

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОСТРОЗЬКА АКАДЕМІЯ»
Навчально-науковий інститут міжнародних відносин та національної безпеки
Кафедра інформаційно-документних комунікацій

ЗАТВЕРДЖУЮ
на засіданні кафедри
інформаційно-документних комунікацій
(протокол № __ від _____ 2025 р.)
Завідувач кафедри _____ Ганна ОХРІМЕНКО

Кваліфікаційна робота
на здобуття освітнього рівня магістра
на тему: **«СИСТЕМА МЕТОДІВ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ У
КОНТЕКСТІ РОСІЙСЬКОЇ АГРЕСІЇ ПРОТИ УКРАЇНИ:
МІЖНАРОДНИЙ АСПЕКТ»**

Виконала здобувачка групи МІнс-21
освітньо-професійної програми
«Інформаційна аналітика та комунікативний менеджмент»
Моїсєєва Валерія Костянтинівна

Керівник – доктор філософії (PhD),
ст. викладач кафедри
інформаційно-документних комунікацій
ФЕДУРЮК Олеся Михайлівна
Рецензент – кандидат наук із соціальних
комунікацій, завідувач кафедри інформаційної
діяльності Маріупольського державного
університету
В'ячеслав КУДЛАЙ

Острого, 2025

**Графік
виконання кваліфікаційної (дипломної) роботи на другому
(магістерському) рівні вищої освіти**

№ з/н	Види й етапи роботи	Термін виконання	Підпис наукового керівника
1	Вибір теми, закріплення її на кафедрі та визначення наукового керівника	Жовтень 2024 р.	
2	Складання графіка роботи над темою і узгодження його з науковим керівником	Листопад 2024 р.	
3	Вивчення джерел, літератури, суспільних реалій, матеріалів архіву, періодичних видань; збір та узгодження фактів, даних	Листопад-грудень 2024 р.	
4	Складання плану кваліфікаційної роботи й узгодження його з науковим керівником	Січень 2025 р.	
5	Формування концепції, написання вступу й теоретичного розділу роботи	Лютий-березень 2025 р.	
6	Завершення рукопису кваліфікаційної (дипломної) роботи та ознайомлення наукового керівника з її першим варіантом	Жовтень 2025 р.	
7	Повне завершення кваліфікаційної (дипломної) роботи, оформлення її та подання на відгук наукового керівника	Листопад 2025 р.	
8	Подання роботи на кафедру	Грудень 2025 р.	
9	Проведення попереднього захисту	21 листопада 2025 р.	
10	Подання рецензії на кафедру	18 грудня 2025 р.	
11	Захист кваліфікаційної роботи	23 грудня 2025 р.	

Здобувач другого (магістерського)
рівня вищої освіти _____ Валерія МОІСЄЄВА

Науковий керівник _____ Олеся ФЕДОРУК

ЗМІСТ

ВСТУП	4
РОЗДІЛ 1 ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ	
ДОСЛІДЖЕННЯ	9
1.1. Сутність та види дезінформації: теоретичний аспект	9
1.2. Нормативно-правове забезпечення протидії дезінформації	15
Висновки до першого розділу	21
РОЗДІЛ 2 АНАЛІЗ РОСІЙСЬКОЇ ДЕЗІНФОРМАЦІЇ У КОНТЕКСТІ	
ГІБРИДНОЇ АГРЕСІЇ ПРОТИ УКРАЇНИ	24
2.1. Аналіз російської дезінформаційної кампанії	24
2.2. Функціонування системи протидії дезінформації в Україні в контексті сучасної інформаційної війни	33
Висновки до другого розділу	46
РОЗДІЛ 3 ОСОБЛИВОСТІ МІЖНАРОДНОГО ДОСВІДУ У	
ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ	48
3.1. Архітектура протидії дезінформації у міжнародній практиці	48
3.2. Перспективи вдосконалення системи протидії дезінформації в Україні (на основі міжнародного досвіду).....	55
Висновки до третього розділу	60
ВИСНОВКИ	63
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	67
ДОДАТКИ	73

ВСТУП

Сьогодні проблема дезінформації в Україні тісно пов'язана з питаннями національної безпеки, демократичного розвитку, суспільної єдності та ефективної комунікації держави з громадянами. Розробка ефективної системи методів протидії дезінформації є важливою не лише для захисту українського інформаційного простору, але й для формування стійкої європейської та міжнародної безпекової архітектури.

Актуальність теми дослідження. Зумовлюється низкою ключових факторів, що визначають сучасний характер інформаційних загроз та потребу в ефективних механізмах їх подолання. Насамперед йдеться про гібридну війну Російської Федерації, для якої інформаційні операції стали системним і стратегічним інструментом впливу на Україну та міжнародну спільноту. В умовах війни дезінформаційні кампанії супроводжують практично всі політичні, соціальні й військові процеси, спрямовуючи свої зусилля на підризу довіри до державних інституцій, послаблення єдності суспільства та створення викривлених інтерпретацій подій.

Додаткової актуальності проблемі надає зміна природи сучасних інформаційних загроз. Дезінформація активно адаптується до цифрових технологій, алгоритмічних систем, соціальних мереж, месенджерів та інструментів таргетованої комунікації. Це значно ускладнює її виявлення, сприяє швидкому розповсюдженню та збільшує її руйнівний потенціал.

У цих умовах виникає необхідність розбудови ефективних державних і суспільних механізмів інформаційної стійкості, що включають розвиток нормативно-правової бази, посилення інституційної координації, вдосконалення стратегічних комунікацій, підтримку просвітницьких програм та системне підвищення рівня медіаграмотності громадян.

Важливим чинником актуальності є й міжнародний характер дезінформації. Оскільки її наслідки виходять за межі окремої держави, ефективна протидія потребує міждержавної взаємодії, обміну досвідом,

вироблення узгоджених стандартів реагування та спільних стратегій інформаційної безпеки.

Окрему роль відіграє зростання впливу цифрових платформ, які перетворилися на основні канали поширення фейкових повідомлень, пропаганди, маніпуляцій і психологічних операцій. Їхня глобальність, алгоритмічність та швидкість розповсюдження інформації створюють нові виклики, що вимагають комплексних і технологічно адаптованих підходів до протидії.

Отже, обрана тема є своєчасною, суспільно значущою, практично орієнтованою та має важливе значення для подальшого наукового осмислення інформаційних загроз і механізмів їх нейтралізації.

Стан наукової розробки теми. Проблематика дезінформації, стратегічних комунікацій та інформаційної безпеки на сучасному етапі характеризується високим рівнем наукової розробленості та міждисциплінарного осмислення. Теоретико-методологічні засади дослідження сформовано у працях українських і зарубіжних науковців, зокрема Г. Почепцова [12], В. Капелюшного [6], В. Шлапаченка [25], Л. Компанцевої [1], а також L. Floridi [35], який одним із перших концептуалізував інтернет як середовище поширення дезінформації та «супермагістраль» інформаційних викривлень. Вагомий внесок у розвиток понятійно-категоріального апарату зроблено в межах підходів НАТО [10] та Європейського Союзу [34] до стратегічних комунікацій і протидії інформаційним загрозам, що забезпечує стандартизацію термінології та формування спільних аналітичних рамок.

Окреме місце у науковій літературі посідає міждисциплінарна модель «інформаційного безладу», запропонована С. Wardle та Н. Derakhshan [59], яка дозволяє комплексно аналізувати дезінформацію у взаємозв'язку з політичними, соціальними й технологічними чинниками. Значний масив досліджень і аналітичних матеріалів присвячено інституційним та нормативно-правовим механізмам протидії дезінформації на національному й наднаціональному рівнях, зокрема в документах ЄС [34, 48, 51, 53, 54] та України [13, 14, 15, 16,

17, 20], а також у діяльності спеціалізованих аналітичних центрів і фактчекінгових ініціатив. Водночас, попри наявність розвиненої теоретичної бази й практичних напрацювань, зберігається потреба у подальшому комплексному узагальненні досвіду поєднання стратегічних комунікацій, інституційних інструментів і розвитку медіаграмотності в умовах тривалих гібридних інформаційних загроз.

Метою дослідження є комплексний аналіз дезінформації як інструменту гібридної агресії Російської Федерації та розробка на його основі науково обґрунтованих пропозицій щодо вдосконалення системи протидії в Україні з урахуванням українського та міжнародного досвіду.

Для досягнення поставленої мети визначено такі **завдання**:

- проаналізувати теоретико-методологічні засади дослідження дезінформації, її сутність, характеристики та види;
- охарактеризувати нормативно-правове забезпечення протидії дезінформації в Україні та Європейському Союзі;
- проаналізувати російську дезінформаційну кампанію;
- оцінити функціонування системи протидії дезінформації в Україні в контексті сучасної інформаційної війни;
- проаналізувати міжнародний досвід та ключові моделі протидії дезінформації на прикладі країн ЄС;
- сформулювати практичні рекомендації щодо вдосконалення національної системи протидії дезінформації з урахуванням міжнародних практик.

Об’єкт дослідження – протидія дезінформації в умовах гібридної війни в контексті російської агресії проти України.

Предмет дослідження – сукупність методів, механізмів і інструментів протидії дезінформації,

Для досягнення поставленої мети та вирішення завдань дослідження було використано комплекс загальнонаукових та спеціальних **методів**, що забезпечили всебічний аналіз проблеми:

Теоретичний аналіз та синтез застосовано для дослідження сутності поняття «дезінформація», його ключових характеристик, а також для систематизації її видів та механізмів впливу.

Системний підхід дозволив проаналізувати національну систему протидії дезінформації як сукупність взаємопов'язаних елементів, що включає державні інституції, регуляторні органи та розгалужену мережу громадських фактчекінгових ініціатив.

Порівняльно-правовий метод використано для зіставлення нормативно-правового забезпечення у сфері інформаційної безпеки та протидії дезінформації в Україні та Європейському Союзі.

Порівняльний аналіз застосовано для вивчення та зіставлення моделей протидії дезінформації, що функціонують в Україні, та успішних практик провідних іноземних держав.

Історико-порівняльний метод дозволив дослідити еволюцію російських дезінформаційних кампаній, виокремити їхні етапи та простежити динаміку зміни тактик і методів.

Метод моделювання використано для розробки практичних пропозицій та інтегрованої моделі вдосконалення національної системи протидії дезінформації.

Наукова новизна роботи полягає у системному узагальненні та аналізі українського та міжнародного досвіду протидії дезінформації в унікальних умовах повномасштабної війни. Наукова новизна полягає у розробці комплексної моделі інформаційної стійкості, адаптованої до українських реалій, яка поєднує інституційні, освітні, технологічні та регіональні компоненти.

Практична значущість отриманих результатів полягає в тому, що матеріали, висновки та рекомендації дослідження можуть бути використані:

- державними органами, зокрема Центром протидії дезінформації при РНБО та Центром стратегічних комунікацій та інформаційної безпеки, для вдосконалення національної політики інформаційної безпеки та розробки стратегічних комунікацій;

- громадськими організаціями та фактчекінговими ініціативами для розробки нових проєктів, методологій моніторингу та реалізації просвітницьких кампаній, спрямованих на підвищення стійкості суспільства до маніпуляцій;
- освітніми установами при розробці та впровадженні навчальних курсів, тренінгів та методичних матеріалів з медіаграмотності, критичного мислення та інформаційної гігієни для різних вікових груп.

Основні **результати дослідження були апробовані** в межах фахових науково-практичних заходів. За матеріалами кваліфікаційної роботи підготовлено та представлено наукові тези для участі у X Міжнародній науково-практичній студентській конференції «Актуальні питання інформаційної діяльності: теорії та інновації», що відбулася 20 березня 2025 року в місті Одеса [8]. Тема дослідження також була апробована під час студентської конференції «Сучасні напрямки соціальних комунікацій в інформаційному просторі», яка пройшла 13 травня 2025 року в місті Острогож. У межах виступу було презентовано ключові підходи, висновки та напрацьовані пропозиції щодо протидії дезінформації в умовах сучасного інформаційного середовища.

Магістерська складається зі вступу, трьох розділів, висновків до розділів, висновків, списку використаних джерел (60 найменувань, з них 23 іноземною мовою) та додатку. Загальний обсяг магістерської роботи становить 74 сторінки, з них 63 сторінки основного тексту. Робота містить 8 рисунків на 7 сторінках.

РОЗДІЛ 1

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

У сучасних умовах гібридної війни, особливої ваги набуває необхідність глибокого теоретичного осмислення дезінформації як інструмента цілеспрямованого впливу на суспільну свідомість. Системність та багатошаровість дезінформаційних операцій вимагають чіткого концептуального розмежування цього явища від суміжних форм викривлення інформації, а також аналізу його механізмів та внутрішньої логіки застосування. Саме тому важливим є виявлення сутнісних ознак дезінформації, класифікація її основних видів і форм, а також аналіз національних та європейських нормативних підходів до її протидії.

1.1. Сутність та види дезінформації: теоретичний аспект

Дезінформація як явище вже тривалий час досліджується науковцями в різних галузях, зокрема в журналістиці, національній та міжнародній безпеці, політології, міжнародних відносинах і психології, але в правовій сфері це явище почало привертати увагу відносно недавно. Незважаючи на активне вивчення терміну «дезінформація» та її впливу в різних наукових напрямках, досі не існує єдиного підходу до її визначення як у науковій спільноті, так і серед законодавців на національному та міжнародному рівнях.

Для поглибленого розуміння сутності дезінформації доцільним є аналіз етимологічного походження даного терміна. Хоча слово «дезінформація» має французькі складові *des* – заперечення та *information* – інформація, його введення у використання не спостерігається у європейських країнах. Слово «дезінформація» вперше з'являється в англійських словниках 1980-х років. Однак його походження можна простежити ще з 1920-х років, коли в Росії почали використовувати цей термін у зв'язку з діяльністю спеціального офісу дезінформації, метою якого було поширення «хибної інформації з наміром ввести громадську думку в оману» [39]. Зокрема, підтверджує наявність терміну «дезінформаційні відомості» в словнику КДБ від 1972 року. Тож словник КДБ

дає таке визначення: «дезінформаційні відомості (рос. дезинформационные сведения) – спеціально підготовлені відомості для створення в супротивника невірною уявлення про дійсність, на основі якої він може ухвалювати рішення, вигідні стороні, що дезінформує. Нерідко для стислості називають просто дезінформацією». Таким чином, навмисне створення невірною уявлення про дійсність і є ключовою рисою дезінформації.

Незважаючи на те, що в Україні у 2021 році за наказом президента [19] був створений Центр протидії дезінформації, а в положенні про його діяльність неодноразово використовується саме поняття «дезінформація», у чинному законодавстві даний термін не закріплений. Зокрема в посібник із протидії дезінформації від Центру протидії дезінформації від 2023 року вже включено в глосарій пояснення «дезінформації» – «неправдива або маніпулятивна інформація, яка навмисно поширюється з метою введення в оману, є наріжним каменем класичної пропаганди та основою сучаснішого явища – фейкові новини» [11].

Також у «EU Code of Practice on Disinformation» [34], Кодексі протидії дезінформації від Європейського Союзу, ми можемо бачити сформоване комісією визначення «дезінформації» як «неправдиву, що може бути перевірена, або оманливу інформацію», яку «створено, представлено та поширено з метою отримання економічної вигоди або навмисного обману громадськості»; «може завдати суспільної шкоди», призначене як «загроза демократичним політичним процесам і процесам формування політики, а також суспільним благам, таким як захист здоров'я громадян ЄС, навколишнього середовища або безпеки» [34].

На офіційному сайті НАТО в матеріалі «Підхід НАТО в галузі боротьби з інформаційними загрозами» ми також можемо знайти пояснення терміну «дезінформації», де зазначено, що «в первісному розумінні її можна визначити як навмисне поширення неправдивої та/або оманливої інформації», але зараз «дезінформацію» доречніше розглядати як «цілеспрямоване маніпулювання інформаційним середовищем іноземними державними й недержавними суб'єктами за допомогою маніпулятивних тактик, методів і процедур» [10].

Cambridge Dictionary дає таке визначення: «дезінформація – неправдива інформація, яка поширюється з метою обману людей» [31].

В одному з найперших обговорень концепції дезінформації філософ Лучано Флоріді стверджував, що «дезінформація виникає щоразу, коли процес інформування є дефектним. Це може статися через необ'єктивність (як у випадку пропаганди), відсутність повноти, відсутність плюралізму (як у випадку цензури). Важливо зазначити, що всупереч тому що здається, кожна форма дезінформації не обов'язково має бути навмисною» [35].

Зазначене корелює з дефініцією терміну «дезінформація», що представлена в словнику Національної академії Служби безпеки України та базується на офіційних документах НАТО: «інформацію, що, передусім поширюється організаціями розвідки чи іншими спеціальними службами, завданням яких є викривлення інформації, шахрайство або вплив на рішення, що приймаються відповідальними фахівцями США, представниками армії США, коаліційними силами, ключовими об'єктами або окремими особами, шляхом використання непрямих або нетрадиційних засобів» [1]. Хоча і в цьому визначенні акцент у першу чергу на те, що це інструмент спеціальних служб держави, ми бачимо, що головна ідея і завдання в навмисному викривленні інформації.

Академічні дослідження також відзначають, що дезінформація відрізняється від звичайної неправдивої інформації (misinformation), яка не містить елементів умисності, та від «фейкових новин» (fake news), які можуть включати сенсаційні або викривлені факти без чіткої маніпулятивної мети.

