attempts-misuse-its-ai-deceptive-activity-2024-05-30.

43. Treyger E., Williams H. J., D'Arrigo A. Measuring the Reach of Russia's Propaganda in the Russia-Ukraine War. RAND Corporation. 23 May 2025. URL: https://www.rand.org/pubs/research_briefs/RBA3450-2.html.

44. Ukraine: Russian Forces' Trail of Death in Bucha. Human Rights Watch. 2022. URL: https://www.hrw.org/news/2022/04/21/ukraine-russian-forces-trail-death-bucha.

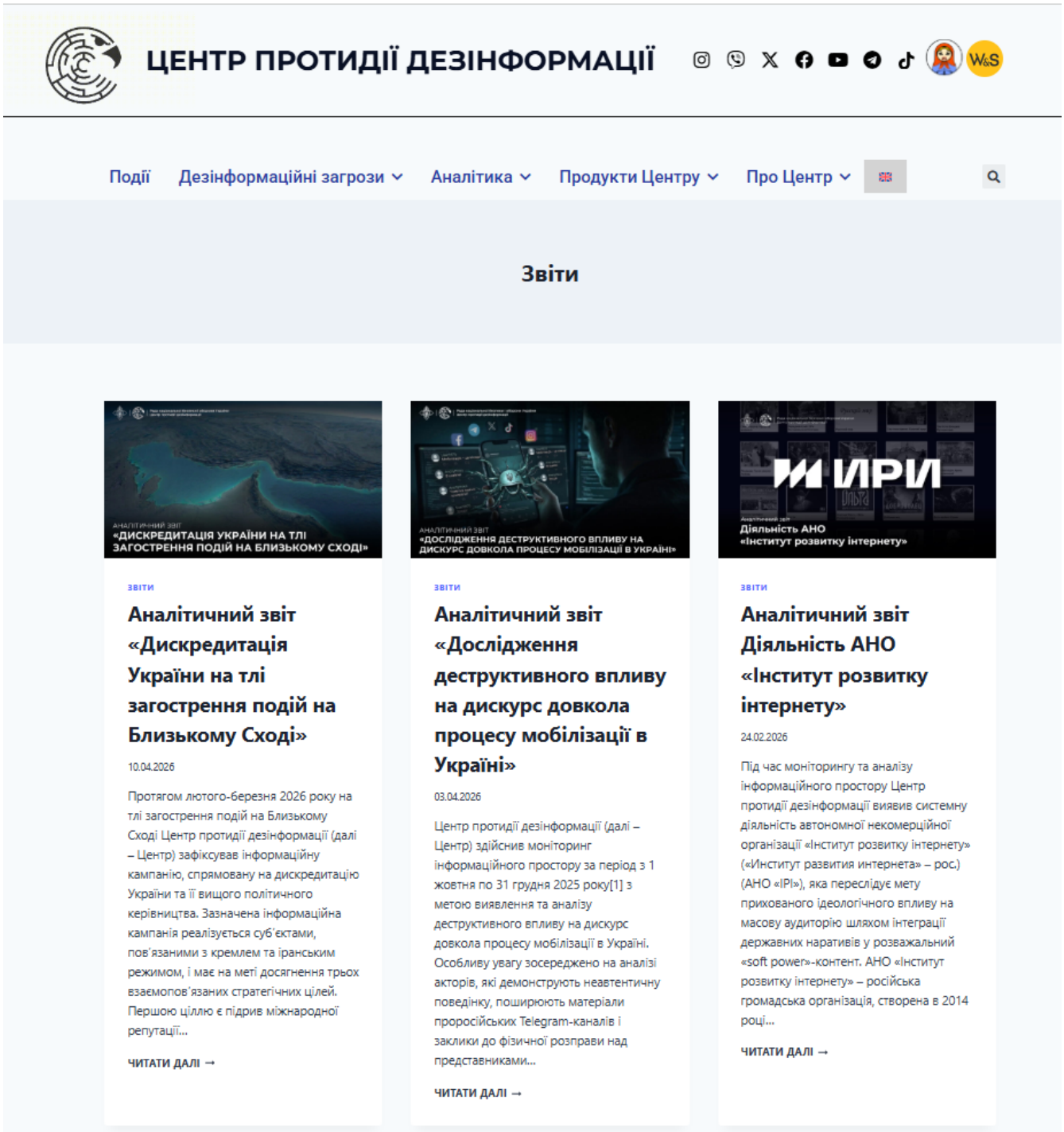
45. United Nations. Not Aware of Any Biological Weapons Programmes, Disarmament Chief Affirms as Security Council Meets to Address Related Concerns in Ukraine. SC/14827. 2022. URL: https://press.un.org/en/2022/sc14827.doc.htm.

