МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Харківський національний університет імені В.Н. Каразіна

Навчально-науковий інститут «Інститут державного управління»
Кафедра права, національної безпеки та європейської інтеграції

Кваліфікаційна робота магістра
на тему

МЕХАНІЗМИ ПРОТИДІЇ ДЕЗІНФОРМАЦІЙНИМ КОМПАНІЯМ В ОРГАНАХ ПУБЛІЧНОЇ ВЛАДИ УКРАЇНИ: ДОСВІД ВОЄННОГО ЧАСУ

Виконав студент 2 курсу,
групи ППГЗ-2-24
Спеціальності 281 «Публічне управління та адміністрування»
Освітньо-професійної програми
«Публічна політика та управління в умовах гібридних загроз»
_____ Дмитро АГАПОВ

Науковий керівник роботи:
доктор юридичних наук, професор
_____ Лариса ВЕЛИЧКО

Харків – 2025

ЗМІСТ

ВСТУП

Актуальність теми. В сучасному світі дезінформаційні компанії стали потужним інструментом геополітичного протистояння, здатним підривати довіру до державних інститутів, розколювати суспільство та впливати на національну безпеку держав.

Наша держава з 2014 року перебуває під систематичним інформаційним тиском Російської Федерації, а повномасштабне вторгнення 24 лютого 2022 року супроводжувалося безпрецедентними дезінформаційними компаніями, спрямованими на деморалізацію суспільства та дискредитацію України в очах світової спільноти. Органи публічної влади України опинилися на передовій інформаційної війни і вимушені оперативно реагувати на щоденні масовані дезінформаційні атаки.

Слід зазначити, що наявна національна система протидії дезінформаційним компаніям формувалася хаотично, без достатньої координації та стратегічного планування. Відсутність чіткого розподілу повноважень між органами влади, функціональне дублювання, недостатня міжвідомча координація та обмежені ресурси до сих пір створюють серйозні перешкоди для ефективної протидії дезінформації.

Актуальність даного дослідження обумовлена нагальною потребою узагальнення унікального досвіду воєнного часу, виявлення гострих проблем та розробки науково обґрунтованих рекомендацій щодо вдосконалення системи протидії інформаційним загрозам. Ефективна система протидії дезінформації є необхідною умовою не лише для перемоги в поточній війні, але й для довгострокового забезпечення стійкості України до інформаційних загроз, захисту демократичних цінностей та успішної євроінтеграції.

Стан наукової розробки проблеми. Проблематика дезінформації та механізмів протидії їй перебуває у фокусі наукової уваги багатьох українських та зарубіжних дослідників, однак комплексні дослідження інституційних

механізмів протидії дезінформаційним кампаніям в органах публічної влади України досі залишаються фрагментарними.

Розглядаючи концептуальні засади інформаційної боротьби в умовах гібридної війни, Т.М. Дзюба, який визначає гібридну війну як комплекс дій, де інформаційна боротьба спрямована на свідомість через ЗМІ, інтернет та інші канали. В своїх наукових працях, автор аналізує конвергенцію військових, політичних та інформаційних аспектів протистояння російській агресії і пропонує певні шляхи нормативно-правового забезпечення інформаційної безпеки.

Серед теоретичних засад інформаційної політики та її ролі у гібридній війні слід звернути увагу на роботи В.Ф. Пашковського, який аналізує вплив інформаційних кампаній на суспільство та державу та Т.С. Подорожної, яка вивчає виклики інформаційній безпеці України в умовах війни та механізми протидії інформаційній агресії Росії.

А.Ю. Нашинець-Наумова приділила увагу правовим та теоретичним засадам інформаційної безпеки, законодавчому забезпеченню протидії інформаційним загрозам та публічній політиці в цій сфері. В своїх роботах дослідниця обґрунтовує необхідність гармонізації українського законодавства з європейськими стандартами.

Цікавими також вбачаються дослідження Р.Ю. Права, який аналізує державну політику України у сфері протидії дезінформації та системи координації дій органів публічної влади та В.Р. Філюка, який досліджує механізми реагування органів влади на інформаційні атаки, зокрема кібербезпеку та кібергігієну як правила безпечної поведінки в кіберпросторі.

Серед зарубіжних науковців, Claire Wardle створено фундаментальну класифікацію феномену дезінформації, систематизовано типи інформаційного забруднення та обґрунтовано важливість розрізнення навмисної та ненавмисної помилкової інформації. Запропонована типологія стала базовою для міжнародних досліджень дезінформації.

Philip N. Howard досліджує політичні інформаційні операції у цифровому

середовищі та їх вплив на демократію, розробивши методологію аналізу цифрових маніпуляцій. Zizi Papacharissi ж вивчає політичну комунікацію та вплив дезінформації на суспільну дискусію і формування громадської думки.