Капелюшний В. П. у статті в Енциклопедії сучасної України дає доволі чітке поняття дезінформації: спотворена, свідомо неправдива, провокаційно-тенденційна інформація, поширена як правдива з метою введення в оману, також сам процес поширення викривлених або свідомо неправдивих відомостей [6].

Дезінформацію також можна інтерпретувати як специфічний різновид інформаційних маніпуляцій, що полягає в цілеспрямованому використанні

психологічних технік та прийомів для конструювання та подальшого поширення недостовірної інформації. Зазвичай цей процес супроводжується пропагандистськими наративами, основною метою яких є формування заданого позитивного або негативного сприйняття певних подій, осіб чи концептів у суспільній свідомості.

Основними характеристиками дезінформації є:

- *навмисність* – дезінформація завжди є результатом свідомої діяльності, коли одна сторона навмисно створює та розповсюджує неправдиві або перекручені відомості;
- *цільова орієнтованість* – її мета полягає в маніпулюванні сприйняттям чи поведінкою аудиторії з певною політичною, економічною чи соціальною метою;
- *когнітивна складність* – дезінформація часто будується на основі психологічних аспектів сприйняття інформації та може включати емоційні маніпуляції, використання перекрученої статистики або цитат.

Шлапаченко В. М. у своїй науковій роботі [25] аналізує дезінформацію як один із ключових інструментів інформаційно-психологічного впливу та виділяє її основні види, залежно від методів і цілей використання. Він розглядає дезінформацію не лише як викривлення реальності, а і як системний засіб маніпуляції, що застосовується у військовій, політичній, економічній та соціальній сферах. Виходячи із цього, Шлапаченко В. М. класифікує дезінформацію за механізмом її впливу на об'єкт, а також за рівнем спотворення інформації та формами її подачі. Він виділяє такі основні види дезінформації:

- *введення в оману* шляхом надання навмисно хибної інформації. Це може включати надання застарілих, неповних або перекручених даних для формування відповідного уявлення про певні події чи факти. Залежно від частки достовірної інформації в підготовлених матеріалах, можна виділити «сіре» дезінформування, яке передбачає використання суміш правдивої та неправдивої інформації, та «чорне» дезінформування, де переважає неправдива інформація;

- *модифікація інформаційного потоку*, що полягає у вибіркового поданні інформації, її дозуванні або замовчуванні певних частин. Це може виражатися в напівправді, тенденційному або упередженому висвітленні фактів за допомогою спеціально підібраних правдивих фактів;
- *«білий шум»* – стратегія створення інформаційного потоку, де поряд із правдивою інформацією навмисно поширюються численні неправдиві версії. Ці версії так само підтверджені певними фактами, свідками, що розчиняє правдиву інформацію в загальному потоці й ускладнює сприйняття істини та змушує об'єкт втратити інтерес до теми. Зазвичай використовується при витокі інформації;
- *дезінформування «від зворотного»* – коли правдива інформація подається в такому контексті, що аудиторія сприймає її як неправдиву. У цьому випадку аудиторія знає правдиву конкретну інформацію але сприймає її неадекватно й може приймати помилкові рішення;
- *термінологічне «мінування»* – перекручення або підміна базових понять та термінів. Це використовується для зміни сприйняття подій та фактів, що впливає на світогляд та прийняття рішень.

Також Шлапаченко В. М. розглядає *маніпулювання* як окремий аспект дезінформації, який спрямований на зміну поведінки аудиторії шляхом впливу на їхні установки та цінності. Це може включати посилення наявних вигідних маніпулятору ідей та установок, або часткову зміну поглядів на певну подію.

Він також виділяє два основних способи дезінформації: дисимуляція – приховування або маскування важливої інформації, та симуляція – створення хибного враження про події чи факти.

Почепцов Г. Г. у матеріалі для «Детектор медіа» [12] описує, що будь-яка дезінформація, коли вона запускається масово і свідомо, становить небезпеку та створює складнощі для протидії, та виділяє ключові чинники, що забезпечують ефективність дезінформації та ускладнюють боротьбу з нею:

- дезінформація з'являється першою в інформаційному просторі, а люди зазвичай довіряють першій почутій версії, а всі наступні спроби її розвінчати часто сприймаються як маніпуляція або спроба замовчати правду;
- дезінформація спирається на вже існуючі стереотипи, страхи та суспільні настрої, що робить її максимально правдоподібною. Вона не створює нової реальності, а лише підсилює ті емоційні тригери, які вже присутні в суспільстві;
- дезінформаційні кампанії направлені на окремі соціальні групи, розпалюючи між ними конфлікти, що сприяє поляризації суспільства, послаблює суспільну єдність та робить його вразливішим до зовнішніх маніпуляцій;
- дезінформація провокує появу контрнарративів, що ще більше загострює ситуацію. Будь-яке спростування може призвести до виникнення нових конспірологічних теорій або альтернативних версій подій, які лише посилюють інформаційний хаос;
- дезінформація робить інформаційне протистояння, яке здатне перерости у фізичний конфлікт, адже постійне нагнітання страху та ненависті в інформаційному просторі, у фізичному просторі переходить у насильницькі дії.

Таким чином, боротьба з дезінформацією ускладнюється її здатністю закріплюватися в суспільній свідомості, адаптуватися до існуючих переконань, розколювати суспільство та ескалувати конфлікти, що потребує системного й комплексного підходу до її подолання.

Отже, на основі здійсненого теоретичного аналізу встановлено, що дезінформація є комплексним, багатогранним феноменом, який виходить за рамки простого поширення неправдивих відомостей. Її сутність полягає в цілеспрямованому спотворенні інформації з метою маніпулятивного впливу на суспільну свідомість та поведінку реципієнтів. Визначено, що дезінформація є різновидом інформаційних маніпуляцій, що передбачає застосування специфічних психологічних та комунікативних технік для створення та розповсюдження фальсифікованого контенту. Її функціонування часто

інтегроване з пропагандистськими наративами, спрямованими на формування заданого емоційного та ціннісного сприйняття об'єктів впливу. Класифікація дезінформації за різними критеріями (за джерелом, формою, метою, каналом поширення) дозволяє краще зрозуміти її архітектоніку та адаптивність до мінливого інформаційного ландшафту, підкреслюючи її роль як деструктивного чинника в архітектоніці сучасного інформаційного простору.

1.2. Нормативно-правове забезпечення протидії дезінформації

З 1991 року державна інформаційна політика України зосереджувалася переважно на забезпеченні свободи слова, що було зумовлено прагненням підкреслити демократичні цінності та гарантувати свободу слова. Проте з часом усвідомлення важливості національної безпеки та захисту від інформаційних загроз посилювалося, що призвело до розробки нових стратегій і підходів у державній політиці. Ось ключові документи та ініціативи:

Доктрина інформаційної безпеки України (Указ Президента України від 25 лютого 2017 року № 47/2017.) [17], є стратегічним документом, що визначає основні напрями державної політики у сфері інформаційної безпеки. Її прийняття у 2017 році було зумовлене необхідністю реагування на інформаційну агресію з боку Російської Федерації та захисту національного інформаційного простору. Доктрина встановлює національні інтереси України в інформаційній сфері, серед яких захист суспільства від деструктивної пропаганди та інформаційних впливів, спрямованих на підрив суверенітету та територіальної цілісності України, а також розвиток національної інформаційної інфраструктури та медіакультури суспільства. Серед загроз визначаються спеціальні інформаційні операції, що дестабілізують суспільно-політичну ситуацію, інформаційна експансія держави-агресора на тимчасово окупованих територіях. Доктрина також визначає пріоритети державної політики у сфері інформаційної безпеки, що включають створення системи оцінки інформаційних загроз та оперативного реагування на них, удосконалення законодавства для виявлення та блокування інформації, що

загрожує національній безпеці, розвиток структур, відповідальних за інформаційно-психологічну безпеку, розвиток системи стратегічних комунікацій та взаємодії держави з інститутами громадянського суспільства для протидії інформаційній агресії. Для реалізації Доктрини передбачена координація діяльності органів виконавчої влади через Раду національної безпеки й оборони України, моніторинг засобів масової інформації та інтернет-ресурсів для виявлення забороненого контенту, розробка стратегічних наративів та їх впровадження в інформаційний простір, а також взаємодія з міжнародними партнерами для зміцнення інформаційної безпеки та протидії дезінформації.

Закон України «Про національну безпеку України» від 21.06.2018 р. № 2469–VIII [15], визначає основи державної політики у сфері національної безпеки та оборони, зокрема правові засади захисту суспільства й кожного громадянина від внутрішніх і зовнішніх загроз. Він встановлює цілі та принципи державної політики безпеки, розмежовує повноваження органів влади у сфері безпеки та оборони й запроваджує всеосяжний підхід до планування в цих галузях. Закон передбачає створення системи стратегічного планування, де Стратегія національної безпеки України є основним документом довгострокового планування. Документ визначає основи для розробки галузевих стратегій, включно зі Стратегією інформаційної безпеки та Стратегією кібербезпеки України. Важливо, що серед загроз прямо називаються інформаційні операції, пропаганда та дезінформація, а серед механізмів забезпечення безпеки розписані демократичний цивільний контроль та координація діяльності органів влади.

Стратегія інформаційної безпеки України (Указ Президента України від 28 грудня 2021 року № 685/2021) [20] є нормативно-правовим актом у сфері інформаційної безпеки і правового врегулювання окремих аспектів дезінформації і була прийнята у 2021 році. Вона розглядає дезінформацію як одну з ключових загроз для національної безпеки, адже деструктивна пропаганда та дезінформація є інструментами, за допомогою яких

держави-агресори, зокрема Росія, намагаються маніпулювати суспільною свідомістю, посіяти розкол у суспільстві та підірвати демократичний лад країни. Документ підкреслює, що дезінформація застосовується як ззовні, так і всередині України, створюючи умови для формування альтернативних, викривлених наративів про державу. У відповідь на це стратегія передбачає створення систем раннього виявлення загроз і оперативного реагування, впровадження заходів щодо обмеження розповсюдження недостовірної інформації та посилення відповідальності за її поширення, а також наголошує на важливості підвищення медіаграмотності населення через просвітницькі кампанії, що сприятимуть розвитку критичного мислення і допоможуть громадянам ефективніше протидіяти маніпуляціям, забезпечуючи тим самим збереження національної єдності та підтримку демократичних цінностей.

Закон України «Про основи національного спротиву» від 16.06.2021 р. №1702–ІХ [16] визначає правові та організаційні засади національного спротиву, який є сукупністю заходів для забезпечення оборони держави, її суверенітету та територіальної цілісності. Основними складовими національного спротиву є територіальна оборона, рух опору та підготовка громадян до спротиву. Інформаційний спротив розглядається як частина руху опору, зокрема в Статті 3 описана участь в інформаційних заходах, спрямованих на підвищення рівня обороноздатності держави та на протидію інформаційним операціям агресора.

Закон України «Про інформацію» від 2.10.1992 р. №2657–ХІІ [13] є базовим актом у сфері інформаційних відносин України, що встановлює правові основи одержання, використання, поширення та зберігання інформації. Він гарантує право особи на достовірну інформацію, закріплює принципи відкритості, доступності та об'єктивності, а також законність її одержання, використання, поширення та зберігання. У Статті 21 визначено порядок обмеження доступу до інформації з міркувань національної безпеки, а також встановлено, що інформація може бути конфіденційною, таємною або службовою, якщо її розголошення може завдати шкоди інтересам держави чи

особи. У Статті 28 визначено неприпустимість зловживання правом на інформацію, що інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини.

Закон України «Про медіа» від 31.03.2023 р. № 2849–IX [14], що набув чинності 31 березня 2023 року, є комплексним нормативно-правовим актом, який регулює діяльність суб'єктів у сфері медіа в Україні. Він замінив попередні закони, такі як «Про телебачення і радіомовлення», «Про друковані засоби масової інформації (пресу) в Україні» та «Про інформаційні агентства», об'єднавши їх положення та адаптуючи до сучасних реалій медіапростору. Закон охоплює широкий спектр медіа, включаючи друковані, аудіовізуальні (телебачення та радіо), онлайн-медіа, а також провайдерів аудіовізуальних сервісів та платформ спільного доступу до відео. Встановлено вимоги щодо змісту інформації, зокрема в Статті 36 заборонено поширення матеріалів, які пропагують насильство, жорстокість, розпалюють національну, расову чи релігійну ворожнечу. А Стаття 119 передбачає спеціальні обмеження щодо поширення інформації під час збройної агресії. Забороняється розповсюдження інформації, що висвітлює збройну агресію як внутрішній або громадянський конфлікт, якщо це призводить до розпалювання ворожнечі або закликів до насильницької зміни конституційного ладу. Також забороняється поширення недостовірних матеріалів щодо дій держави-агресора, її посадових осіб або організацій, контрольованих агресором.

Серед напрацювань Європейської Комісії з протидії дезінформації, на сьогодні існують такі нормативно-правові документи та ініціативи як:

«EU Code of Practice on Disinformation» (Кодекс ЄС щодо дезінформації) [34] є добровільним саморегуляторним документом, уперше розробленим у 2018 році як відповідь на зростаючі виклики, пов'язані з поширенням дезінформації. Його оновлена версія [51], ухвалена у 2022 році,

зберегла принцип добровільності, проте суттєво розширила сферу зобов'язань підписантів. Документ розмежовує дезінформацію та інші форми контенту, що можуть містити неточності, але не є свідомо маніпулятивними, зокрема журналістські помилки, сатиру, пародію та чітко ідентифіковані партійні коментарі. Кодекс запроваджує низку зобов'язань для цифрових платформ та інших підписантів. Зокрема, документ передбачає посилення контролю за рекламними розміщеннями з метою припинення фінансових потоків для розповсюджувачів дезінформації, підвищення прозорості політичної та тематичної реклами, що включає маркування таких оголошень, розкриття інформації про рекламодавців і витрати на кампанії, а також розробку та імплементацію алгоритмічних рішень, які сприяють зменшенню поширення недостовірної інформації та покращенню видимості авторитетних джерел. Крім того, Кодекс забезпечує користувачам доступ до інструментів для оцінки достовірності інформації та можливості звертатися до різних джерел. Окрім заходів на рівні цифрових платформ, Кодекс передбачає активну співпрацю з академічною та дослідницькою спільнотою. Він зобов'язує підписантів надавати незалежним дослідникам доступ до даних, необхідних для аналізу інформаційних маніпуляцій, із дотриманням принципів захисту персональних даних. Таким чином, Кодекс 2022 року відображає перехід від добровільних ініціатив до комплексної системи протидії дезінформації, що поєднує регулювання інформаційних потоків, технологічні рішення та міжінституційну співпрацю. У 2025 році вже під назвою «The Code of Conduct on Disinformation» [53] цей документ став частиною Digital Services Act (DSA).

Digital Services Act (DSA) (Акт про цифрові послуги) [54] – це законодавчий акт Європейського Союзу, прийнятий у 2022 році, який встановлює нові правила для цифрових платформ, таких як соціальні мережі, пошукові системи та онлайн-маркетплейси. Його основною метою є створення більш безпечного та прозорого цифрового середовища, а також посилення відповідальності онлайн-платформ за поширення незаконного контенту, дезінформації та інших загроз. Закон зобов'язує цифрові сервіси швидко

реагувати на повідомлення про незаконний контент, запроваджує механізми оскарження рішень про його видалення та підвищує прозорість алгоритмів рекомендацій, а також політичної та таргетованої реклами. Особливу увагу DSA приділяє великим цифровим платформам, які мають понад 45 мільйонів користувачів у ЄС, зобов'язуючі їх проводити регулярну оцінку ризиків, пов'язаних із поширенням дезінформації та маніпулятивною поведінкою. Крім того, документ гарантує незалежним дослідникам доступ до даних для аналізу інформаційних загроз і передбачає жорсткі санкції за порушення, включаючи штрафи до 6 % від глобального обороту компанії. DSA став ключовою частиною регуляторної політики ЄС у сфері цифрових послуг, забезпечуючи прозорість, відповідальність та захист прав користувачів. Закон набув чинності для великих онлайн-платформ 25 серпня 2023 року, а для всіх інших цифрових сервісів 17 лютого 2024 року.

У січні 2025 року Європарламент ухвалив резолюцію, **Resolution on Russia's disinformation and historical falsification to justify its war of aggression against Ukraine 2024/2988(RSP)** [48], щодо дезінформації та історичних фальсифікацій Росії, де особливий акцент зроблено на системному використанні російським режимом дезінформації та історичного ревізіонізму для виправдання агресії проти України, а також для підризу демократичних процесів у країнах ЄС. У пунктах Е, F та Н наголошується, що початок повномасштабної війни супроводжувався публічними заявами російського керівництва, які базувалися на історичних фальсифікаціях та неправдивих твердженнях. Російський режим, як зазначено в пункті F, активно використовує дезінформацію, зокрема спотворені історичні аргументи, а також маніпуляції інформацією для виправдання злочину агресії, втручання в демократичні процеси інших країн і зниження підтримки України серед громадськості держав-членів ЄС.

У пункті 3 резолюції парламент прямо засуджує систематичне фальшування історії та використання викривлених історичних аргументів російською владою для маніпуляції громадською думкою, виправдання війни та

підриву міжнародної підтримки України. Водночас у пункті 8 міститься заклик до ЄС і держав-членів посилити та координувати зусилля для своєчасної і рішучої протидії російській дезінформації, а також іноземному маніпулюванню інформацією з метою захисту демократичних процесів і зміцнення стійкості європейських суспільств. Особливо підкреслюється важливість розвитку медіаграмотності, підтримки якісних медіа, професійної журналістики та розслідувань, які викривають російську пропаганду, а також досліджень нових технологій гібридного впливу.