46. Wack M., Duskin K., Hodel D. Political Fact-Checking Efforts are Constrained by Deficiencies in Coverage, Speed, and Reach. 19 December 2024. URL: https://arxiv.org/pdf/2412.13280.

ДОДАТКИ

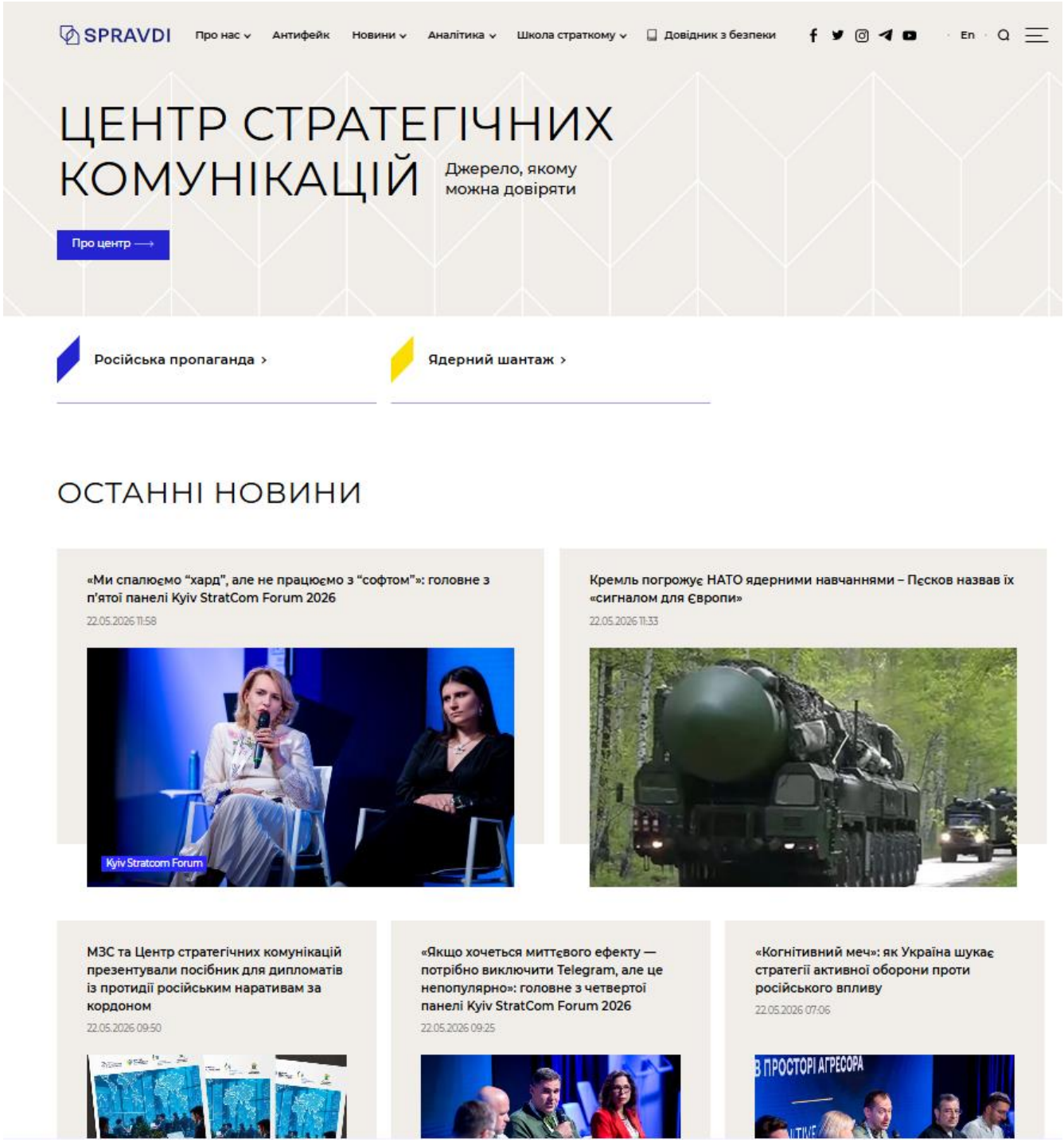
Додаток А

Веб-сайт Центру протидії дезінформації CPD.GOV.UA