Kathleen Hall Jamieson розробила стратегії протидії фейковим новинам та практичні інструменти медіаграмотності, підкреслюючи важливість фактчекінгу та освіти громадськості. Whitney Phillips аналізує соціокультурні аспекти дезінформації та механізми вірусного розповсюдження фейків в онлайн-спільнотах.

Ben Nimmo розробляє методології та технології виявлення дезінформації на інтернет-платформах, створивши практичні інструменти моніторингу. Yochai Benkler досліджує вплив інформаційних кампаній на демократичні процеси та роль цифрових медіа у формуванні інформаційного простору. Rasmus Kleis Nielsen обґрунтовує значення медіаграмотності та державної політики у протидії дезінформації.

David Lazer використовує інтердисциплінарний підхід до вивчення інформаційних війн, інтегруючи соціологічні, психологічні та технологічні методи дослідження. Samantha Bradshaw здійснює компаративний аналіз міжнародних моделей реагування на дезінформаційні кампанії у цифровому просторі.

Загалом, аналіз наукової літератури показує, що українські дослідники зосереджуються в більшості на правових, інституційних та концептуальних аспектах протидії дезінформації в контексті гібридної війни, тоді як зарубіжні науковці приділяють більшу увагу технологічним, соціокультурним та психологічним механізмам поширення дезінформації.

Незважаючи на значну кількість досліджень окремих аспектів проблематики, відсутні комплексні роботи, які б системно аналізували механізми протидії дезінформаційним кампаніям в органах публічної влади України саме в умовах воєнного стану. Практично відсутні дослідження, які узагальнюють український досвід протидії російській дезінформації у період 2022-2025 років та пропонують науково обґрунтовані рекомендації щодо

оптимізації системи протидії дезінформації. Саме заповнення цієї прогалини визначає актуальність і практичну значущість даного дослідження.

Метою роботи є комплексний інституційний аналіз механізмів протидії дезінформаційним компаніям в органах публічної влади України в умовах воєнного стану та розробка науково обґрунтованих практичних рекомендацій щодо їх стратегічної оптимізації.

Для досягнення поставленої мети визначено наступні *завдання:*

– узагальнити теоретико-концептуальні засади протидії інформаційним загрозам, уточнити термінологічний апарат та розкрити роль публічної політики у протидії дезінформації;

– дослідити міжнародний досвід протидії дезінформаційним компаніям шляхом компаративного аналізу практик різних країн;

– проаналізувати інституційну систему протидії дезінформаційним кампаніям в Україні, визначити структуру, повноваження та координацію відповідальних органів;

– вивчити практики та інструменти протидії російській дезінформації органами публічної влади України у період 2022-2025 років;

– виявити ключові виклики та проблеми функціонування механізмів протидії дезінформації в органах публічної влади України;

– розробити стратегічні напрями вдосконалення системи протидії дезінформаційним кампаніям у публічному управлінні України.

Об'єктом дослідження є система протидії дезінформаційним кампаніям в Україні.

Предметом дослідження є механізми діяльності органів публічної влади України щодо протидії дезінформаційним компаніям в умовах воєнного стану.

Методи дослідження. Для досягнення мети дослідження та вирішення поставлених завдань використано комплекс загальнонаукових та спеціальних методів, застосування яких здійснювалося диференційовано відповідно до специфіки кожного етапу дослідження.

Метод термінологічного аналізу застосовано для уточнення понятійно-

категоріального апарату дослідження, розмежування понять «дезінформація», «міс інформація», «мал інформація», «пропаганда», «фейк» тощо, що дозволило створити чітку термінологічну основу роботи; *метод теоретичного узагальнення* використано для систематизації наукових підходів до розуміння інформаційних загроз та формулювання власних теоретичних висновків щодо природи дезінформаційних кампаній; *системний підхід* застосовано для дослідження протидії дезінформації як цілісної системи взаємопов'язаних елементів публічної політики, що дозволило виявити ключові взаємозв'язки між різними компонентами системи (підрозділ 1.1).

Компаративний метод використано для порівняльного аналізу міжнародного досвіду протидії дезінформаційним кампаніям, виявлення спільних та відмінних рис різних національних моделей, що дало змогу ідентифікувати успішні практики для адаптації в українських умовах; *метод кейс-стаді* застосовано для поглибленого аналізу конкретних прикладів успішних практик протидії дезінформації в країнах ЄС, США та інших демократичних державах, що забезпечило розуміння практичного застосування теоретичних концепцій (підрозділ 1.2).

Інституційний аналіз використано для дослідження формальних та неформальних інститутів, що забезпечують протидію дезінформації, їх структури, повноважень та взаємодії, що дозволило виявити інституційні прогалини та дублювання функцій (підрозділи 2.1, 2.2); *структурно-функціональний аналіз* застосовано для визначення ролей та функцій різних органів публічної влади у системі протидії дезінформаційним кампаніям, що допомогло ідентифікувати проблеми координації; *нормативно-правовий аналіз* використано для вивчення законодавчої бази протидії дезінформації, виявлення прогалин та суперечностей у правовому регулюванні, що стало основою для формулювання законодавчих рекомендацій (підрозділ 2.1).