Резолюція є політичним документом і не встановлює обов'язкових норм, але визначає позицію Європейського Союзу щодо російських дезінформаційних операцій та їх наслідків для безпеки й демократії в ЄС, і формує підстави для подальших законодавчих дій у сфері інформаційної безпеки, а також служить аргументом для збереження і розширення санкцій проти російських пропагандистських структур і дезінформаційних мереж.

Таким чином, аналіз нормативно-правового забезпечення протидії дезінформації засвідчує, що на сучасному етапі відбувається системна інституціоналізація та імплементація комплексних механізмів регулювання інформаційного простору. Ключовим вектором є перехід від реактивної до проактивної політики, що включає розробку законодавчих актів, запровадження механізмів саморегуляції для онлайн-платформ та підвищення медіаграмотності населення. Зокрема, на прикладі Європейського Союзу, спостерігається тенденція до поєднання добровільних кодексів поведінки з обов'язковими вимогами, що забезпечує посилення відповідальності ключових осіб інформаційного простору. Це дозволяє створювати архітектуру протидії дезінформації, яка є адаптивною до динамічних змін у гібридному інформаційному середовищі та спрямована на захист демократичних цінностей і суспільної довіри.

Висновки до першого розділу

У першому розділі роботи було здійснено аналіз поняття «дезінформація», її видів та основних характеристик, а також розглянуто

нормативно-правове забезпечення протидії цьому явищу на національному рівні та в Європейському Союзі.

Аналіз теоретико-методологічних основ дослідження дезінформації дозволив визначити її як комплексне явище, що має глибокі історичні корені та еволюціонує відповідно до розвитку інформаційних технологій та змін у суспільно-політичному середовищі. Дезінформація є багатоаспектним явищем, що має різні визначення залежно від контексту дослідження. Незважаючи на те, що дезінформація є предметом вивчення в журналістиці, політології, міжнародних відносинах, психології та інших наукових сферах, її точне визначення та правове регулювання все ще залишаються дискусійними.

Таким чином, на основі проведеного аналізу, основними характеристиками дезінформації визначено її навмисний характер, цільову орієнтованість, когнітивну складність, а також використання психологічних прийомів для маніпулятивного впливу на суспільну свідомість. Ідентифіковано різноманітні види дезінформації, серед яких пряма фальсифікація фактів, вибіркове представлення інформації, технологія «білого шуму», термінологічне «мінування» та інші методи цілеспрямованих інформаційних впливів.

Проблема дезінформації для України є особливо актуальною в контексті російської агресії, що супроводжується системними інформаційними операціями, спрямованими на дестабілізацію суспільства, підрив довіри до державних інституцій та виправдовування агресора. Попри те, що явище дезінформації існує вже давно, системні кроки з протидії на державному рівні в Україні розпочалися лише після 2016 року, коли загрози інформаційній безпеці стали очевидними. Водночас у Європейському Союзі формування законодавчої бази для боротьби з дезінформацією почалося ще пізніше, але має достатньо ефективну тенденцію.

Отже, результати аналізу свідчать про комплексний характер дезінформації як явища, що потребує міждисциплінарного підходу до вивчення та багаторівневої стратегії протидії. Важливу роль у цьому процесі відіграють

як державні інституції, так і міжнародні ініціативи, що сприяють формуванню ефективних механізмів захисту інформаційного простору.

РОЗДІЛ 2

АНАЛІЗ РОСІЙСЬКОЇ ДЕЗІНФОРМАЦІЇ У КОНТЕКСТІ ГІБРИДНОЇ АГРЕСІЇ ПРОТИ УКРАЇНИ

В умовах стрімкої трансформації інформаційного простору та зростання впливовості цифрових комунікацій, дезінформація постає не просто як супровідний елемент війни, а як один із її центральних інструментів, здатних формувати альтернативну реальність, підривати суспільну стійкість і розмивати довіру до державних інституцій. Масштабність, гнучкість і адаптивність російських інформаційних операцій демонструють їхню здатність трансформуватися. Для України, що перебуває у стані постійного інформаційного тиску, надзвичайно важливим є ґрунтовне вивчення логіки, механізмів і структур дії цих дезінформаційних кампаній, а також оцінка ефективності існуючих державних, громадських і технологічних інструментів протидії. Саме такий аналітичний підхід дає змогу окреслити ключові вразливості інформаційного простору, визначити сильні сторони національної системи захисту та створити підґрунтя для формування дієвих стратегій підвищення інформаційної стійкості України.

2.1. Аналіз російської дезінформаційної кампанії

Російська дезінформаційна кампанія в Україні є ключовим елементом гібридної агресії, спрямованим на руйнування національної єдності, підриєв довіри до влади, деморалізацію суспільства та дестабілізацію внутрішньополітичної ситуації. Її мета не лише спотворення реальності, а й формування таких умов, за яких українське суспільство саме починає сумніватися у власній державності, армії, союзниках і перемозі.

Інформаційні компанії вже давно є компонентом російської стратегії у війні, про що ще у 2013 році відкрито заявляв у своїй доктрині Герасимов (на той час начальник Генштабу Збройних Сил РФ) [3]. За його словами невійськові засоби в багатьох випадках за ефективністю значно перевищують силу зброї, а

під невійськовими засобами він описує «інформаційне протиборство» та «залученням протестного потенціалу населення».

Етапи розвитку дезінформаційної кампанії під час війни

За період 2014–2025 років російська дезінформаційна діяльність в Україні може бути поділена на три відносно чіткі етапи.

Перший етап (2014–2021 рр.) характеризувався активним впливом через українські медіа, легальні медійні майданчики підконтрольні проросійським політикам. На той момент основним джерелом інформації для переважної більшості мешканців України було телебачення. Через канали «112 Україна», «NewsOne», «ZIK», «Наш» поширювалися меседжі про «утиски Донбасу», «некомпетентну владу», «майдан був помилкою», «Україні треба помиритися з Росією», «Україна під зовнішнім управлінням США». У цей період активно залучалися проросійські експерти та аналітики, та й самі ведучі в студії виголошували щось подібне. Послідовне просування тез російської пропаганди подавалось як опозиційні погляди формуючи думку, узгоджену з кремлівськими методичками.

Другий етап розпочався з лютого 2021 року, коли було підписане рішення Ради національної безпеки й оборони України «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» (Указ Президента України від 2 лютого 2021 року № 43/2021) [18] яке поклало початок блокуванню проросійських каналів та змусило інформаційні структури РФ перейти в цифрове середовище. Головним інструментом стали соціальні мережі та месенджери такі як Telegram, TikTok, YouTube, Facebook. Сформувалася широка мережа анонімних каналів, замаскованих під українські джерела, таких як «Резидент», «Легітимний», «Политика страны», «Сплетница UA». Вони поширюють «інсайди» та «зливи з Офісу Президента», часто апелюючи до нібито «внутрішніх джерел». Ціллю є створити недовіру до влади та посіяти відчуття хаосу. Також формується нова інфраструктура інформаційного впливу через особистісні комунікаційні формати, блогерів, стрімерів, коментаторів, які поширюють російські меседжі під виглядом

«суб'єктивної думки». Такі діячі, як правило, уникають відкритої проросійської позиції, натомість апелюють до «втоми від війни», «непрофесійності політиків», «втрати сенсу». У цей період активно розвиваються ботоферми, що симулюють суспільну дискусію в коментарях під публікаціями. Організовані мережі акаунтів поширюють однотипні коментарі для створення видимості суспільного консенсусу. Здебільшого акцент йде на масовість повідомлень, а не на якість, то ж ми могли спостерігати велику кількість помилок швидкого перекладу наративів із російської на українську мову: «немає сечі терпіти ці борошна», «у самих пика в гармату», «підлога країни хоче змінити державний будуй» та інші.

Третій етап (2023–2025 рр.) характеризується локалізацією впливу та глибокою інфільтрацією в регіональні інформаційні середовища. Російські меседжі поширюються через місцеві пабліки та спільноти, маскуються під місцеві медіа, псевдо волонтерські сторінки. Паралельно, активізується діяльність псевдоаналітичних сторінок та ініціатив, які позиціонують себе як економічні або експертні платформи («Економіка країни», «Бізнес Online UA», «Український аналітик» тощо). Їхній зміст часто базується на напівправдивих даних, вирваних із контексту економічних звітів або міжнародних прогнозів. Такі ресурси поширюють меседжі про «знецінення гривні через війну», «втому Заходу від України», «неефективність антикорупційних реформ». Цей формат особливий тим, що імітує експертність і подає дезінформацію як «раціональну економічну оцінку», а не як пропаганду. Дезінформація стає більш інтегрованою в структуру повсякденного українського інформаційного споживання. Вона не протиставляє себе офіційному дискурсу відкрито, а співіснує з ним, імітує «здоровий скепсис», що особливо небезпечно через її наближеність до форматів повсякденної комунікації.

Динаміка розвитку російської дезінформаційної кампанії в Україні свідчить про її здатність до постійної адаптації під зміни медіасередовища та поведінки аудиторії. Від відкритої пропаганди через телеканали вона

еволюціонувала до мережових, регіонально орієнтованих форм, що діють приховано й системно.

Основні стратегічні цілі інформаційних операцій Російської Федерації в Україні полягають у підриві державного суверенітету та суспільної стійкості шляхом формування викривленого інформаційного поля. Це включає цілеспрямоване делегітимізацію української влади та її інституцій, представлення України як «неспроможної держави», а також дискредитацію її міжнародних партнерів і підтримки. Ключовими завданнями є також розкол українського суспільства за регіональними, мовними чи політичними ознаками, деморалізація Збройних Сил України та населення, а також нейтралізація опору шляхом поширення паніки, страху та дезінформації щодо військових успіхів та політичних намірів. На міжнародній арені ці операції спрямовані на зменшення обсягів військово-технічної та фінансової допомоги Україні та формування хибного наративу про справедливість чи вимушеність російської агресії для виправдання своїх дій перед світовою спільнотою.

Виходячи із цього основними стратегічними цілями інформаційних операцій РФ в Україні є:

- *підрив довіри до українських інституцій* (державного керівництва, місцевої влади), створення враження, що влада некомпетентна, корумпована або працює проти інтересів громадян;
- *розпалювання паніки та деморалізації населення*, особливо в критичні моменти, та створення враження, що ситуація в Україні безнадійна;
- *створення ілюзії розколу суспільства* за регіональними, мовними, релігійними чи політичними ознаками;
- *дискредитація зовнішньої допомоги Україні й партнерів* та формування переконання що допомога неефективна, що «Захід втопився від України» або «використовує українців у своїх інтересах»;
- *заволодіння інформаційним полем як складової контролю*: не лише донесення наративу, але і блокування або ускладнення достовірної інформації.

Тактики, які застосовує Російська Федерація, поєднують класичні пропагандистські підходи із сучасними технологіями цифрового впливу, психологічних операцій (PSYOP) та алгоритмічного маніпулювання інформаційними потоками (Рис. 2.1.).

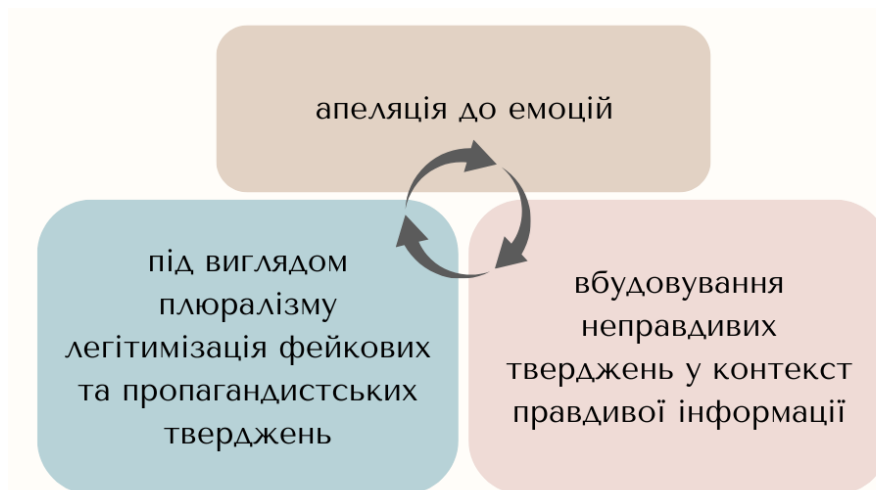


Рис. 2.1. Пропагандистські підходи

Джерело: [за автором]

Однією з базових тактик російських інформаційних операцій є **апеляція до емоцій** (Рис. 2.2.), а не до раціонального сприйняття фактів. Емоційно орієнтовані повідомлення, спрямовані на виклик страху, розпачу або відчаю. Для цього активно використовуються контент із шокowymi заголовками, фото та відео без контексту, вирвані з реальності цитати або навмисно спотворені повідомлення. Найчастіше це інформація про втрати ЗСУ, «зраду керівництва», «масову мобілізацію» чи «неминучість поразки». Такі повідомлення поширюються у форматі «чутток», скриншотів переписок, коротких відео з коментарями на кшталт «подивіться, що приховує влада».

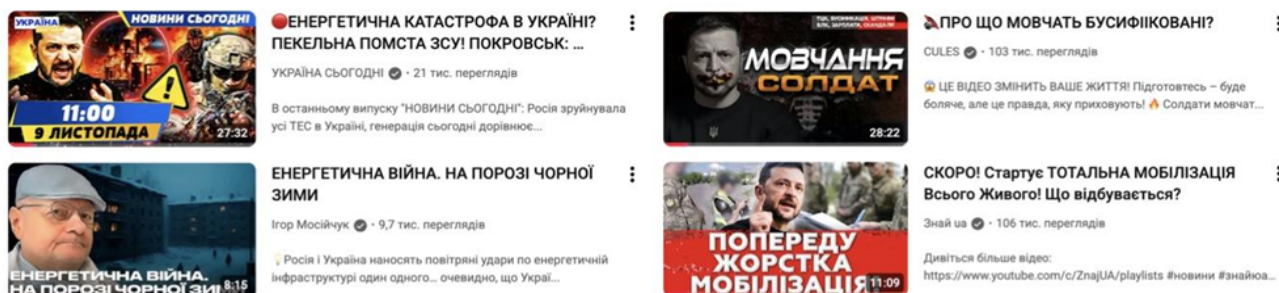


Рис. 2.2. Тактика «апеляція до емоцій»

Джерело: [за автором]

Емоційна насиченість знижує критичність сприйняття, і користувач неспівомодно бере участь у поширенні дезінформації, навіть не вірячи в неї повністю. Цей прийом активно використовується для підсилення емоційного напруження під час кризових подій, масованих обстрілів, блекаутів, політичних скандалів. Така тактика дозволяє дестабілізувати емоційний стан суспільства та зменшити рівень довіри до офіційних джерел інформації.

Ще однією ключовою тактикою є **вбудовування неправдивих тверджень у контекст правдивої інформації** (Рис. 2.3.). Такі повідомлення виглядають достовірними, оскільки базуються на реальних подіях, але містять фрагменти маніпуляцій, викривлених цитат або спотворених причинно-наслідкових зв'язків.

Інформаційні повідомлення можуть містити достовірні елементи такі як дати, цитати, фото, опис реальних подій, але з маніпулятивною інтерпретацією. Це створює ілюзію достовірності й ускладнює спростування, оскільки формально факт існує, але сенс перекошено.

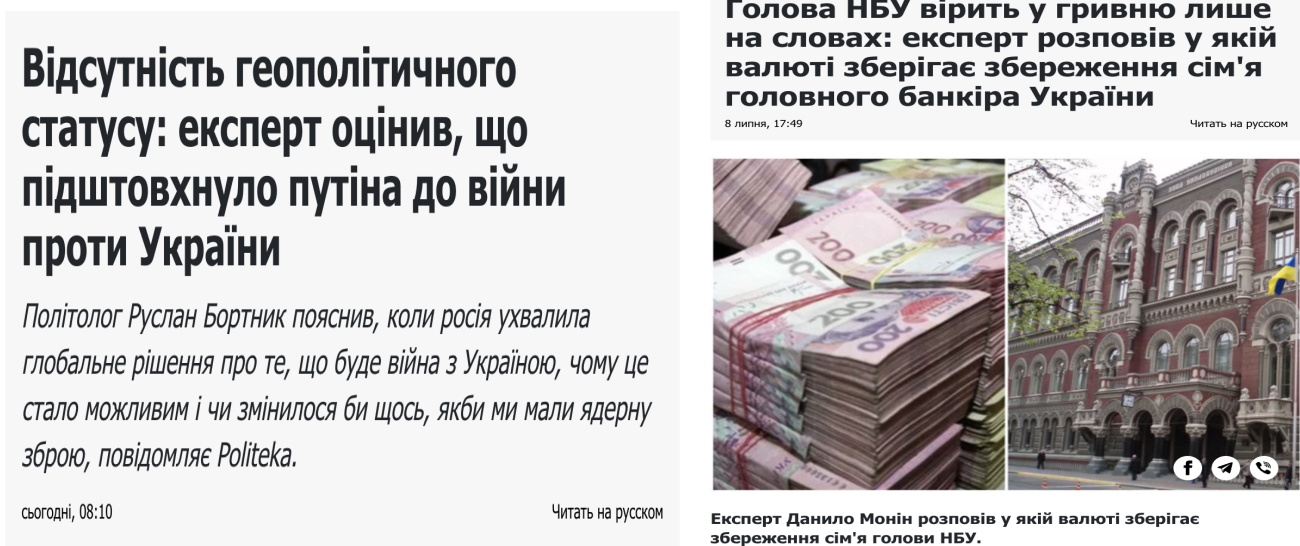


Рис. 2.3. Тактика «вбудовування неправдивих тверджень у контекст правдивої інформації»

Джерело: [за автором]

Наприклад, повідомлення «Україна втратила підтримку Заходу» може спиратися на окремі заяви політиків або економічні труднощі, однак узагальнює їх у спосіб, що формує хибне враження про міжнародну ізоляцію. Ця тактика

ефективна тому що знижує критичність мислення аудиторії: якщо частина повідомлення здається знайомою або правдивою, люди схильні сприймати весь контент як достовірний. Зазвичай в українському інфопросторі вона використовувалась при кадрових змінах влади або міжнародних, політичних, економічних подіях, коли аудиторія знає факт але занурюватись у питання не хоче або не може.