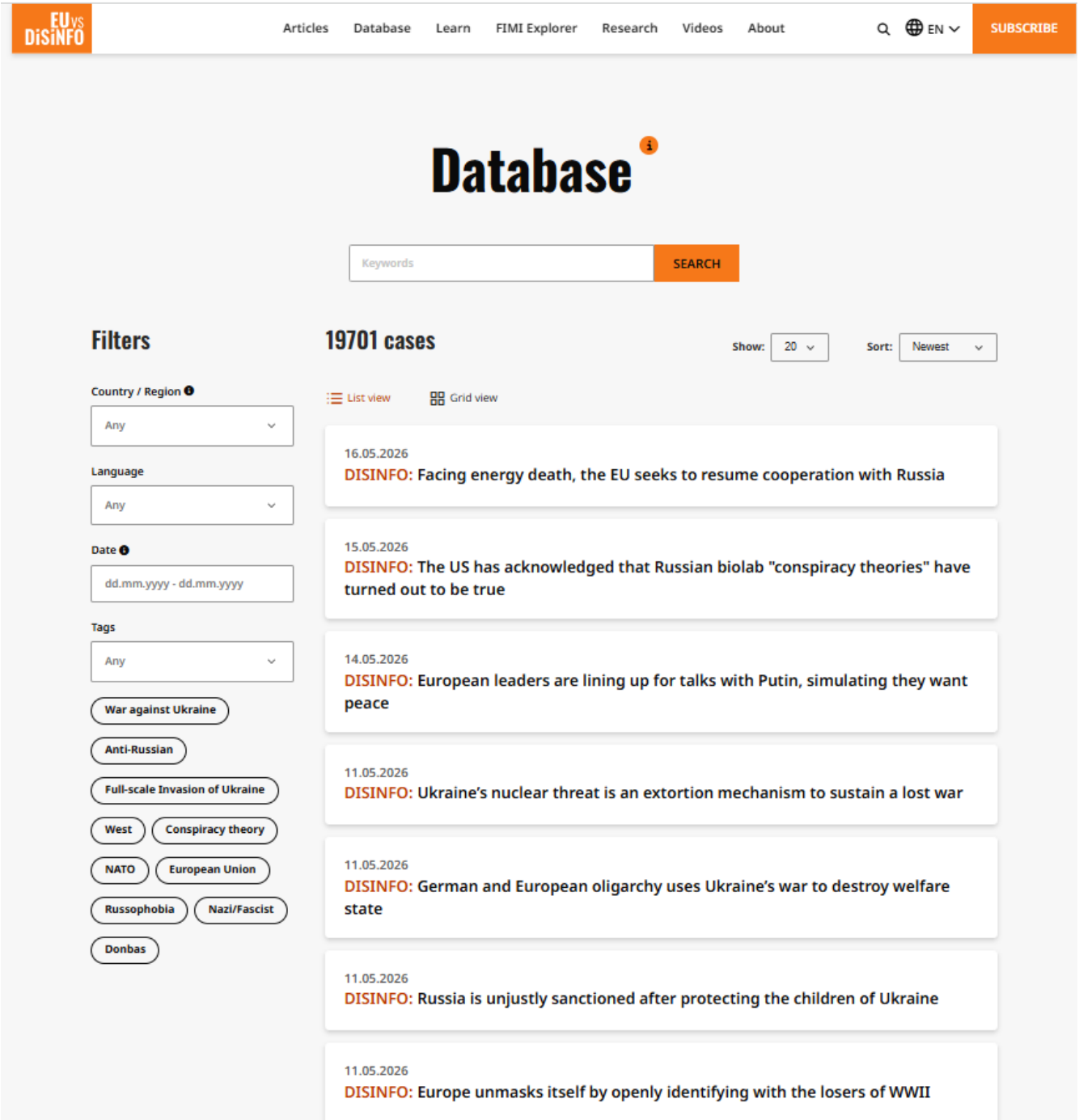
Додаток Б

Веб-сайт Центру стратегічних комунікацій SPRAVDI.ORG



Додаток В

Веб-сайт Європейської фактчекінг бази EUvsDISinfo.EU



Додаток Г

Веб-сайт Дипломатичної служби Європейського союзу EEAS.europa.eu