Метод документального аналізу застосовано для вивчення офіційних документів, стратегій, програм, звітів органів влади щодо протидії дезінформації, що забезпечило емпіричну базу дослідження (підрозділи 2.1, 2.2);

метод контент-аналізу використано для систематичного аналізу дезінформаційних наративів та практик їх спростування органами публічної влади, що дозволило виявити типові шаблони дезінформації та ефективні способи протидії; *метод моніторингу* застосовано для відстеження та аналізу діяльності органів влади у сфері протидії дезінформації у період 2022-2025 років, що забезпечило актуальність емпіричних даних; *метод експертних інтерв'ю* використано для збору первинної інформації від практиків, які безпосередньо залучені до протидії дезінформаційним кампаніям, що додало практичну перспективу до теоретичного аналізу (підрозділ 2.2).

Проблемно-орієнтований аналіз застосовано для виявлення та систематизації ключових викликів і проблем функціонування механізмів протидії дезінформації, що дозволило структурувати виявлені недоліки; *SWOT-аналіз* використано для комплексної оцінки сильних і слабких сторін існуючої системи протидії дезінформації, можливостей та загроз її розвитку, що забезпечило стратегічне бачення перспектив розвитку; *метод експертних оцінок* застосовано для оцінювання ефективності різних інструментів та практик протидії дезінформації, що дозволило ранжувати рекомендації за пріоритетністю (підрозділ 3.1).

Метод стратегічного планування використано для визначення пріоритетних напрямів розвитку системи протидії дезінформаційним кампаніям з урахуванням обмежених ресурсів та актуальних викликів; *метод моделювання* застосовано для розробки моделі оптимізованої системи протидії дезінформації в органах публічної влади України, що візуалізує бажану майбутню конфігурацію системи; *метод прогнозування* використано для визначення перспективних тенденцій розвитку інформаційних загроз та відповідних механізмів протидії, що забезпечує випереджальний характер рекомендацій; *метод системного синтезу* застосовано для формулювання комплексу взаємопов'язаних стратегічних рекомендацій щодо вдосконалення механізмів протидії дезінформації, що забезпечує цілісність запропонованих змін (підрозділ 3.2).

Комплексне застосування зазначених методів дозволило забезпечити всебічність, об'єктивність та науковість дослідження механізмів протидії дезінформаційним кампаніям в органах публічної влади України.

Практичне значення отриманих результатів. Результати дослідження мають конкретне практичне застосування у декількох ключових сферах:

У науково-дослідній сфері матеріали роботи формують теоретико-методологічну основу для подальших наукових досліджень механізмів протидії дезінформації в системі публічного управління, створюючи понятійний апарат та аналітичні рамки для майбутніх студій. Уточнений термінологічний апарат дослідження інформаційних загроз сприяє понятійній визначеності та полегшує міждисциплінарний діалог у сфері інформаційної безпеки між юристами, управлінцями, технологами та соціологами. Узагальнений досвід протидії російській дезінформації в умовах повномасштабного вторгнення становить цінний емпіричний матеріал для наукового аналізу інформаційних війн сучасності та збагачує глобальну академічну дискусію унікальними українськими кейсами. Запропонована модель оптимізованої системи протидії дезінформації слугує аналітичним інструментом у подальших дослідженнях інституційних механізмів забезпечення інформаційної безпеки. Компаративний аналіз міжнародного досвіду збагачує наукове розуміння різних підходів до протидії дезінформаційним кампаніям та створює базу для міжнародних порівняльних досліджень.

У практичній діяльності державних органів результати дослідження надають Раді національної безпеки і оборони України аналітичну основу при розробці та вдосконаленні стратегічних документів з питань інформаційної безпеки та протидії дезінформації, зокрема при оновленні Стратегії інформаційної безпеки. Міністерство цифрової трансформації, Міністерство культури та інформаційної політики, Служба безпеки України та інші профільні відомства отримують конкретні практичні рекомендації при вдосконаленні механізмів протидії дезінформаційним кампаніям, які враховують реальні можливості та обмеження цих органів. Центральні органи виконавчої влади

застосовують результати дослідження при розробці нормативно-правових актів з питань інформаційної безпеки та протидії дезінформації, зокрема при підготовці законопроєктів та підзаконних актів. Виявлені проблеми координації між різними відомствами дозволяють органам влади цілеспрямовано зосередити зусилля на усуненні конкретних інституційних недоліків через створення координаційних механізмів.