Активно використовується також прийом коли дезінформація подається у форматі нібито збалансованої дискусії, де «є різні точки зору», «правда десь посередині». Це створює ілюзію об'єктивності, однак **під виглядом плюралізму легітимізує фейкові або пропагандистські твердження** (Рис. 2.4.). Така тактика особливо помітна у відео- та стрімінгових форматах, де створюється видимість публічної дискусії, хоча насправді структура формату заздалегідь спрямована на підтвердження потрібних наративів. Баланс думок є штучним, умовно проросійську позицію представляє харизматичний або більш агресивний спікер, а «проукраїнський» опонент виглядає менш підготовленим, що створює в глядача враження логічності чи переконливості саме дезінформаційної сторони. Їхній контент часто складається з «аналітичних обговорень» на теми корупції, оборонних витрат або відносин України із Заходом. Формально вони запрошують «псевдоекспертів» та коментаторів із нібито аналітичним бекграундом, але без жодної перевіреної компетенції.

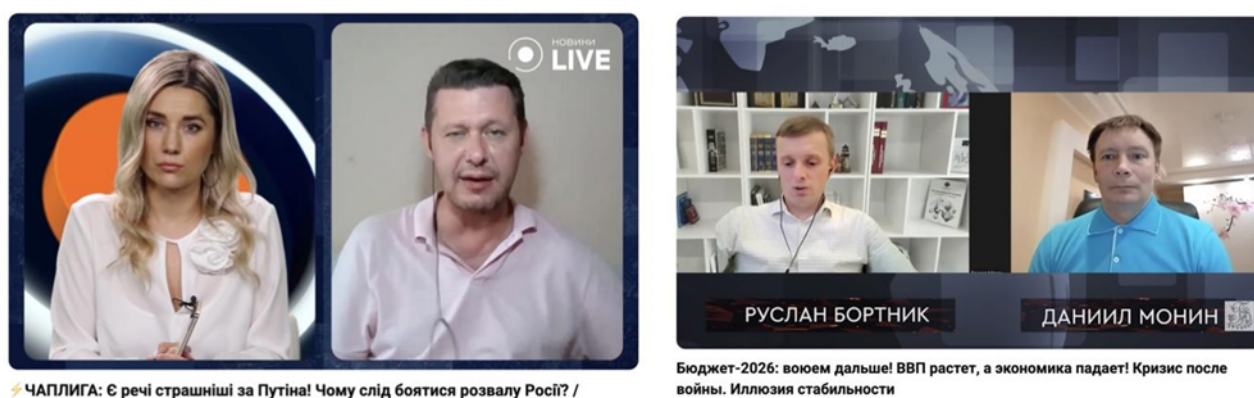


Рис. 2.4. Тактика «під виглядом плюралізму»

Джерело: [за автором]

Унаслідок цього частина аудиторії починає сприймати дезінформаційні твердження як одну з «альтернативних» позицій, а не як відверту маніпуляцію. У такий спосіб підривається саме поняття істини, аудиторія звикає до того що «всі брешуть» і що «ніхто не знає всієї правди». Це розмиває межу між фактами та думками, сприяючи поширенню скепсису щодо офіційних джерел і посилюючи вплив російських наративів у інформаційному просторі України. Ще одним прикладом є псевдоекспертні формати в TikTok і Facebook, де короткі відео подаються у вигляді «виваженого аналізу ситуації». Автор починає з формули на кшталт: «давайте розберемося без емоцій», «об'єктивно кажучи, винні всі», «не все так однозначно» й після цього поступово вводить дезінформаційний меседж, наприклад: «владі вигідна війна», «пора думати про перемовини». Такий прийом ефективно знижує пильність аудиторії, оскільки апелює до прагнення бути «раціональним» і не сприймати світ у чорно-білих категоріях.

Методи впливу та поширення

Сучасна російська дезінформаційна діяльність в Україні відзначається високим рівнем адаптивності та гнучкості до змін інформаційного середовища. Її оператори активно використовують інструменти цифрового маркетингу, алгоритми соціальних мереж і психологічні прийоми для ефективнішого впливу на різні групи населення.

Одним із найпоширеніших методів є **імітація українських джерел інформації**, створення сайтів, Telegram-каналів, сторінок у Facebook і TikTok, які візуально й лексично нагадують українські медіа. Вони використовують українську мову, національну символіку, стилістику та регіональні назви («Харків LIVE», «Київ INFO», «UA Патріот» тощо) і виглядають як «місцеве» медіа, але фактично поширюють проросійські наративи. Така мімікрія підвищує рівень довіри та дозволяє інтегрувати фейки у звичний інформаційний потік.

Також активно застосовується **мікротаргетинг, точкове спрямування контенту на конкретні соціальні групи**. Мікротаргетинг забезпечується аналітикою поведінки користувачів у соцмережах, алгоритмами платформ і

масовими даними про інтереси та активність аудиторії. Це дозволяє дезінформаційним кампаніям доставляти потрібні наративи саме тим людям, які ймовірно на них відреагують, збільшуючи ефективність впливу і водночас знижуючи ймовірність їх спростування через традиційні медіа. Цей підхід дозволяє «підганяти» меседжі під цінності та страхи аудиторії: для матерів військових історії про «масові втрати й байдужість командування», для переселенців тези про «недостатню соціальну підтримку», для підприємців меседжі про «безглузді податки». У підсумку, мікротаргетинг перетворює дезінформацію із «загальної інформаційної атаки» на індивідуально адаптовану маніпуляцію, що суттєво підвищує шанси на формування емоційного впливу та зміни поведінки цільових груп.

Одним з основних методів впливу є **мережева багатоканальність**, реалізується через автоматичне дублювання контенту на різних платформах і каналах для підвищення видимості, синхронізоване поширення ботами коментарів, репостів і лайків, що формує ефект «штучного тренду» та перехресне посилення між ресурсами, коли контент з одного каналу активно поширюється іншими «сателітними» джерелами, створюючи відчуття, що інформація циркулює незалежно й підтверджується багатьма джерелами. Як результат, підвищується рівень довіри до повідомлення через його повторюваність, так як споживачі інформації схильні швидше приймати повторювані повідомлення як істинні. Це створює видимість «масової думки» або «широкого суспільного резонансу».

Для проведення дезінформаційних кампаній у цифровому просторі ключове значення мають платформи, що забезпечують швидке та масове поширення контенту. Серед таких платформ найчастіше використовуються Telegram, TikTok і Facebook.

Telegram залишається основним каналом для поширення проросійських наративів завдяки анонімності, відсутності ефективної модерації та простоті створення каналів і чатів. Дезінформаційні оператори можуть швидко запускати нові канали, дублювати контент між десятками ресурсів та створювати

бот-мережі для масового поширення повідомлень. Особливістю Telegram є також вбудована функціональність каналів і супергруп, яка дозволяє формувати видимість активного обговорення і суспільної підтримки того чи іншого меседжу.

TikTok використовують для поширення коротких відео з емоційним навантаженням, які легко стають «вірусними». Алгоритми рекомендацій платформи стимулюють поширення контенту серед користувачів, що підпадають під цільову аудиторію, без необхідності прямої підписки на канал чи автора. Це робить TikTok ефективним інструментом мікротаргетингу.

Facebook залишається важливим каналом для поширення текстових і відеопублікацій та коментарів, незважаючи на впроваджені механізми фактчекінгу та цензури. Дезінформаційні оператори використовують групи, сторінки та спільноти, де повідомлення активно обговорюються, підсилюючи ефект «масової думки». Крім того, Facebook дозволяє створювати контент, орієнтований на конкретні регіони, соціальні групи чи інтереси користувачів, що також інтегрується з мікротаргетингом.

Отже, сучасна російська дезінформаційна кампанія в Україні демонструє високу адаптивність та багатовекторність, поєднуючи традиційні пропагандистські прийоми із цифровими технологіями, психологічними маніпуляціями та алгоритмічним поширенням контенту, вона здатна одночасно впливати на різні соціальні групи, формувати ілюзію масової підтримки повідомлень і легітимізувати фейкові наративи. Використання платформ, що забезпечують швидке й таргетоване поширення контенту, підсилює ефективність кампанії та інтегрує дезінформацію в повсякденне інформаційне споживання українців, що робить її особливо небезпечною для суспільної довіри та стабільності.

2.2. Функціонування системи протидії дезінформації в Україні в контексті сучасної інформаційної війни

У сучасних умовах інформаційної війни дезінформація стає серйозною загрозою для національної безпеки та стійкості суспільства. Україна активно протидіє цим викликам, поєднуючи зусилля державних інституцій, громадських ініціатив, незалежних аналітичних центрів та медіа, використовуючи і традиційні, і сучасні технологічні методи протидії дезінформації.

Інституційні механізми протидії дезінформації.

Інституційні механізми протидії дезінформації в Україні формуються в межах державної політики інформаційної безпеки. Вони охоплюють систему органів та установ, що здійснюють координацію стратегічних комунікацій, моніторинг інформаційного простору, регулювання діяльності медіа та розробку аналітичних і просвітницьких заходів. Комплексний підхід до протидії дезінформації передбачає взаємодію державних структур, незалежних регуляторів та публічних медіа, що спільно сприяють підвищенню стійкості суспільства до інформаційних впливів.

Центр протидії дезінформації при РНБО України [23] є спеціалізованим органом, створеним для боротьби з дезінформацією та захисту інформаційного простору України. Центр було засновано 11 березня 2021 року відповідно до рішення РНБО. Центр протидії дезінформації здійснює моніторинг та аналіз інформаційного простору України, виявляючи поточні та потенційні загрози інформаційній безпеці, готує аналітичні матеріали для РНБО та Президента України, пропонує стратегії протидії дезінформації, координує діяльність державних органів у цій сфері та сприяє розвитку національної системи стратегічних комунікацій. Серед ключових напрямів роботи Центру – проведення інформаційно-просвітницьких кампаній, розробка методологій виявлення маніпулятивних та дезінформаційних матеріалів, а також організація тренінгів та семінарів з медіаграмотності. Центр протидії дезінформації регулярно публікує звіти та аналітичні статті, що стосуються актуальних інформаційних загроз та способів їх нейтралізації. Окрім того, Центр активно взаємодіє з громадськістю через офіційний вебсайт та сторінки в соціальних мережах, надаючи оперативну інформацію та роз'яснення щодо поточних подій.

Центр стратегічних комунікацій та інформаційної безпеки [24] це урядова організація, створена в березні 2021 року при Міністерстві культури та інформаційної політики України. Основною діяльністю Центру є протидія дезінформації та інформаційним загрозам, а також розбудова національної стійкості через співпрацю державних установ, громадянського суспільства та міжнародних партнерів. А також забезпечення цілісності інформаційного середовища України, підвищення обізнаності громадян про інформаційні загрози та зміцнення стійкості суспільства до дезінформації. Центр стратегічних комунікацій та інформаційної безпеки проводить аналіз інформаційного простору та моніторинг дезінформаційних наративів, розробляє комунікаційні стратегії для державних установ, працює над покращенням системи швидкого реагування на інформаційні загрози, підвищенням стійкості вразливих аудиторій через інформаційні кампанії та освітні заходи, а також співпрацює з громадянським суспільством у сфері протидії гібридним загрозам. Центр також організовує інформаційно-просвітницькі заходи для підвищення медіаграмотності населення. Офіційною платформою Центру стратегічних комунікацій та інформаційної безпеки є сайт **SPRAVDI** (Рис. 2.5.) [49], який слугує основним каналом поширення аналітичних матеріалів, фактчекінгових оглядів та роз'яснень щодо дезінформаційних кампаній і російських наративів.

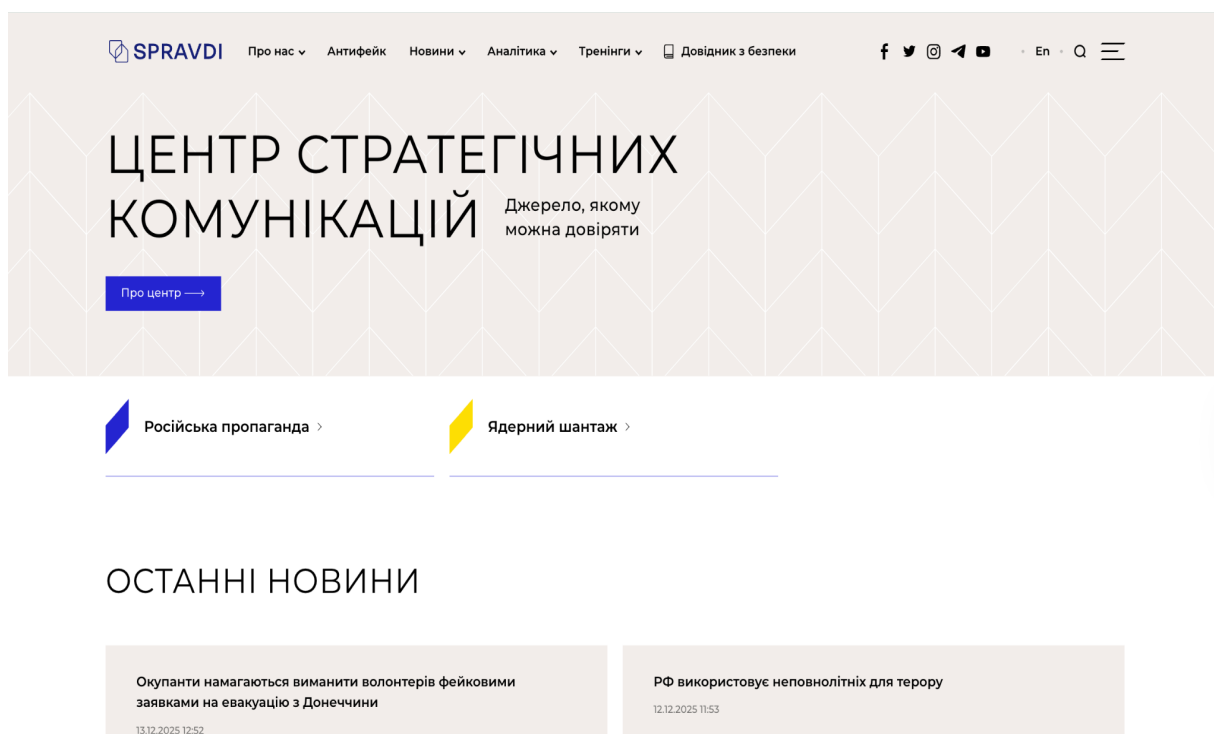


Рис. 2.5. SPRAVDI

Джерело: [49]

Суспільне мовлення України (Національна суспільна телерадіокомпанія України, НСТУ) було створено 19 січня 2017 року [22] на основі об'єднання державних телерадіоорганізацій відповідно до Закону України «Про суспільні медіа України» [21]. Його головна мета забезпечення об'єктивного, неупередженого та збалансованого інформування громадян, незалежного від політичного чи комерційного впливу. НСТУ має розвинену мережу регіональних філій, що забезпечують висвітлення місцевих новин та подій громади у всіх областях України. Підлаштовуючись під постійну потребу у швидкому отриманні достовірної інформації, новини розміщуються не тільки на регіональних сайтах, а також і у соцмережах і месенджерах місцевих каналів Суспільного. У своїй діяльності Суспільне мовлення дотримується журналістських стандартів достовірності, точності та балансу думок, що є одним із ключових інструментів протидії дезінформації. Під час повномасштабного вторгнення Росії Суспільне стало одним з основних джерел перевіреної інформації який покликаний забезпечити оперативне, достовірне й офіційно підтверджене інформування населення про ситуацію в країні. Також, у

2020 році НСТУ започаткували Дитячу академію суспільного (РМА Juniors) [4], це навчальний проєкт для дітей та підлітків. Дитяча академія була створена щоб допомогти розкрити творчий потенціал молоді, але останні роки все більше концентрується на розвитку критичного мислення, аналізу інформації в медіа та виявленню дезінформації.

Національна рада з питань телебачення і радіомовлення [9] є центральною інституцією, що забезпечує державний нагляд і регуляцію медіапростору, діяльність якої ґрунтується на положеннях Закону України «Про медіа» від 31 березня 2023 року № 2849–IX [14]. Вона здійснює моніторинг інформаційного простору, веде Реєстр суб'єктів у сфері медіа, наглядає за дотриманням журналістських стандартів і законодавчих обмежень щодо поширення забороненого контенту. Одним із ключових завдань Нацради є виявлення фактів поширення дезінформації, пропаганди війни, мови ворожнечі та інших проявів інформаційної агресії. У межах своїх повноважень Національна рада має право застосовувати санкції до суб'єктів медіа. Згідно зі Статтею 99 та Статтею 116 Закону «Про медіа», до порушників можуть бути застосовані попередження, штрафи або анулювання ліцензії. Розмір штрафу становить від п'яти до сорока п'яти мінімальних заробітних плат, залежно від характеру та наслідків порушення. У разі повторного або систематичного порушення Нацрада має право звернутися до суду щодо анулювання ліцензії або припинення діяльності медіа. Особливої ваги діяльність Нацради набуває під час воєнного стану, коли контроль за інформаційним простором є частиною системи національної безпеки.

Система інституційних механізмів протидії дезінформації в Україні є багаторівневою та взаємопов'язаною. Її ефективність забезпечується координацією між урядовими структурами, регуляторними органами та суспільним мовником, діяльність яких спрямована на захист інформаційного простору, підвищення медіаграмотності населення та формування стійкості суспільства до деструктивних інформаційних впливів. Централізована державна політика в поєднанні з незалежним регулюванням медіа створює основу для

побудови цілісної системи інформаційної безпеки, що відповідає сучасним викликам гібридної війни.

Громадські ініціативи та незалежні аналітичні центри.

В Україні протидія дезінформації значною мірою розвивається завдяки діяльності громадських організацій, аналітичних центрів та незалежних медіа. На відміну від державних структур, які потребували часу для формування нормативної бази та інституційних механізмів, громадський сектор виявився більш гнучким і швидше відреагував на нові виклики інформаційної війни. Завдяки цьому саме неурядові ініціативи першими почали системно здійснювати фактчекінг, аналітику медіаконтенту та просвітницьку діяльність у сфері медіаграмотності. Вони відіграють ключову роль у моніторингу інформаційного простору, підвищенні рівня критичного мислення громадян і формуванні стійкості суспільства до маніпуляцій. Нижче розглянуто найбільш впливові з них.

Одна з перших і найвідоміших українських ініціатив із перевірки фактів **StopFake** (Рис. 2.6.) [50], заснована в березні 2014 року викладачами та студентами Могиллянської школи журналістики НаУКМА. Проєкт виник як відповідь на масштабну хвилю російської дезінформації, що супроводжувала анексію Криму та початок війни на Донбасі. Від початку своєї діяльності StopFake зосередився на виявленні, аналізі та спростуванні фейкових повідомлень про Україну. Окрім фактчекінгу, організація проводить моніторинг інформаційного простору, аналітичні дослідження механізмів поширення пропаганди, а також освітні програми з медіаграмотності для журналістів, викладачів, студентів і широкої аудиторії. Матеріали публікуються українською, англійською, російською та одинадцяттю мовами, що дає змогу ефективно доносити правдиву інформацію до міжнародної спільноти.

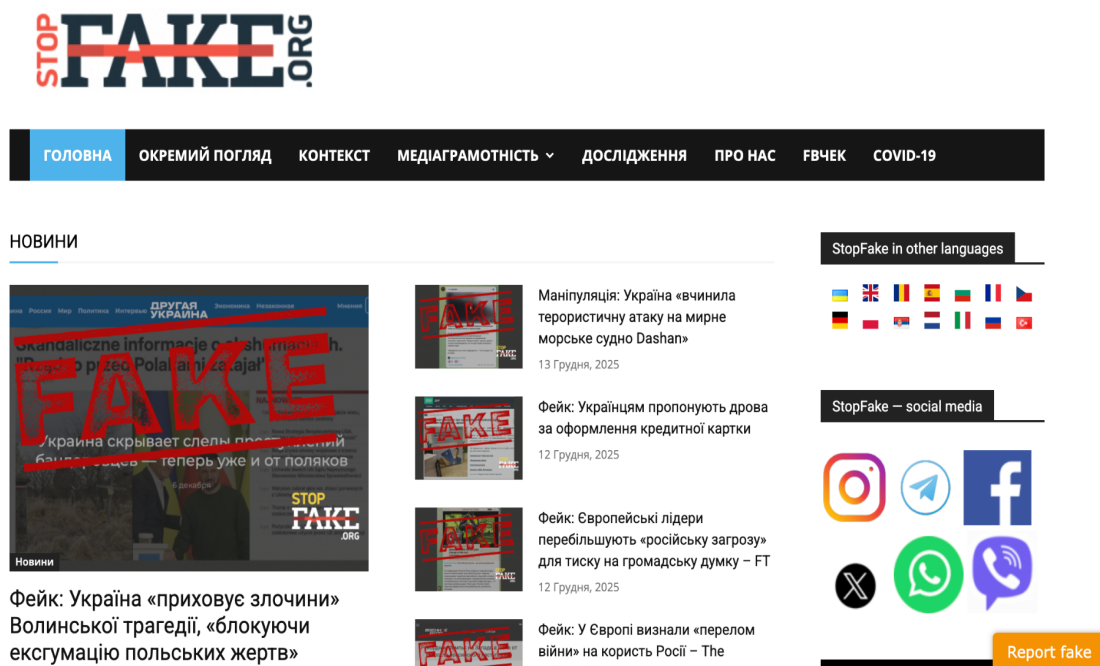


Рис. 2.6. StopFake

Джерело: [50]

StopFake також реалізує міжнародні освітні ініціативи у сфері протидії дезінформації. У співпраці з Google News Initiative, яка працює з видавцями та журналістами задля боротьби з дезінформацією, обміну ресурсами й розвитку інноваційної новинної екосистеми, команда StopFake провела серію тренінгів та воркшопів у країнах Європейського Союзу для поширення досвіду українських фактчекерів і розвитку професійного потенціалу європейських колег у сфері протидії фейкам і пропаганді.

Ще одна незалежна громадська організація **Detector Media** [32], заснована у 2016 році як продовження діяльності аналітичного проєкту «Телекритика», що функціонував із 2001 року. Організація займається дослідженням українського медіапростору, моніторингом телебачення, онлайн-ЗМІ та соціальних мереж, а також аналізом інформаційних кампаній, спрямованих на маніпулювання громадською думкою. Detector Media здійснює регулярний моніторинг політичних ток-шоу, новинних програм та суспільно-політичних матеріалів, фіксуючи порушення журналістських стандартів, прояви пропаганди та проросійських наративів.

Окрім аналітичної діяльності, організація активно розвиває напрям медіаосвіти, сприяючи підвищенню рівня медіаграмотності та критичного мислення громадян. Detector Media організовує публічні обговорення, тренінги та просвітницькі кампанії, публікує рекомендації для журналістів і медіаменеджерів щодо етичних стандартів та відповідального висвітлення тем, пов'язаних із війною, дезінформацією і гібридними загрозами. Організація також ініціює публічні дискусії щодо реформування медіасфери, сприяючи зміцненню стійкості українського суспільства до дезінформаційних впливів, а також надає експертні оцінки різних аспектів роботи ЗМІ.

Detector Media спільно з ІМІ у 2023 році започаткували проєкт «**Мапа рекомендованих медіа**» (Рис. 2.7.) [7], покликаний допомогти аудиторії орієнтуватися у великому розмаїтті українських медіа та знаходити якісні журналістські ресурси в усіх регіонах країни. Мапа є інтерактивною онлайн-платформою, що відображає якісні та прозорі редакції по всій Україні, які дотримуються професійних журналістських стандартів, забезпечують прозорість власності, не поширюють маніпуляцій, фейків чи мови ворожнечі. Завдяки «Масі рекомендованих медіа» користувачі отримують можливість обирати достовірні інформаційні джерела та бути впевненими в новинах які читають, а самі редакції підвищують рівень довіри аудиторії.

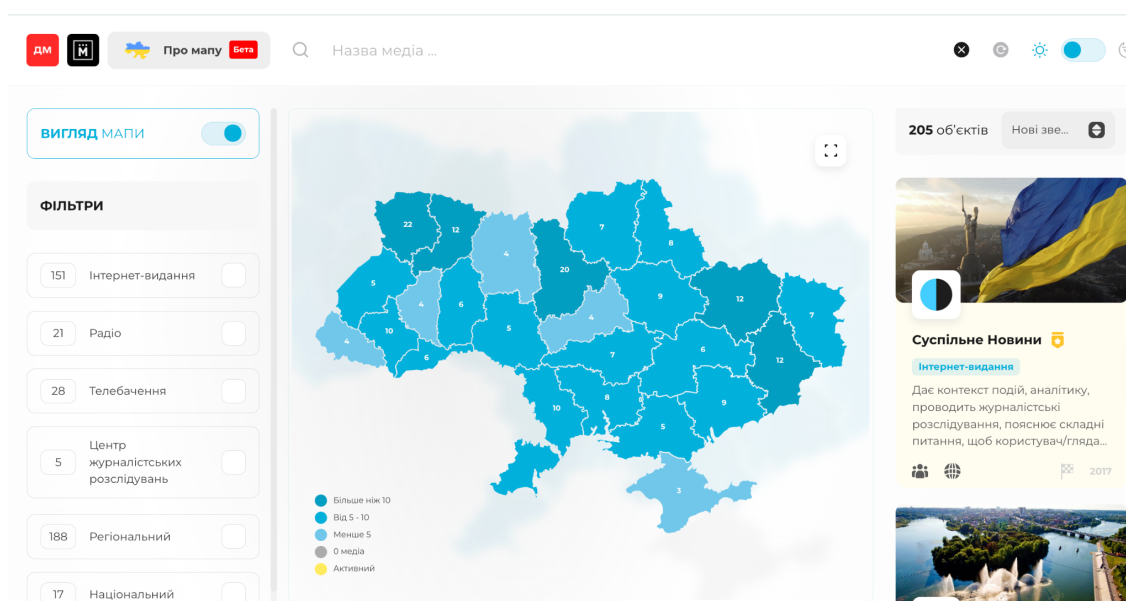


Рис. 2.7. Мапа рекомендованих медіа

Джерело: [7]

Інститут масової інформації (ІМІ) [5] це незалежна громадська організація, заснована в 1995 році, яка є одним із провідних аналітичних центрів у сфері захисту свободи слова, моніторингу журналістських стандартів та протидії дезінформації в Україні. ІМІ системно досліджує стан медіаринку, публікує аналітичні звіти про тенденції в інформаційному просторі, порушення прав журналістів, прояви пропаганди, мови ворожнечі та маніпуляцій у ЗМІ. Організація здійснює постійний моніторинг українських медіа, має широку мережу регіональних представників для фіксації локальних порушень, а також проводить тренінги з фактчекінгу та медіаграмотності для журналістів і редакцій. ІМІ розробляє методичні рекомендації з перевірки інформації, організовує адвокаційні кампанії на підтримку якісної журналістики та сприяє впровадженню єдиних стандартів у медіасфері. Завдяки своїй діяльності ІМІ відіграє ключову роль у формуванні стійкості українського медіапростору до дезінформації та інформаційних впливів, забезпечуючи професійну підтримку журналістської спільноти й розвиток критичного мислення в суспільстві.

Із 2019 року Інститут масової інформації публікує **«Білий список медіа»** (Рис. 2.8.) [2], це перелік найякісніших українських онлайн-видань, сформований за результатами піврічного моніторингу дотримання професійних стандартів. До списку входять загальноукраїнські медіа, що демонструють найвищі показники достовірності, балансу думок та відсутності маніпуляцій, фейків, джинси, сексизму чи мови ворожнечі. Середній рівень дотримання стандартів у медіа, які входять до списку, становить близько 96 %.

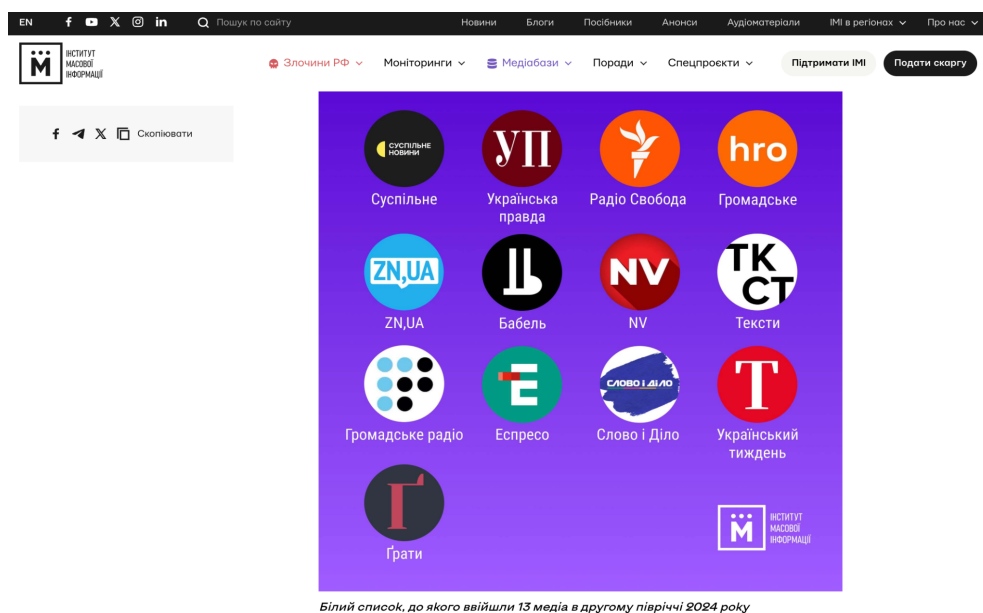


Рис. 2.8. Білий список медіа

Джерело: [2]

VoxCheck [58], незалежний фактчекінговий проєкт, створений у 2015 році командою аналітичного центру VoxUkraine. Основна мета ініціативи — підвищення рівня відповідальності політиків і публічних осіб за свої висловлювання, а також розвиток культури критичного мислення в українському суспільстві. Команда VoxCheck здійснює системну перевірку достовірності заяв політиків, публічних діячів і медіа, використовуючи відкриті джерела, офіційні статистичні дані та експертні коментарі. Окрім регулярного фактчекінгу, проєкт публікує аналітичні матеріали, присвячені поширенню дезінформації, маніпулятивним наративам і тенденціям у медійному просторі. Одним із ключових напрямів роботи є моніторинг російських дезінформаційних кампаній. Одним із помітних напрямів діяльності VoxCheck був проєкт **Propaganda Diary** (2022–2023) [46], присвячений моніторингу та класифікації російських дезінформаційних наративів у європейському інформаційному просторі. VoxCheck є членом міжнародної мережі IFCN (International Fact-Checking Network) та активно співпрацює з такими міжнародними платформами, як Facebook, для маркування фейків у соцмережах.

Ініціатива **UkraineWorld** [57] виникла як волонтерський проєкт Internews Ukraine щоб допомогти іноземним журналістам під час подій Євромайдану

2013–2014 років, а у 2017 році набула сталого інституційного формату. Її основною метою є пояснення подій в Україні міжнародній аудиторії, протидія дезінформації та поширення достовірної інформації англійською мовою. Проект поєднує елементи журналістики, аналітики та фактчекінгу, зосереджуючись на розвінчуванні російських дезінформаційних наративів у глобальному інформаційному просторі. Команда UkraineWorld готує аналітичні матеріали, подкасти, відео та звіти, присвячені політичним, соціальним і безпековим процесам в Україні, а також гуманітарним аспектам війни. Важливим напрямом діяльності є моніторинг міжнародних медіа та інформаційних кампаній, спрямованих на дискредитацію України. UkraineWorld також співпрацює із журналістами, експертами й дослідницькими центрами з різних країн, сприяючи формуванню міжнародної спільноти, стійкої до дезінформації. Навколо UkraineWorld сформовано мережу з понад 300 міжнародних журналістів та дослідників, які отримують оперативну аналітичну інформацію від українських фахівців. Аналітичні матеріали та коментарі експертів UkraineWorld регулярно цитуються провідними міжнародними медіа, такими як The New York Times, Financial Times, Le Monde, Atlantic Council, FRANCE 24.

Таким чином, діяльність українських громадських ініціатив і незалежних аналітичних центрів стала фундаментом національної системи протидії дезінформації. Їхня робота не лише сприяє оперативному спростуванню фейків, а й забезпечує розвиток медіаграмотності, критичного мислення та довіри до якісних джерел інформації.

Технологічні та OSINT-інструменти протидії дезінформації.

У сучасних умовах, коли поширення дезінформації здійснюється переважно в цифровому середовищі, технологічні рішення та OSINT-методи (Open Source Intelligence – розвідка на основі відкритих джерел) стають невід’ємним компонентом системи протидії інформаційним загрозам. Вони дозволяють не лише оперативно виявляти фейки, а й аналізувати джерела походження інформації, візуальні матеріали, а також структури бот-мереж, що поширюють пропагандистські наративи.

OSINT-інструменти широко застосовуються як у діяльності журналістів-розслідувачів, так і в роботі аналітичних центрів, громадських організацій та незалежних фактчекінгових ініціатив. Пошук першоджерел контенту, верифікація зображень, геолокація, аналіз мережевих взаємодій, забезпечують не лише оперативне спростування фейків, їх використання сприяє підвищенню прозорості інформаційного простору та забезпечує доказовість публікацій, а також формують доказову базу для міжнародних розслідувань злочинів проти України.

Одним із провідних українських проєктів, який активно використовує технологічні засоби для аналізу великих обсягів інформації, є аналітична платформа **Texty.org.ua** [52]. Вони спеціалізуються на журналістиці даних та аналізі інформаційних процесів в Україні. Створена у 2010 році команда Texty поєднує методи дата-журналістики, програмування та візуалізації для дослідження соціально значущих тем, включно з дезінформаційними кампаніями, діяльністю бот-мереж і поширенням маніпулятивних наративів у медіа та соціальних мережах. Організація здійснює контент-аналіз інформаційного простору, розробляє власні методики виявлення пропаганди й автоматизованого аналізу медіапотоків, а також публікує аналітичні звіти, policy briefs і розслідування за міжнародними стандартами. Завдяки поєднанню журналістики, аналітики й технологій, Texty.org.ua стали одним із провідних українських центрів аналітики даних, матеріали якого часто цитуються в наукових і медіадослідженнях. Дослідження команди неодноразово відзначалися міжнародними нагородами, зокрема Data Journalism Awards, Sigma Awards та іншими відзнаками у сфері журналістики даних.