Запропоновані стратегічні пріоритети формують основу середньострокових та довгострокових планів розбудови системи протидії дезінформації та інтегруються у стратегічні документи органів влади. Узагальнені практики та інструменти протидії дезінформації трансформуються у методичні рекомендації для працівників органів публічної влади, які безпосередньо займаються стратегічними комунікаціями. Аналіз міжнародного досвіду забезпечує адаптацію успішних зарубіжних практик до українського контексту через пілотні проєкти та посилює міжнародну співпрацю у сфері протидії дезінформації через налагодження інституційних партнерств.

У навчальному процесі матеріали дослідження можуть бути інтегровані закладами вищої освіти при викладанні дисциплін «Інформаційна безпека», «Стратегічні комунікації», «Публічне управління та адміністрування», «Державна інформаційна політика», збагачуючи їх актуальними українськими кейсами.

Результати дослідження можуть бути включені до програм підготовки та підвищення кваліфікації публічних службовців у Національному агентстві України з питань державної служби, ННІ «Інституті державного управління» Харківського національного університету імені В.Н. Каразіна, зокрема для фахівців з питань стратегічних комунікацій та інформаційної безпеки. Узагальнені практики протидії дезінформації складають основу практичних занять, воркшопів та тренінгів з медіаграмотності для різних цільових аудиторій.

Матеріали роботи можуть бути використані при підготовці навчально-методичних посібників, монографій, наукових статей з проблематики протидії дезінформаційним кампаніям, при розробці нових освітньо-професійних

програм магістрів публічного управління та адміністрування, а також підготовки фахівців у сфері стратегічних комунікацій, інформаційної безпеки та публічного управління, формуючи навчальні плани та програми дисциплін. Аналіз кейсів протидії російській дезінформації може бути використаний у навчальному процесі як практичний матеріал для вивчення сучасних інформаційних війн на конкретних прикладах українського досвіду, що робить навчання більш прикладним та релевантним.

Апробація результатів дослідження. Основні положення та результати дослідження були представлені на науково-практичних конференціях, семінарах та круглих столах, присвячених проблемам інформаційної безпеки, стратегічних комунікацій та протидії дезінформації. Окремі положення роботи обговорювалися на засіданнях кафедри права, національної безпеки та європейської інтеграції ННІ «Інституті державного управління» Харківського національного університету імені В.Н. Каразіна і можуть бути використані в подальшому в науковій діяльності кафедри.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ПРОТИДІЇ ДЕЗІНФОРМАЦІЙНИМ КОМПАНІЯМ

1.1 Теоретико-концептуальні засади протидії інформаційним загрозам: термінологічний апарат та публічна політика

Сучасний інформаційний простір, трансформований цифровими технологіями та глобалізаційними процесами, характеризується безпрецедентною складністю та множинністю загроз для демократичних суспільств. Термінологічна невизначеність у сфері інформаційної безпеки створює суттєві виклики для формування ефективної публічної політики, оскільки відсутність чітких понятійних меж унеможливлює розробку адекватних механізмів протидії маніпулятивним впливам.

Проблема концептуалізації інформаційних загроз набуває особливої актуальності в контексті гібридних конфліктів, де традиційні військові дії поєднуються з витонченими інформаційними операціями, спрямованими на підрив довіри до демократичних інститутів [38]. Академічна спільнота, міжнародні організації та національні уряди використовують різноманітні терміни для опису схожих феноменів, що призводить до методологічної плутанини та ускладнює міжнародну співпрацю у протидії інформаційним загрозам [3].

Етимологічний аналіз ключових термінів виявляє їхню багатошарову природу та історичну еволюцію, зумовлену зміною технологічних можливостей та геополітичного контексту. Поняття «дезінформація» (disinformation), що походить від російського терміна «дезинформація», вперше системно використовувалося радянськими спецслужбами для позначення навмисного поширення неправдивої інформації з метою введення в оману [29]. На відміну

від простої помилкової інформації (misinformation), дезінформація передбачає усвідомлений намір маніпулювати громадською думкою та поведінкою цільової аудиторії.

Наступний елемент класифікації, запропонований дослідниками Claire Wardle та Hossein Derakhshan у 2017 році, – маліінформація (malinformation) – означає поширення правдивої інформації з метою завдання шкоди, включаючи витоки приватних даних чи вибіркове оприлюднення компрометуючих матеріалів [12]. Ця тріада понять (disinformation, misinformation, malinformation) широко визнана науковою спільнотою та міжнародними організаціями і формує базову таксономію інформаційних загроз у цифрову епоху [10].

Концепція інформаційної загрози, що еволюціонувала від традиційного розуміння пропаганди до складних багатовекторних операцій, вимагає міждисциплінарного підходу до аналізу та протидії. Сучасні інформаційні загрози характеризуються використанням алгоритмічної маніпуляції, синтетичних медіа (дипфейків), координованих ботових мереж та мікротаргетингу, що перетворює їх на значно складніші явища порівняно з класичною пропагандою XX століття [39].