Одним із найвідоміших українських проєктів, що спеціалізуються на застосуванні OSINT-методів для аналітики та розслідувань, є **Molfar** [41], незалежна розвідувально-аналітична агенція, створена у 2019 році. Команда Molfar розпочала роботу, зосереджуючись на приватних розслідуваннях і OSINT-дослідженнях, але після повномасштабного вторгнення Росії в Україну використовуючи власні ресурси Molfar створила доказову базу, яка

використовувалась для введення санкцій проти росіян, викриття воєнних злочинців і зрадників, пошуку дітей, викрадених Росією тощо. Використовуючи свої знання з розвідки з відкритих джерел вони почали робити розслідування для інформаційного спротиву Росії. З 2023 року Molfar значно розширили взаємодію з українськими та міжнародними медіаплатформами та беруть активну участь у підготовці та реалізації журналістських розслідувань, що висвітлювали суспільно важливі теми та забезпечують медіа аналітичною підтримкою, перевіркою фактів, збором відкритих даних (OSINT) та глибинною перевіркою фігурантів. У 2025 вони створили **Molfar Intelligence Institute** [42], окрему громадську організацію, яка проводить некомерційні розслідування, а також є освітньою платформою з OSINT, що навчає та розповідає про розвідку, алгоритми пошуку та етапи аналізу даних, як робити фактчекінг та основні правила інформаційної та цифрової безпеки. Фахівці Molfar також долучилися до впровадження основ OSINT та кібербезпеки в шкільну програму в Україні. Розслідування Molfar неодноразово публікувались такими провідними міжнародними медіа як The Telegraph, The Times, The Independent, The New York Times.

Міжнародна волонтерська спільнота **InformNapalm** [37], заснована у 2014 році вимушеним переселенцем із Криму, здійснює збір і верифікацію відкритих даних про участь Росії у війні проти України, зокрема ідентифікацію російських військовослужбовців, техніки та підрозділів, задіяних у бойових діях. Їхня діяльність не лише документує воєнні злочини, але й розкриває структуру російських інформаційно-психологічних операцій. Одне з напрямлень їх діяльності це спростовування російської пропаганди. Сайт InformNapalm працює в 30 мовних версіях. Результати розслідувань InformNapalm неодноразово були представлені офіційними українськими делегаціями на засіданнях Парламентської асамблеї Ради Європи, НАТО й ОБСЄ, а також долучені до позову України проти Росії в Європейському суді з прав людини.

Ще одна унікальна ініціатива **DeepState** [30], яка починалась як новинний телеграм-канал у 2020 році, 24 лютого 2022 року запустила

інтерактивну карту, яка стала одним із найвідоміших джерел верифікованої інформації про перебіг бойових дій в Україні. Команда DeepState використовує методи OSINT, геолокаційний аналіз та супутникові знімки для створення інтерактивної карти війни, яка оновлюється в режимі реального часу на основі перевірених відкритих даних і офіційних повідомлень. Платформа стала інструментом не лише ситуаційної обізнаності, а й підвищення прозорості у воєнних повідомленнях, що зменшує потенціал дезінформаційних спекуляцій зі сторони Росії про хід бойових дій, уточненню інформації щодо звільнених або окупованих територій і фіксації воєнних злочинів. Постійне оновлення інформації з передової та зручний формат зробили DeepState важливим джерелом для багатьох українців, також карта використовується військовими аналітиками та українськими медіа. Інформація про DeepState цитувалася такими виданнями як BBC News, Forbes та The New York Times.

Таким чином, поєднання технологічних рішень, інструментів відкритої розвідки та громадських OSINT-ініціатив створює ефективну екосистему протидії дезінформації, що зміцнює інформаційну стійкість українського суспільства та підвищує рівень прозорості в глобальному медіапросторі.

Висновки до другого розділу

Російська дезінформаційна кампанія в Україні є постійним і гнучким інструментом гібридної війни. Це складний багатовимірний процес, який постійно адаптується до змін інформаційного середовища й застосовує комплекс тактик від класичної пропаганди до сучасних цифрових технологій і психологічних операцій. Вона змінює форми, але не мету — послабити Україну зсередини, позбавити її суспільної стійкості та зруйнувати довіру до власних інституцій.

Еволюція ведення дезінформації пройшла кілька етапів — від відкритого поширення через традиційні медіа до складних мережових і регіонально маскованих форматів, із широким використанням мікротаргетингу та багатоканальності впливу. Ключовим викликом є те, що сучасна російська

дезінформація дедалі менше виглядає як «пропаганда» — вона інтегрується у звичний український інформаційний простір, використовуючи локальні джерела, мову і факти в перекрученому контексті.

Водночас Україна активно протидіє цим загрозам на різних рівнях. Державні інституції створюють системні механізми боротьби з дезінформацією, моніторять медіапростір та розробляють стратегії інформаційного захисту. Громадські ініціативи та незалежні аналітичні центри першими реагують на нові загрози, здійснюють фактчекінг, аналізують медіаконтент і проводять просвітницькі кампанії. Сучасні технології та OSINT-інструменти дозволяють виявляти фейки, аналізувати джерела та структури поширення дезінформації, що підвищує прозорість інформаційного простору і формує доказову базу для міжнародних розслідувань.

Протидія дезінформації в Україні є постійним, адаптивним процесом, який потребує швидкої реакції та коригування підходів у відповідь на нові виклики. Державні органи, громадські ініціативи та технологічні платформи змінюють свої методи і стратегії, щоб ефективно протистояти різноманітним формам інформаційного впливу та мінімізувати наслідки маніпуляцій для суспільства.

Таким чином, протидія дезінформації в Україні є комплексною та багаторівневою, поєднуючи державні заходи, громадську активність та технологічні рішення. Це дозволяє підвищувати медіаграмотність населення, зміцнювати стійкість суспільства до маніпуляцій і захищати національну безпеку в умовах гібридної агресії.

РОЗДІЛ 3

ОСОБЛИВОСТІ МІЖНАРОДНОГО ДОСВІДУ У ПРОТИДІІ ДЕЗІНФОРМАЦІЇ

У контексті глобальної цифровізації та зростання ролі інформації як інструмента політичного впливу дезінформація перетворилася на один із ключових викликів для демократичних держав. Масштабність і системність сучасних інформаційних операцій свідчать про їхню здатність впливати на суспільні настрої, послаблювати інституційну стійкість і створювати сприятливі умови для зовнішньополітичного тиску. Для України, яка протягом багатьох років перебуває в умовах гібридної агресії Російської Федерації, ці загрози мають особливо гострий характер. Тому актуальним є звернення до міжнародного досвіду держав, що сформували ефективні механізми інформаційної стійкості, та виявлення можливостей використання цих підходів в українських умовах, з урахуванням специфіки війни та довготривалої інформаційної загрози.

3.1. Архітектура протидії дезінформації в міжнародній практиці

Інституційні механізми протидії дезінформації в Європейському Союзі.

Сучасна система протидії дезінформації в Європейському Союзі не обмежується регуляторними документами, такими як EU Code of Practice on Disinformation та Digital Services Act. Вона включає розгалужену мережу дослідницьких, аналітичних та стратегічних структур, що забезпечують виявлення, аналіз та стримування інформаційних загроз.

Інституційна система протидії дезінформації в Європейському Союзі вибудована за поліцентричним принципом, вона не утворює жорсткої адміністративної вертикалі, а складається з автономних, але взаємодоповнюючих центрів експертизи. У межах такої моделі науково-дослідницькі інфраструктури, урядові підрозділи та спеціалізовані

аналітичні рамки виконують окремі функції, які разом формують комплексну відповідь на зовнішні інформаційні загрози.

Важливою складовою інституційної архітектури ЄС у сфері боротьби з дезінформацією є **East StratCom Task Force**, створена у 2015 році в межах Європейської служби зовнішніх дій (European External Action Service, EEAS) як відповідь на хвилю російських інформаційних операцій після початку агресії РФ проти України у 2014 році. У документі «Action Plan on Strategic Communication» [27] вперше було продемонстровано, що дезінформація розглядається не як побічний продукт інформаційного шуму, а як «цілеспрямована зовнішня інформаційна атака, що має стратегічні військово-політичні цілі». East StratCom Task Force працює на принципах проактивної комунікації та аналітичного відслідковування наративів, що дозволяє не лише спростовувати окремі фейки, а й моделювати довготривалі інформаційні стратегії. Підрозділ здійснює моніторинг багатомовного медіапростору, виявляє повторювані патерни, класифікує їх за тематичними тегамі (військова сфера, міжнародні відносини, економіка, етнічні конфлікти) та координує реакції між інституціями ЄС. Особлива увага приділяється аналізу інформаційних впливів у країнах Східного партнерства, де уразливість медійних екосистем використовується в інтересах Росії для гібридної ескалації.

East StratCom Task Force розробив методологію «наративної аналітики», у якій ключовим є не виявлення факту неправдивості інформації, а розуміння політичної функції наративу: делегітимація демократичних інституцій, дискредитація України та ЄС, підриг довіри до західних союзницьких механізмів. Такий підхід відрізняється від класичного фактчекінгу, який фокусується на точності тверджень, тоді як стратегічна комунікація виходить з аналізу інтерпретаційних рамок та намірів актора.

Одним із ключових інструментів підрозділу є платформа **EUvsDisinfo** [29], заснована у 2015 році як офіційний проєкт ЄС для документування та аналізу російських дезінформаційних кампаній. База даних EUvsDisinfo містить більше дев'ятнадцяти тисяч задокументованих кейсів, що фіксують конкретні

прикладі маніпуляцій, їхнє походження, механізми поширення та повторювані наративи. На платформі представлена структурована інформація про еволюцію пропагандистських меседжів, їхню адаптацію до різних мовних та регіональних контекстів, а також про роль державних і афілійованих із РФ медіа у формуванні і трансляції цих наративів. Завдяки регулярному оновленню і дотриманню прозорої методології EUvsDisinfo виконує функцію доказової бази, яка дозволяє відтворювати динаміку інформаційних атак, а також забезпечує інформаційну підтримку для рішень органів ЄС у сфері стратегічних комунікацій.

Однак для цілісного розуміння та документування інформаційних операцій ЄС потребував уніфікованої аналітичної методології. Саме тому останніми роками центральним інструментом оцінки інформаційних впливів стала рамка **Foreign Information Manipulation and Interference (FIMI)** [28], яку системно застосовує Європейська служба зовнішніх дій (EEAS).

З 2022 року Європейська служба зовнішніх дій публікує EEAS Report on Foreign Information Manipulation and Interference (FIMI) – аналітичні звіти, у яких дезінформація аналізується не через точковий фактчекінг, а як цілісний тип поведінки акторів міжнародної політики. Згідно з методологією FIMI, інформаційні операції розглядаються як «переважно не незаконна, маніпулятивна та в багатьох випадках скоординована форма зовнішньої інформаційної діяльності, що здатна негативно впливати на політичні процеси, цінності та демократичні процедури» [26].

У звітах FIMI використовується модель поведінкового відбитка (behavioural fingerprinting), аналітики визначають не окремі повідомлення, а параметри деструктивної діяльності – координація між акаунтами, неавтентичні патерни публікацій, використання бот-мереж, повторюваність повідомлень у різних мовних сегментах. Такий аналіз дозволяє виявляти архітектуру інформаційної операції, встановлювати геополітичну мотивацію та оцінювати масштаб можливого впливу на демократичні процеси. FIMI не лише фіксує прояви впливу, але й забезпечує урядові структури даними для дипломатичних

дій, санкцій, обмеження мовлення пропагандистських ресурсів або попередження іноземних урядів. Згідно зі звітом EEAS за 2024 рік, основним актором, що здійснює системні інформаційні атаки проти Європейського Союзу та країн-партнерів, залишається Російська Федерація.

Забезпечити практичне застосування цих аналітичних підходів у дослідницькому, освітньому та фактчекінговому середовищі Європейського Союзу дозволяє розгалужена науково-експертна інфраструктура, центральним елементом якої виступає **European Digital Media Observatory (EDMO)** (Європейська обсерваторія цифрових медіа) [55]. Це незалежна ініціатива Європейського Союзу, створена для підтримки боротьби з дезінформацією через дослідження, перевірку фактів та співпрацю між зацікавленими сторонами. EDMO розпочала свою діяльність у червні 2020 року за фінансової підтримки Європейської комісії. Обсерваторія об'єднує дослідницькі центри, університети, журналістів, фактчекерів та експертів із цифрових технологій, сприяючи розробці ефективних стратегій протидії інформаційним загрозам. Основними завданнями EDMO є аналіз механізмів поширення дезінформації в онлайн-середовищі, надання підтримки національним та регіональним центрам з перевірки фактів, розвиток медіаграмотності серед громадян та сприяння доступу незалежних дослідників до даних цифрових платформ. Обсерваторія також співпрацює з органами ЄС у сфері імплементації «The Code of Conduct on Disinformation» та оцінки ефективності заходів, які вживають цифрові платформи для обмеження поширення маніпулятивного контенту. Також, EDMO відіграє важливу роль у реалізації Digital Services Act (DSA), оскільки забезпечує незалежний аналіз інформаційних загроз та сприяє формуванню доказової бази для ухвалення регуляторних рішень у ЄС.

Таким чином, поліцентрична модель протидії дезінформації ЄС об'єднує науковий потенціал EDMO, стратегічно-комунікаційні інструменти East StratCom Task Force та стандартизовані аналітичні методики FIMI в одну функціональну систему. Її сила полягає саме у взаємодоповненості різних інституційних рівнів, що дозволяє Європейському Союзу не лише виявляти

інформаційні операції, а й реагувати на них у регуляторному, дипломатичному та комунікаційному вимірах.

Моделі протидії дезінформації в міжнародній практиці.

У міжнародній практиці протидії дезінформації особливе місце посідають країни Північної Європи та Балтійського регіону, що стабільно демонструють високий рівень інформаційної грамотності населення та низьку вразливість до інформаційно-психологічних впливів. За даними Media Literacy Index 2023 [40] перші позиції займають Фінляндія, Данія, Норвегія, Естонія та Швеція. Стійкість цих держав до дезінформації пояснюється не лише рівнем розвитку інформаційної культури або якістю освіти, а й наявністю комплексних державних стратегій, інституційної підтримки та системної інтеграції медіаграмотності в освітні стандарти.

Значна частина міжнародних практик виходить з концепції інформаційної стійкості (information resilience). Найрезультативнішим прикладом є **Фінляндія**, де елементи медіаграмотності інтегровані в навчальні програми з дошкільного рівня [43]. Цей підхід не спрямований на боротьбу з окремими фейками, а формує здатність громадян критично оцінювати джерела, розпізнавати маніпулятивні наративи та уникати когнітивних пасток.

На відміну від більшості держав Європи, фінська система медіаосвіти не є реакцією на сучасні загрози, а становить результат довгострокової політики, закладеної в державні документи та навчальні стандарти ще у 2000-х роках. Ключову роль у розробці цієї політики відіграє Міністерство освіти та культури, яке в співпраці з Національним аудіовізуальним інститутом (KAVI) [56] здійснює методичну підтримку вчителів, створює навчальні ресурси та відповідає за інтеграцію медіаосвіти в шкільну програму. У сучасній фінській системі освіти медіаграмотність не виступає окремою навчальною дисципліною, а формується як наскрізна компетентність, присутня в різних предметах початкової та середньої школи. Така інституційно-освітня інтеграція не лише сприяє формуванню критичного мислення з раннього віку, але і

створює умови, за яких громадяни сприймають інформаційні ризики не як зовнішню загрозу, а як частину повсякденних комунікацій.

Данія демонструє дещо відмінний підхід, який можна визначити як педагогічну модель інформаційної стійкості. На відміну від концепції, що передбачає загальне формування критичного мислення як універсальної компетентності, у данському дискурсі акцент зміщується на педагогічні інструменти, підготовку вчителів та створення дидактичних матеріалів, спрямованих на роботу з конкретними типами інформаційних загроз. Відповідні освітні ресурси інтегровані в національні шкільні програми, включаючи модулі з медіаграмотності, цифрової грамотності, розпізнавання маніпуляцій у соціальних мережах, розуміння алгоритмів платформ і безпечної поведінки в онлайн-середовищі. Медіаосвіта реалізується не лише в межах загальної освіти, а й через державні інформаційні ресурси, створені спеціально для педагогів, шкіл і бібліотек, що дозволяє формувати адаптивні навчальні практики відповідно до розвитку цифрового середовища. Значна частина освітніх інструментів, зокрема на порталі EMU – Danmarks læringsportal [36], спрямована на роботу з конкретними проявами дезінформації, включаючи фейкові новини, візуальні маніпуляції, а також діпфейки, які вважаються однією з ключових загроз.