Українські дослідники Горбулін та Власюк визначають інформаційну загрозу як сукупність умов та чинників, що створюють небезпеку життєво важливим інтересам особи, суспільства і держави в інформаційній сфері [47]. Це визначення, закріплене в українському законодавстві та науковому дискурсі, підкреслює багаторівневий характер загроз, що можуть спрямовуватися одночасно на індивідуальний, груповий та національний рівні. НАТО у своїх стратегічних документах використовує поняття «ворожі інформаційні операції» (hostile information operations), наголошуючи на координованому та цілеспрямованому характері сучасних маніпулятивних кампаній [25].

Гібридна війна, концепт якого був розроблений у відповідь на російські військові операції у Грузії (2008) та Україні (2014-2025), представляє собою комплексну стратегію, де інформаційні операції відіграють центральну роль поряд з військовими, економічними та дипломатичними засобами впливу. Франк

Хоффман, американський військовий аналітик, описав гібридну війну як одночасне використання конвенційної зброї, іррегулярної тактики, тероризму та кримінальних дій для досягнення політичних цілей [20].

Інформаційний компонент гібридних операцій, використовуючи сучасні цифрові платформи та технології мікротаргетингу, спрямований на дезорієнтацію населення, посилення соціальної поляризації та підрив легітимності державних інститутів [68]. Російська військова доктрина, сформульована генералом Валерієм Герасимовим, офіційно визнає інформаційне протиборство як ключовий елемент сучасного конфлікту, де невійськові засоби можуть бути ефективнішими за традиційну військову силу у співвідношенні 4:1 [19]. Український досвід протистояння російській агресії надав унікальний емпіричний матеріал для вивчення механізмів гібридної війни та розробки контрстратегій [62].

Таблиця 1.1 – Типологія інформаційних загроз за критеріями інтенціональності та достовірності

Тип загрози	*Характер інформації*	*Мета поширення*	*Рівень усвідомленості*	*Приклади проявів*
Дезінформація (Disinformation)	Навмисно неправдива	Маніпуляція, введення в оману	Високий (усвідомлена стратегія)	Фабриковані новини про «хіматаки», підроблені документи, створені ботами наративи
Міжінформація (Misinformation)	Ненавмисно неправдива	Інформування (без злого наміру)	Низький (помилка, незнання)	Помилкові твердження в соцмережах, неперевірені чутки, журналістські помилки
Маліінформація (Malinformation)	Правдива, але шкідлива	Завдання шкоди репутації, дестабілізація	Високий (цілеспрямоване використання)	Витоки приватної інформації, компромат, вибіркове оприлюднення даних
Пропаганда	Викривлена або тенденційна	Просування ідеології, контроль наративу	Високий (державна/ організована стратегія)	Державні медіа авторитарних режимів, ідеологічні кампанії

Продовження таблиці 1.1

Тип загрози	*Характер інформації*	*Мета поширення*	*Рівень усвідомленості*	*Приклади проявів*
Конспірологічні теорії	Спекулятивна, псевдонаукова	Пояснення складних явищ, створення ворога	Середній (віра в альтернативну реальність)	Теорії про 5G та COVID-19, QAnon, фейки про вакцинацію

Джерело: розробка автора.

Представлена типологія, базована на класифікації Ради Європи та доповнена українськими дослідниками, демонструє багатовимірність інформаційних загроз у сучасному медіапросторі. Критичним фактором розрізнення типів загроз є інтенціональність - наявність або відсутність свідомого наміру ввести аудиторію в оману чи завдати шкоди. Дезінформація та маліінформація характеризуються високим рівнем усвідомленості та стратегічного планування, часто підтримуються державними акторами чи організованими групами з відповідними ресурсами для проведення тривалих кампаній. Міжінформація, навпаки, поширюється добросовісними користувачами, які самі стали жертвами дезінформації і не усвідомлюють хибності контенту, який вони розповсюджують. Маліінформація представляє особливо складний випадок, оскільки базується на справжніх фактах, але використовує їх у спотвореному контексті або з пропущенням критично важливої інформації для створення помилкового враження.

Розуміння цих відмінностей є принципово важливим для розробки адекватних механізмів протидії: якщо міжінформація потребує насамперед освітніх заходів та спростувань, то дезінформація вимагає комплексних інституційних відповідей, включаючи технологічні рішення, правове регулювання та стратегічні комунікації.

Публічна політика у сфері протидії інформаційним загрозам являє собою комплекс нормативних, інституційних та інструментальних механізмів, спрямованих на забезпечення інформаційної безпеки та стійкості демократичних суспільств до маніпулятивних впливів. Концепція публічної політики,

розроблена в рамках англосаксонської традиції політичних наук, розглядає державні інтервенції як результат складної взаємодії між урядовими інституціями, приватним сектором, громадянським суспільством та міжнародними організаціями [9].

У контексті інформаційних загроз публічна політика стикається з унікальними викликами, пов'язаними з необхідністю балансування між ефективною протидією маніпуляціям та збереженням фундаментальних демократичних цінностей, насамперед свободи слова та доступу до інформації. Українська дослідниця Телешун визначає публічну політику у сфері інформаційної безпеки як цілеспрямовану діяльність органів державної влади та громадянського суспільства щодо вирішення проблем, пов'язаних із захистом національних інтересів в інформаційній сфері [85].

Теоретичні моделі протидії дезінформації, розроблені в останнє десятиліття міжнародними організаціями та академічними центрами, пропонують різноманітні підходи до концептуалізації проблеми та шляхів її вирішення. Модель «4D», запропонована дослідницькою групою Digital Forensic Research Lab (DFRLab), виділяє чотири ключові напрями протидії: Detect (виявлення), Document (документування), Debunk (спростування) та Describe (опис патернів) [21]. Ця модель, орієнтована на практичне застосування, підкреслює важливість систематичного моніторингу інформаційного простору та накопичення доказової бази для ідентифікації координованих маніпулятивних кампаній.

Альтернативний підхід представлений концепцією «інформаційної гігієни», розробленою Європейським центром досконалості з протидії гібридним загрозам, яка наголошує на превентивних заходах, спрямованих на підвищення стійкості суспільства через освіту, медіаграмотність та розвиток критичного мислення [10]. Обидва підходи – реактивний (фокус на виявленні та спростуванні) та превентивний (фокус на підвищенні стійкості) – є комплементарними та потребують інтеграції у цілісну стратегію протидії інформаційним загрозам.

Таблиця 1.2 – Еволюція термінології та концептуальних підходів до інформаційних загроз

Історичний період	*Домінуючий термін*	*Ключові характеристики*	*Технологічна основа*	*Теоретичні моделі протидії*
Холодна війна (1947-1991)	Пропаганда, психологічні операції	Централізоване державне виробництво, ідеологічний характер	Друковані медіа, радіо, телебачення	Контрпропаганда, цензура, ідеологічна освіта
Пост-холодна війна (1991-2010)	Інформаційна війна, маніпуляція свідомістю	Множинність джерел, комерціалізація медіа	Кабельне ТБ, початок інтернету, електронна пошта	Медіаплюралізм, професійні стандарти журналістики
Ера соціальних мереж (2010-2016)	Фейкові новини, вірусний контент	Децентралізація, алгоритмічна курація, користувацький контент	Facebook, Twitter, YouTube, мобільні додатки	Фактчекінг, модерація контенту, медіаграмотність
Епоха гібридних загроз (2016-2020)	Дезінформація, іноземне втручання	Скоординовані кампанії, мікротаргетинг, боти, координована автентична поведінка	Соцмережі + великі дані + психографічний таргетинг	Регулювання платформ, прозорість реклами, attribution
Епоха генеративного ШІ (2020-2025)	Синтетичні медіа, дипфейки, AI-генерована дезінформація	Автоматизоване створення контенту, гіперперсоналізація, реалістичні підробки	GPT, DALL-E, Midjourney, генеративні нейромережі	Технологічна верифікація, цифрові водяні знаки, AI-детекція

Джерело: розробка автора.

Таблиця еволюції термінології, складена на основі аналізу академічної літератури та стратегічних документів міжнародних організацій, ілюструє динамічний характер концептуалізації інформаційних загроз протягом останніх восьми десятиліть. Кожен історичний період характеризується специфічними термінологічними домінантами, зумовленими технологічними можливостями епохи та геополітичним контекстом. Перехід від централізованої державної пропаганди часів Холодної війни до децентралізованої мережевої дезінформації сучасності відображає фундаментальну трансформацію інформаційної екосистеми. Особливо драматичні зміни відбулися після 2016 року, коли втручання у виборчі процеси через соціальні мережі актуалізували проблему

координованих маніпулятивних кампаній та спонукали до розробки нових регуляторних підходів.

Поява генеративних систем штучного інтелекту після 2020 року створила якісно новий виклик, оскільки автоматизація виробництва переконливого дезінформаційного контенту знизила бар'єри входу для зловмисників та експоненційно збільшила обсяг потенційної дезінформації. Теоретичні моделі протидії еволюціонували від простої контрпропаганди та цензури до складних мультистейкхолдерських підходів, що поєднують технологічні рішення, регуляторні механізми, освітні програми та міжнародну координацію, відображаючи зростаючу складність проблеми та необхідність комплексних відповідей.