Норвегія демонструє комплексний підхід, та орієнтується на поєднання медіаосвіти, цифрової грамотності та розвитку відповідального інформаційного споживання, що охоплює як шкільний, так і позашкільний сектор. Особливістю норвезької моделі є активне залучення громадських і культурних інституцій, насамперед бібліотек, культурних центрів та громадських платформ, які виступають просторами формування навичок критичного аналізу інформації та медіаграмотності в дорослого населення. Цей підхід відображений у національних стратегіях цифрової компетентності та інформаційної безпеки, де підкреслюється необхідність посилення суспільної стійкості до інформаційних впливів та застосування медіаосвітніх інструментів як у школах, так і за межами формальної освіти [44]. Важливу роль відіграє державна політика із

цифрової освіти дітей і молоді, яка передбачає співпрацю між урядом, освітнім сектором і медіаорганізаціями з метою попередження дезінформації в онлайн-середовищі та захисту підлітків від онлайн-маніпуляцій [45].

Естонія посідає особливе місце серед держав, що мають тривалий досвід російського інформаційного впливу, що зумовлює орієнтацію державної політики не лише на протидію дезінформації, але й на стратегічні підходи до інформаційної безпеки. Особливістю естонської моделі є її проактивний цифровий курс, який сформувався після масштабної кібератаки 2007 року та визначив пріоритет у побудові державних сервісів і оборонної інфраструктури. Цей підхід поєднує елементи кіберзахисту й інформаційної стійкості та розглядається урядом як необхідна умова протидії зовнішнім інформаційним впливам [38]. Модель Естонії базується на загальносуспільному підході, у якому освіта, цифрова грамотність та компетентність громадян розглядаються як основа для розпізнавання маніпулятивних наративів і підвищення суспільної стійкості. Важливу роль у цьому напрямі відіграє Estonian Atlantic Treaty Association (EATA) [33], яка реалізує освітні програми та публічні кампанії, спрямовані на формування критичного мислення і розпізнавання пропагандистських впливів. На міжнародному рівні Естонію вважають одним із лідерів кібердипломатії та формування міжнародних норм у цифровому просторі, зокрема в рамках співпраці з ЄС та НАТО.

Швеція демонструє унікальну модель, модель психологічної оборони. У 2022 році держава створила Swedish Psychological Defence Agency [47], метою якої є підвищення здатності населення розпізнавати інформаційні впливи та зменшувати їхню ефективність. На відміну від попередніх моделей, шведська система поєднує медіаосвіту з елементами стратегічних комунікацій та психологічної стійкості, що структурно наближає її до сфер національної безпеки. В офіційних урядових документах психологічна оборона визначається як комплекс заходів, спрямованих на захист демократичних інституцій та формування здатності громадян сприймати кризові повідомлення без впливу дезінформації.

Таким чином, аналіз міжнародної практики засвідчує існування кількох відмінних, проте взаємно доповнювальних моделей інформаційної стійкості, спільною рисою яких є довготривала стратегія формування компетентностей громадян, а не спонтанне реагування на інформаційні загрози. Відмінності пояснюються історичними обставинами, рівнем загроз та політичною структурою, що дозволяє розглядати цей досвід як репрезентативний для формування власної системи протидії дезінформації в Україні.

3.2. Перспективи вдосконалення системи протидії дезінформації в Україні (на основі міжнародного досвіду)

Після більш ніж одинадцяти років безперервної інформаційної агресії Російської Федерації, Україна накопичила унікальний практичний досвід протидії дезінформації, який у низці аспектів випереджає європейські та міжнародні підходи. На відміну від держав ЄС, де проблема дезінформаційних кампаній усвідомлювалася переважно в контексті виборчих процесів, цифрової безпеки чи інформаційної культури, для України питання інформаційної стійкості від початку мало стратегічне, а після 2014 року безпосередньо безпекове та оборонне значення. Саме тому становлення українських інституцій, практик фактчекінгу, OSINT-спільнот та стратегічних комунікацій відбувалося не стільки як елемент державної інформаційної політики, скільки як реакція на реальний воєнний тиск та необхідність збереження суверенітету.

Повномасштабне вторгнення РФ у 2022 році лише підтвердило, що дезінформація використовується державою-агресором як структурний елемент гібридних операцій, спрямованих на деморалізацію населення, дискредитацію державних інституцій, руйнування міжнародної підтримки України й управління громадською думкою за межами українських кордонів. У цьому контексті досвід України стає не лише внутрішнім інструментом національної безпеки, а й потенційною моделлю для європейських партнерів, які лише після 2022 року почали системно перебудовувати політику протидії дезінформації,

зокрема через Digital Services Act, оновлений Кодекс практики ЄС та ініціативи East StratCom.

Разом із тим, попри наявність важливих інституційних та громадських механізмів, українська система поки що залишається фрагментованою та неоднорідною, а стратегічні функції розподілені між різними суб'єктами без достатнього рівня координації. Отже, зараз особливої актуальності набуває завдання розробки інтегрованої моделі протидії дезінформації, яка б відповідала специфічним умовам воєнного стану, а також враховувала перспективу післявоєнного відновлення та міжнародної інтеграції.

Вдосконалення української системи протидії дезінформації може відбуватися за кількома ключовими напрямками, які відображають успішні міжнародні практики:

Інституціоналізація комплексної інформаційної стійкості.

Україні доцільно перейти від реактивної політики (спростування окремих фейків) до проактивної стратегії, що передбачає системне формування інформаційної стійкості суспільства в довгостроковій перспективі. За аналогією зі Шведським агентством психологічної оборони, такий напрям має зосереджуватися не лише на реагуванні, а на попередженні, підготовці населення до розпізнавання інформаційних впливів, зменшенні ефективності психологічних операцій противника та підвищенні здатності суспільства до колективної саморегуляції в кризових умовах.

В українських умовах, особливо в контексті активних російських психологічних операцій, така інституціоналізація має включати не лише державні органи, а і громадський сектор, медіаспільноту, дослідницькі центри та локальні громади. Фактично йдеться про формування загальнонаціональної системи «інформаційної оборони», яка працюватиме не епізодично, а на постійній основі.

Інтеграція медіаграмотності в освітню систему.

Другим стратегічним напрямом є поглиблення інтеграції медіаграмотності в освітні стандарти, що вже продемонструвало ефективність у

Фінляндії та Данії. При цьому український контекст вимагає розширення підходу, медіаграмотність має бути не окремою дисципліною, а наскрізною компетентністю в різних предметах, починаючи з дошкільної освіти та закінчуючи підготовкою дорослого населення.

Особливу увагу необхідно приділити підготовці вчителів, оскільки саме вони є ключовим посередником у формуванні критичного мислення, та створенні дидактичних матеріалів для роботи з конкретними типами загроз (візуальні маніпуляції, діпфейки, алгоритми платформ).

Важливо, що в умовах війни медіаграмотність дорослого населення не менш важлива, ніж шкільна. Тому варто використовувати громадські та культурні центри, бібліотеки, а також пенсійні фонди та служби зайнятості для формування навичок критичного аналізу інформації серед дорослого населення.

Формування локальної інформаційної стійкості громад.

Зважаючи на те, що дезінформація в Україні часто має регіональну специфіку, важливим напрямом є підтримка локальних комунікаційних центрів, локальних журналістів, редакцій та громадських ініціатив, які працюють безпосередньо з населенням на місцевому рівні. Особливо це стосується невеликих громад, де інформаційна ситуація є найбільш вразливою і де російські інформаційні впливи нерідко спрямовані на створення панічних настроїв, деморалізацію або руйнування довіри до державних інституцій.

Важливо підкреслити, що локальні медіа виконують не лише функцію новинного інформування, але і є одним із головних джерел для населення. Проте в умовах повномасштабної війни більшість місцевих редакцій втратили традиційні джерела фінансування, насамперед рекламні надходження. Це призводить до скорочення штату, призупинення діяльності, а інколи й повного закриття локальних медіапроектів. У результаті аудиторія, залишившись без звичних перевірених джерел інформації, дедалі частіше звертається до незрозумілих телеграм-каналів та сторінок у Facebook, де активно працюють пропагандистські бот-мережі.

Таким чином, підтримка локальних медіа є не лише питанням інформаційної політики, але й елементом національної безпеки. Потрібно розробляти програми грантової, фінансової чи організаційної підтримки, створювати умови для продовження їхньої діяльності та сприяти їхній інтеграції в національну систему протидії дезінформації. У перспективі саме локальні медіа можуть стати опорними центрами інформаційної стійкості громад, виконуючи функцію перевірки фактів, пояснення державної політики, боротьби з панічними вкидами та протидії локальним інформаційним атакам.

Посилення аналітичних можливостей та співпраці.

Окремим стратегічним напрямом є розвиток національних аналітичних спроможностей щодо виявлення, класифікації та прогнозування інформаційних впливів. В українських умовах ця робота потребує не лише технологічної модернізації, але й комплексної координації між державними установами, фактчекінговими організаціями, університетами, OSINT-спільнотами та міжнародними партнерами.

Передусім варто підкреслити, що в Україні вже сформовано значний потенціал незалежних аналітичних ініціатив, проте їхня діяльність залишається фрагментованою, що ускладнює кумуляцію даних і використання результатів аналізу для ухвалення державних рішень. Бракує єдиного аналітичного простору, до якого надходили б дані не лише від державних структур, але й від дослідницьких спільнот, медіа та міжнародних партнерів.

Враховуючи те, що російські інформаційні кампанії є комплексними, багаторівневими та технологічно різноманітними, Україні необхідно створювати системи, здатні аналізувати не тільки контент, але і його джерела, маршрути поширення та поведінкові моделі аудиторій. У цьому контексті має значення спільна робота державних структур із цифровими платформами, науковими центрами та громадським сектором.

Особливо важливо розвивати міжнародне співробітництво в межах ЄС, оскільки нові методи інформаційних впливів здебільшого тестуються Росією на українському інформаційному просторі, а лише потім експортуються у

європейські країни. Тому Україна повинна виступати не лише «користувачем» європейського досвіду, а і його джерелом, транслуючи власні розробки, аналітичні підходи та результати досліджень на міжнародному рівні.

У перспективі доцільно формувати мережеву систему співпраці, яка поєднуватиме державні інституції, фактчекінгові центри, медіа, академічні структури, технологічні компанії та міжнародні організації. Такий формат забезпечить повніший аналіз інформаційної екосистеми й дозволить перейти від реактивного реагування до проактивного попередження дезінформаційних кампаній.

Запровадження посиленого регулювання цифрового простору.

Ще одним важливим напрямом є розвиток правового регулювання цифрового простору та встановлення чітких механізмів відповідальності за поширення дезінформації в онлайн-середовищі. В останні роки в Україні вже здійснено низку кроків у цьому напрямі, зокрема ухвалено Закон «Про медіа»[14] та започатковано реформу медійного законодавства з урахуванням європейських стандартів. Однак ці процеси залишаються порівняно повільними, а правові механізми нерідко виявляються «сирими» з огляду на потреби воєнного часу.

На відміну від країн Європейського Союзу, які перейшли до обов'язкового регулювання цифрових платформ (насамперед через Digital Services Act), Україні поки бракує дієвих інструментів впливу на цифрові сервіси, що активно використовуються для поширення ворожих інформаційних кампаній. Водночас механічне перенесення європейських регуляцій в український контекст є недостатнім, адже в умовах війни дезінформація має не лише інформаційний, але й безпековий характер, спрямований на підрив обороноздатності, деморалізацію населення та зниження міжнародної підтримки.

Тому необхідно посилювати нормативні інструменти, які забезпечуватимуть оперативне реагування на дезінформаційні кампанії, передбачатимуть співпрацю з платформами щодо маркування і обмеження

російських пропагандистських ресурсів, а також встановлюватимуть юридичні механізми притягнення до відповідальності організованих мереж, що систематично поширюють шкідливий контент.

У перспективі доцільно розробити комплексну нормативну рамку, яка дозволить не лише реагувати на дезінформацію постфактум, а й попереджати її появу в цифровому середовищі, забезпечуючи інформаційну безпеку держави та громадян.

Запропонована модель протидії дезінформації – це багаторівнева стратегія стійкості (Додаток А). Перелічені напрями не є ізольованими, оскільки вони відображають взаємодоповнюючі елементи єдиної системи інформаційної безпеки. У сукупності вони формують підґрунтя для переходу від фрагментарної, переважно реактивної протидії дезінформації до проактивної моделі інформаційної оборони, що поєднує інституційні, технологічні, освітні та регіональні компоненти.

Таким чином, в умовах повномасштабної війни та постійної загрози інформаційного впливу така комплексність є ключовою передумовою формування стійкого інформаційного середовища. Запропонована модель передбачає не лише оперативне реагування на поточні інформаційні атаки, але і зміцнення довгострокової інформаційної стійкості суспільства, завдяки чому воно стає менш вразливим до маніпуляцій, деструктивних інформаційних кампаній та інших форм гібридного впливу.

Висновки до третього розділу

У третьому розділі було проаналізовано міжнародний досвід протидії дезінформації та окреслено перспективи його адаптації в українських умовах. Дослідження показало, що сучасні підходи в Європейському Союзі та країнах Північної і Балтійської Європи ґрунтуються не стільки на окремих актах регулювання, скільки на комплексних, довгострокових стратегіях формування інформаційної стійкості суспільства.

Інституційна модель протидії дезінформації в ЄС побудована за поліцентричним принципом і включає низку взаємодоповнювальних структур які утворюють цілісний простір, у якому поєднуються стратегічні комунікації, наративна аналітика, оцінка інформаційних операцій як типу поведінки зовнішніх акторів та створення доказової бази для регуляторних і дипломатичних рішень. Така система дозволяє не лише фіксувати окремі випадки дезінформації, а й виявляти структурні закономірності інформаційних атак і реагувати на них у різних політичних і правових вимірах.

Аналіз практик Фінляндії, Данії, Норвегії, Естонії та Швеції засвідчив, що ключовим чинником стійкості до дезінформації є системна інтеграція медіаграмотності, цифрової та інформаційної компетентності в освіту й ширший суспільний контекст. У цих країнах медіаграмотність розглядається як наскрізна компетентність, що формується з раннього віку, а в окремих випадках напряду пов'язується з національною безпекою та стратегічними комунікаціями держави.

Український досвід, розглянутий крізь призму міжнародних моделей, показує наявність значного й у багатьох аспектах випереджального потенціалу. Водночас існуюча система залишається фрагментованою, спостерігається нестача координації між державними органами, громадським сектором і цифровими платформами, відсутній єдиний аналітичний простір, а правові механізми регулювання цифрового середовища не завжди відповідають динаміці сучасних інформаційних операцій у воєнних умовах.

Узагальнення міжнародного досвіду та українського контексту дозволило сформулювати запропоновану в роботі модель протидії дезінформації як багаторівневу стратегію стійкості. Вона поєднує інституційні, освітні, аналітичні, регіональні та регуляторні компоненти й орієнтована на перехід від фрагментарних, ситуативних заходів до цілісної, проактивної моделі інформаційної оборони. Такий підхід дає підстави розглядати український досвід не лише як приклад адаптації європейських практик, але і як потенційне

джерело інноваційних рішень для міжнародної спільноти в умовах гібридної війни та довготривалої інформаційної агресії.

ВИСНОВКИ

У першому розділі відповідно до першого першого дослідницького завдання був проведений аналіз теоретико-методологічних засад дослідження дезінформації та встановлено, що це явище є складним, багатоаспектним і динамічним інструментом інформаційного впливу, який сформувався історично, але зазнав принципової трансформації в умовах розвитку цифрових медіа та гібридних конфліктів.

Здійснене теоретичне опрацювання різних підходів до визначення дезінформації показало відсутність єдиного універсального її трактування, що зумовлено міждисциплінарністю феномену та розмаїттям контекстів його застосування. Узагальнення існуючих концепцій дозволило окреслити дезінформацію як навмисне, цілеспрямоване поширення викривлених або маніпулятивно інтерпретованих відомостей, спрямованих на когнітивний вплив на аудиторію з метою отримання політичної, військової чи соціальної переваги.

Також, проведений аналіз дав змогу виокремити основні характеристики дезінформації – навмисність, цільову орієнтованість, когнітивна складність, контекстуальну адаптивність і здатність до маскуванню. Виявлено, що дезінформація функціонує не лише як форма перекрученої інформації, а й як системний інструмент комунікаційних операцій, що поєднує інформаційні, психологічні та емоційні впливи. Класифікація її видів (пряма фальсифікація, напівправа, інформаційний «шум», фабрикація контексту, термінологічна маніпуляція тощо) стала теоретичною основою подальшого аналізу дезінформаційних практик Російської Федерації.

У межах вивчення нормативно-правового забезпечення протидії дезінформації в Україні та ЄС було з'ясовано, що обидві правові системи демонструють поступову інституціоналізацію реагування на інформаційні загрози, однак відмінні за своїми принципами та темпами розвитку.

Українська правова база інтенсивно формувалася після 2014 року як відповідь на комплекс російських інформаційних операцій. Нормативно-правові акти спрямовані на забезпечення інформаційної безпеки, регулювання

діяльності медіа, протидію пропаганді держави-агресора та створення інституційних механізмів взаємодії державних структур.

Правова система ЄС, навпаки, надає перевагу не санкційним, а регуляторним, координаційним та превентивним механізмам. Європейська модель акцентує увагу на поліцентричності, прозорості онлайн-середовища, співрегулюванні з приватними платформами та розвитку медіаграмотності. Порівняльний аналіз продемонстрував, що українська система значною мірою реагує на загрозу у кризовому режимі, тоді як ЄС вибудовує довгострокову архітектуру стійкості.

У межах третього завдання, дослідження етапів, стратегічних цілей та тактик російської дезінформаційної кампанії, встановлено, що вона є системним і багатоетапним проєктом, інтегрованим у стратегію гібридної війни проти України.