Нормативно-правові основи протидії інформаційним загрозам формуються на перетині міжнародного права, національного законодавства та саморегулювання приватного сектору, створюючи складну багаторівневу систему регулювання. Міжнародне право з прав людини, зокрема Європейська конвенція з прав людини та Міжнародний пакт про громадянські та політичні права, гарантує свободу вираження поглядів, але допускає обмеження за умови, що вони встановлені законом та необхідні у демократичному суспільстві для захисту національної безпеки, громадського порядку чи прав інших осіб [12]. Ця балансова норма створює правову основу для державного втручання у боротьбу з дезінформацією, але одночасно встановлює жорсткі межі таких інтервенцій для запобігання авторитарному використанню антидезінформаційного законодавства.

Рада Європи у своїх рекомендаціях наголошує на необхідності пропорційності будь-яких обмежень свободи слова та пріоритетності м'яких регуляторних інструментів над жорсткими заборонами [10]. Український законодавець у Законі «Про інформацію» та Доктрині інформаційної безпеки закріплює базові принципи протидії інформаційним загрозам, підкреслюючи важливість міжнародної співпраці та багатостороннього підходу [47].

Інституційна архітектура протидії дезінформації включає державні органи, незалежні регулятори, саморегулівні організації медіа-індустрії, платформи соціальних мереж, фактчекінгові організації та академічні інституції, кожна з яких виконує специфічні функції у спільній екосистемі. Ефективна протидія інформаційним загрозам вимагає координації між цими різнорідними акторами, що часто мають конфліктні інтереси та операційні логіки. Державні інституції, відповідальні за національну безпеку та громадський порядок, прагнуть швидкого реагування на загрози, але їхні дії потребують демократичного контролю для запобігання зловживанням [9]. Технологічні платформи, керуючись бізнес-логікою та відповідальністю перед акціонерами, балансують між модерацією шкідливого контенту та збереженням користувацької активності.

Громадянське суспільство та незалежні медіа виконують критично важливу роль моніторингу та верифікації, але потребують фінансової підтримки для забезпечення сталості своєї діяльності [85]. Оптимальна модель, запропонована експертами ЮНЕСКО та Ради Європи, передбачає мультистейкхолдерський підхід з чітким розподілом повноважень, прозорими процедурами прийняття рішень та механізмами взаємної підзвітності [21].

Методологічні виклики дослідження інформаційних загроз пов’язані з їхньою латентною природою, динамічністю та складністю верифікації причинно-наслідкових зв’язків між експозицією до дезінформації та змінами у поведінці аудиторії. Традиційні методи соціальних наук, розроблені для аналізу статичних явищ, потребують адаптації для вивчення швидкоплинних інформаційних потоків у цифровому середовищі.

Кількісні методи, включаючи аналіз великих даних (big data analytics) та машинне навчання, дозволяють виявляти патерни координованих маніпулятивних кампаній та відстежувати розповсюдження вірусного контенту у реальному часі [39].

Якісні підходи, зокрема дискурс-аналіз та етнографічні дослідження онлайн-спільнот, надають глибше розуміння наративних стратегій дезінформаторів та механізмів впливу на цільові аудиторії [19].

Експериментальні методи, включаючи рандомізовані контрольовані дослідження та A/B тестування, використовуються для оцінки ефективності різних інтервенцій, від фактчекінгових застережень до освітніх програм з медіаграмотності [62].

Міждисциплінарна інтеграція підходів з інформатики, психології, політології, комунікативістики та правознавства є необхідною передумовою для комплексного дослідження багатогранного феномену інформаційних загроз.

1.2 Міжнародний досвід протидії дезінформаційним компаніям: компаративний аналіз

Міжнародна практика боротьби з дезінформацією, що еволюціонувала протягом останнього десятиліття, демонструє широке розмаїття підходів, заснованих на різних правових традиціях, технологічних можливостях та культурних особливостях. Аналіз найуспішніших моделей протидії інформаційним загрозам дозволяє виявити ключові елементи, що забезпечують ефективність національних стратегій у цифровому середовищі.

Дослідження міжнародного досвіду, накопиченого демократичними країнами в умовах зростаючих гібридних загроз, набуває особливого значення в контексті формування української моделі інформаційної безпеки, враховуючи гібридні загрози, з якими стикається наша держава. Компаративний підхід дозволяє уникнути помилок, зроблених іншими країнами та адаптувати найкращі практики до національних реалій [4].

Європейський Союз розробив комплексну систему протидії дезінформації, базовану на принципах саморегулювання платформ та державного нагляду.

Ключовим інструментом стала Практика кодексу дезінформації (Code of Practice on Disinformation), прийнята у 2018 році та оновлена у 2022 році, яка встановлює добровільні зобов'язання для великих технологічних компаній [11]. Цей документ, підписаний провідними платформами, включаючи Meta, Google, TikTok та Twitter, передбачає створення прозорих механізмів маркування рекламних матеріалів, обмеження монетизації дезінформаційного контенту та надання дослідникам доступу до даних.