Аналіз засвідчив, що російська дезінформаційна кампанія пройшла три основні етапи, демонструючи високу адаптивність. Вона еволюціонувала від прямого впливу через підконтрольні телеканали до масштабних мережевих компаній, які на початковому етапі відзначалися низькою якістю машинних перекладів, але згодом перейшли до глибокої інфільтрації в регіональні інформаційні середовища. Ключовими тактиками залишаються апеляція до емоцій, вбудовування фейкових тверджень у контекст правдивої інформації, імітація плюралізму та легітимізація пропагандистських наративів.

Дослідження показало, що стратегічною метою російських операцій є підрив суспільної довіри, деморалізація населення, фрагментація суспільних груп, делегітимація державних інституцій та створення хаосу у медіапросторі. Тактичний арсенал включає фабрикацію фактів, компрометаційні кампанії, підміну понять, симуляцію громадської думки, маніпуляцію емоціями та використання наперед спланованих інформаційних криз.

У рамках четвертого завдання, оцінки українських інституційних, механізмів та громадських ініціатив протидії дезінформації, встановлено, що

Україна створила розвинену систему інформаційної протидії, однак ця система потребує покращення координації та стратегічного узгодження.

У роботі проаналізовано діяльність державних органів, громадських організацій, фактчекінгових ініціатив, журналістських проєктів та аналітичних центрів. Перевагою українського підходу є оперативність реагування, сильний громадянський сектор, широке використання OSINT, швидкість адаптації до нових типів загроз і практичний досвід, здобутий у реальних умовах війни.

Водночас ключовою проблемою залишається фрагментованість системи, різні інституції часто працюють паралельно, без повноцінної інтеграції в єдину стратегічну модель, що знижує потенційну ефективність їх зусиль.

Виконання аналізу міжнародного досвіду та моделей протидії дезінформації дозволило сформувати узагальнену картину ефективних практик, характерних для країн Європейського Союзу.

Міжнародний аналіз підтвердив, що стійкість до дезінформації забезпечує не один інструмент, а сукупність взаємопов'язаних політик: розвиток медіаграмотності, формування критичного мислення з раннього віку, інтеграція стратегічних комунікацій у державне управління, наявність аналітичних структур для оцінки інформаційних загроз і створення правових рамок для прозорості цифрових платформ.

Європейський досвід демонструє, що інформаційна стійкість це не реакція на загрозу, а довготривалий системний процес, що поєднує освіту, політику, регулювання та комунікацію. Це стало концептуальною основою для формування пропозицій, представлених у роботі.

У межах шостого завдання, розробки практичних рекомендацій щодо вдосконалення національної системи протидії дезінформації, сформульовано комплексну модель інформаційної стійкості. Модель адаптована до українських умов воєнного часу та враховує унікальний досвід країни, що робить її потенційно корисною не лише на національному, але й на міжнародному рівні.

Наукова новизна роботи полягає в обґрунтуванні інтегрованої моделі протидії дезінформації, яка долає обмеження існуючих, переважно реактивних,

підходів. Модель адаптує найкращі міжнародні практики до унікальних умов України – держави, що перебуває в стані довготривалої, повномасштабної гібридної війни. Вона робить акцент на переході від реагування на окремі фейки до формування проактивної інформаційної стійкості на національному, регіональному та індивідуальному рівнях.

Таким чином, враховуючи динамічність інформаційного середовища, подальші наукові розвідки можуть бути зосереджені на таких перспективних напрямках:

- аналіз впливу дезінформації, створеної за допомогою штучного інтелекту (діпфейки, генеративні тексти), на українське суспільство та розробка відповідних механізмів протидії;
- дослідження довгострокових психологічних наслідків систематичного інформаційного тиску на громадян в умовах війни та розробка програм психологічної стійкості;
- порівняльний аналіз ефективності моделей інформаційної стійкості на рівні окремих регіональних громад України для виявлення найбільш дієвих локальних практик.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ ТА ЛІТЕРАТУРИ

1. Базові поняття стратегічних комунікацій: стандарти на основі документів НАТО (англійсько-український та українсько-англійський словник) / Л. Компанцева та ін. Київ: Нац. акад. СБУ, 2019. С. 64. Режим доступу: https://nasbu.edu.ua/uploads/p_157_73307337.pdf (дата звернення: 01.03.2025)
2. Білий список медіа. Інститут масової інформації (IMI). URL: <https://imi.org.ua/doslidzhennya-standartiv> (дата звернення: 01.11.2025)
3. Гула Р., Голота А. «Доктрина герасимова»: «керований хаос» у війсьній теорії епохи постмодерну. *Воєнно-історичний вісник*. 2021. № 1(39). С. 141-155.
4. Дитяча академія суспільного мовлення РМА Juniors. URL: <https://academy.suspilne.media/juniors> (дата звернення: 01.11.2025)
5. Інститут масової інформації (IMI). URL: <https://imi.org.ua/> (дата звернення: 01.11.2025)
6. Капелюшний В. Дезінформація. / Енциклопедія Сучасної України; НАН України, НТШ. К. : Інститут енциклопедичних досліджень НАН України, 2007. URL: <https://esu.com.ua/article-21273>
7. Мапа рекомендованих медіа. URL: <https://map.detector.media/> (дата звернення: 01.11.2025)
8. Моїсєєва В. Сутність поняття «дезінформація» та її вплив на суспільну думку. Актуальні питання інформаційної діяльності: теорії та інновації: матеріали X Міжнародної науково-практичної конференції (м. Одеса, 20 березня 2025 року) / за заг. ред. В. Г. Спрінсяна. Одеса, 2025. С. 321-327.
9. Національна рада України з питань телебачення і радіомовлення. URL: www.nrada.gov.ua (дата звернення: 01.11.2025)
10. Підхід НАТО у галузі боротьби з інформаційними загрозами. URL: https://www.nato.int/cps/en/natohq/topics_219728.htm?selectedLocale=uk (дата звернення: 01.03.2025)

11. Посібник з протидії дезінформації розроблено працівниками Центру протидії дезінформації робочого органу Ради національної безпеки і оборони України за підтримки Консультативної місії Європейського Союзу в Україні. URL:

<https://cpd.gov.ua/announcement/posibnyk-z-protydyiyi-dezinformacziyi/> (дата звернення: 01.03.2025)

12. Почепцов Г. Г. (Дез)інформація. К.: ПАЛИВОДА А. В., 2019. 248 с. URL: https://detector.media/php_uploads/files/books/disinformation_pochepcov_book_web.pdf.

13. Про інформацію: Закон України [зі змінами, внесеними згідно із Законами № 4240-IX від 12.02.2025]. URL: <https://zakon.rada.gov.ua/laws/show/2657-12> (дата звернення: 01.03.2025)

14. Про медіа: Закон України [зі змінами, внесеними згідно із Законами № 4510-IX від 19.06.2025]. URL: <https://zakon.rada.gov.ua/laws/show/2849-20#Text> (дата звернення: 01.03.2025)

15. Про національну безпеку України: Закон України [зі змінами, внесеними згідно із Законами № 4631-IX від 09.10.2025]. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text> (дата звернення: 28.10.2025)

16. Про основи національного спротиву: Закон України [зі змінами, внесеними згідно із Законами № 4331-IX від 26.03.2025]. URL: <https://zakon.rada.gov.ua/laws/show/1702-20#Text> (дата звернення: 01.03.2025)

17. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 року №47/2017. URL: <https://www.president.gov.ua/documents/472017-21374> (дата звернення: 01.03.2025)

18. Про рішення Ради національної безпеки і оборони України від 2 лютого 2021 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: Указ Президента України від 2 лютого

2021 року №43/2021. URL: <https://www.president.gov.ua/documents/432021-36441>
(дата звернення: 01.12.2025)

19. Про рішення Ради національної безпеки і оборони України від 11 березня 2021 року «Про створення Центру протидії дезінформації»: Указ Президента України від 19 березня 2021 року №106/2021. URL: <https://www.president.gov.ua/documents/1062021-37421> (дата звернення: 01.03.2025)

20. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28 грудня 2021 року № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text> (дата звернення: 01.03.2025)

21. Про суспільні медіа України: Закон України [зі змінами, внесеними згідно із Законами № 3136-IX від 30.05.2023]. URL: <https://zakon.rada.gov.ua/laws/show/1227-vii#Text> (дата звернення: 03.11.2025)

22. Суспільне Мовлення. URL: <https://corp.suspilne.media/pro-nas/885-pro-suspilne-misiya-istoriya-zvity/> (дата звернення: 09.11.2025)

23. Центр протидії дезінформації. URL: <https://cpd.gov.ua/> (дата звернення: 09.11.2025)

24. Центр стратегічних комунікацій та інформаційної безпеки. URL: <https://mcsc.gov.ua/projects/a-href=https-spravdi-gov-ua-tsentr-stratehichnykh-komunikatsiy-ta-informatsiynoi-bezpeky-a/> (дата звернення: 11.11.2025)

25. Шлапаченко В. М. Дезінформація як спосіб інформаційно-психологічного впливу. *Інформаційна безпека людини, суспільства, держави.* – 2013. № 2. С. 78-86.

26. 3rd EEAS Report on Foreign Information Manipulation and Interference Threats. Strategic Communications. 2025. URL: <https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf> (дата звернення: 26.11.2025)

27. Action Plan on Strategic Communication. European Commission and EEAS. 2015. URL: https://www.eeas.europa.eu/sites/default/files/action_plan_on_strategic_communication.docx_eeas_web.pdf (дата звернення: 01.03.2025)
28. Council conclusions on Foreign Information Manipulation and Interference (FIMI). Council of the EU. 2022. URL: <https://data.consilium.europa.eu/doc/document/ST-11429-2022-INIT/en/pdf> (дата звернення: 01.12.2025)
29. Database. EUvsDisinfo. URL: <https://euvsdisinfo.eu/disinformation-cases/> (дата звернення: 01.11.2025)
30. DeepState. URL: <https://deepstatemap.live/#6/49.4383200/32.0526800> (дата звернення: 11.11.2025)
31. Definition of disinformation. Cambridge Advanced Learner's Dictionary & Thesaurus. Cambridge University Press. URL: <https://dictionary.cambridge.org/dictionary/english/disinformation> (дата звернення: 01.03.2025)
32. Detector Media. URL: <https://go.detector.media/> (дата звернення: 07.11.2025)
33. Estonian Atlantic Treaty Association (EATA). URL: <https://www.eata.ee/en/> (дата звернення: 15.11.2025)
34. EU Code of Practice on Disinformation. European Commission. 2018. URL: <https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation> (дата звернення: 01.03.2025)
35. Floridi L. Brave.net.world: The internet as a disinformation superhighway? *Electronic Library*. 1996. № 14. Pp. 509–514.
36. Gratis platform skal styrke børn og unges digitale dannelse. EMU. URL: <https://emu.dk/grundskole/gratis-platform-skal-styrke-boern-og-unges-digitale-dannelse?b=> (дата звернення: 01.12.2025)
37. InformNapalm. URL: <https://informnapalm.org/ua/> (дата звернення: 11.11.2025)

38. Inside Estonia's Strategy Against Disinformation and Cyber Threats. The Baltic Centre for Media Excellence. 2025. URL: <https://bcme.eu/en/articles/inside-estonias-strategy-against-disinformation-and-cyber-threats/> (дата звернення: 01.12.2025)
39. Mahairas A., Dvilyanski M. Disinformation – Дезінформація (Dezinformatsiya). *The Cyber Defense Review*. Vol. 3, No. 3 (FALL 2018), С. 21-28.
40. Media Literacy Index 2023. Open Society Institute Sofia. 2023. URL: <https://osis.bg/wp-content/uploads/2023/06/MLI-report-in-English-22.06.pdf> (дата звернення: 01.12.2025)
41. Molfar Intelligence Firm. URL: <https://molfar.com/> (дата звернення: 11.11.2025)
42. Molfar Intelligence Institute. URL: <https://www.molfar.institute/> (дата звернення: 11.11.2025)
43. National core curriculum for ECEC in a nutshell. Finnish National Agency for Education. URL: <https://www.oph.fi/en/education-and-qualifications/national-core-curriculum-ecec-nutshell> (дата звернення: 01.12.2025)
44. Norway's Proactive Approach. Oscar Westlund. AFT. 2025. URL: https://www.aft.org/ae/fall2025/westlund?utm_ (дата звернення: 01.12.2025)
45. Norwegian Safer Internet Centre: NSIC. Medietilsynet. URL: <https://www.medietilsynet.no/english/norwegian-safer-internet-centre-nsic/> (дата звернення: 01.12.2025)
46. Propaganda Diary. VoxCheck. URL: <https://russiandisinfo.voxukraine.org/reports> (дата звернення: 11.11.2025)
47. Psychological Defence Agency. URL: <https://www.mpf.se/english/> (дата звернення: 01.12.2025)
48. Resolution on Russia's disinformation and historical falsification to justify its war of aggression against Ukraine 2024/2988(RSP), 23.01.2025. URL: https://www.europarl.europa.eu/doceo/document/TA-10-2025-0006_EN.html (дата звернення: 01.12.2025)

49. SPRAVDI. Центр стратегічних комунікацій. URL: <https://spravdi.gov.ua/> (дата звернення: 08.11.2025)
50. StopFake. URL: <https://www.stopfake.org/uk/golovna/> (дата звернення: 01.11.2025)
51. Strengthened Code of Practice on Disinformation. European Commission. 2022. URL: <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation> (дата звернення: 01.03.2025)
52. Texty.org.ua. URL: <https://texty.org.ua/> (дата звернення: 11.11.2025)
53. The Code of Conduct on Disinformation. European Commission. 2025. URL: <https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation> (дата звернення: 01.12.2025)
54. The Digital Services Act. European Commission. 2022. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en (дата звернення: 01.03.2025)
55. The European Digital Media Observatory (EDMO). URL: <https://edmo.eu/> (дата звернення: 28.11.2025)
56. The National Audiovisual Institute (KAVI). URL: <https://kavi.fi/en/about-kavi/> (дата звернення: 01.12.2025)
57. UkraineWorld. URL: <https://ukraineworld.org/ua> (дата звернення: 09.11.2025)
58. VoxCheck. URL: <https://voxukraine.org/category/voks-informue> (дата звернення: 10.11.2025)
59. Wardle, C., & Derakhshan, H. Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking. *Council of Europe*. 2017. 107 с.

ДОДАТКИ

Додаток А

Інтегрована модель протидії дезінформації України

Рівень моделі	Стратегічний напрям	Ключова мета	Основні інструменти та механізми	Залучені актори	Очікуваний результат
I. Інституційний	Інституціоналізація комплексної інформаційної стійкості	Перехід від реактивної до проактивної державної політики; формування загальнонаціональної системи «інформаційної оборони»	Створення та посилення спеціалізованих інституцій; постійні програми протидії інформаційним впливам; координація між державою, медіа, дослідниками та громадами	Державні органи, громадський сектор, медіаспільнота, дослідницькі центри, місцеві громади	Стійкість суспільства до психологічних операцій, зниження ефективності ворожих інформаційних атак, здатність до саморегуляції в кризових умовах
II. Освітній	Інтеграція медіаграмотності в освітню систему	Формування критичного мислення як базової компетентності з раннього віку до дорослого життя	Включення медіаграмотності в стандарти освіти; розвиток програм для дорослих; підготовка вчителів; створення дидактичних матеріалів щодо діпфейків, маніпуляцій, алгоритмів платформ	МОН, освітні заклади, тренери та вчителі, громадські та культурні центри, бібліотеки, служби зайнятості	Підвищення критичності сприйняття інформації населенням, зменшення вразливості до дезінформації у соціальних мережах
III. Локальний (громадський)	Формування локальної інформаційної стійкості громад	Посилення спроможності громад протидіяти локальним інформаційним атакам і панічним вкидам	Підтримка локальних медіа та журналістів; грантові програми; інтеграція місцевих редакцій у національні системи фактчекінгу; розвиток локальних комунікаційних центрів	Місцеві громади, редакції, журналісти, громадські ініціативи, донорські та державні фонди	Поява опорних центрів інформаційної стійкості на місцях; зменшення переходу населення до джерел сумнівного походження; запобігання деморалізації та руйнуванню довіри

Продовження додатка А

IV. Аналітичний	Посилення аналітичних можливостей та міжсекторальної співпраці	Створення єдиної національної системи аналізу, прогнозування та класифікації інформаційних впливів	Створення єдиного аналітичного простору; OSINT-інструменти; платформи збору й обробки даних; співпраця з університетами, фактчекерами; аналіз поведінкових моделей поширення контенту	Державні органи, фактчекінгові ініціативи, університети, OSINT-спільноти, цифрові платформи, міжнародні партнери	Перехід від реактивного реагування до проактивного прогнозування дезінформаційних кампаній; підвищення ефективності державних рішень
V. Цифровий	Запровадження посиленого регулювання цифрового простору	Створення правової рамки, здатної оперативно реагувати на інформаційні атаки, обмежувати діяльність ворожих ресурсів та запобігати появі дезінформації	Розвиток законодавства на основі Закону «Про медіа»; механізми маркування та обмеження російських пропагандистських платформ; юридична відповідальність організованих мереж, що систематично поширюють шкідливий контент; оперативні процедури реагування на інформаційні кампанії	Парламент, уряд, регуляторні органи у сфері медіа та цифрових послуг, правоохоронні органи, цифрові платформи, експертні спільноти	Підвищення інформаційної безпеки держави; зменшення впливу російських пропагандистських ресурсів; створення умов для швидкого реагування на загрози; запобігання поширенню дезінформації ще до її масової появи