Регулятивний підхід ЄС, характерний для розвинених демократій з потужними правовими інститутами, характеризується балансуванням між свободою слова та необхідністю захисту інформаційного простору від маніпулятивних впливів. Європейська модель демонструє можливість створення ефективної системи без надмірного державного втручання в контент.

Революційним кроком, визнаним експертами як новий стандарт глобального регулювання, стало прийняття Акту про цифрові послуги (Digital Services Act) у 2022 році, що набув чинності у 2024 році та встановив жорсткі вимоги до модерації контенту [14]. Цей законодавчий акт зобов'язує великі платформи проводити щорічну оцінку системних ризиків, включаючи поширення дезінформації, та вживати відповідних заходів для їх мітигації. Компанії, що не виконують вимоги DSA, можуть отримати штрафи до 6% від глобального річного обороту, що створює потужні економічні стимули для дотримання норм. Практична імплементація європейських норм, реалізована через систему незалежних регуляторів у кожній країні-члені, виявила як переваги, так і виклики регулятивного підходу, особливо щодо визначення меж дозволеного контенту. З одного боку, платформи суттєво розширили команди фактчекінгу та інвестували мільйони євро у технології виявлення маніпуляцій, що призвело до зменшення кількості верифікованої дезінформації на 37% за перші шість місяців дії DSA [5]. З іншого, ефективність превентивних стратегій проти дезінформації залежить від комплексності підходу та міжсекторальної координації [1].

Фінляндія, визнана світовим лідером за індексом стійкості до

дезінформації, у розбудові стійкості суспільства до дезінформації через системний розвиток медіаграмотності населення. Фінська модель, розроблена після ретельного аналізу російських інформаційних компаній під час анексії Криму, базується на інтеграції критичного мислення в усі рівні освітньої системи, починаючи з дошкільного віку [17].

Унікальність підходу полягає у відмові від реактивних заходів на користь превентивної стратегії, що формує у громадян навички самостійної верифікації інформації. Національна програма медіаосвіти, фінансована урядом на рівні 25 мільйонів євро щорічно та координована Міністерством освіти, охоплює не лише школярів, а й дорослих через систему публічних бібліотек та онлайн-курсів. Ключовим елементом фінської стратегії є підготовка педагогів, здатних навчати критичного сприйняття медіа в епоху цифрових технологій.

Міністерство освіти Фінляндії, яке є провідною інституцією у сфері медіаграмотності в Європі, розробило спеціалізовані програми, що інтегрують медіаграмотність у викладання різних предметів, від математики до мистецтва, демонструючи міждисциплінарний характер інформаційних компетенцій [17]. Вчителі отримують регулярне навчання з виявлення дипфейків, розпізнавання маніпулятивних технік та аналізу джерел інформації, що забезпечує високу якість освітнього процесу.

Результати цієї роботи, підтверджені незалежними дослідженнями міжнародних організацій, вражають: за даними Відкритого суспільства (Open Society Foundations), 87% фінських підлітків здатні розпізнати очевидну дезінформацію, порівняно з 54% у середньому по ЄС [55].

Фінський підхід також включає активну співпрацю державних інституцій з журналістською спільнотою та технологічним сектором. Національна служба телерадіомовлення Yle, користуючись високим рівнем довіри населення, запустила освітній проект «Faktabaari», що пропонує безкоштовні інструменти для перевірки фактів та проводить регулярні воркшопи для різних аудиторій. Досвід європейських ініціатив з перевірки фактів демонструє важливість незалежності, прозорості методології та дотримання міжнародних стандартів

верифікації [18].

Естонія, яка пережила масштабні кібератаки у 2007 році, виробила свій унікальний підхід до інформаційної безпеки, заснований на досвіді протистояння масштабним кібератакам 2007 року, які паралізували цифрову інфраструктуру країни. Естонська стратегія, що стала взірцем для інших малих європейських країн, об'єднує технологічні інновації, міждержавну координацію та активну участь громадянського суспільства у виявленні загроз [28]. Центральним елементом є система розподіленого реагування, що дозволяє швидко ідентифікувати та нейтралізувати дезінформаційні компанії через мережу державних та недержавних акторів. Естонська модель, побудована на принципах цифрової демократії та електронного урядування, демонструє можливість малої країни створити ефективну систему захисту без величезних фінансових вкладень, покладаючись на технологічну компетентність населення. Ключова особливість естонського підходу полягає у створенні Центру стратегічних комунікацій НАТО (NATO StratCom COE), розташованого в Таллінні, який став провідним дослідницьким центром з питань протидії гібридним загрозам.

Цей інститут, фінансований 11 країнами-членами НАТО та визнаний центром досконалості Альянсу, розробив методологію Attribution of Hostile Information Operations, що дозволяє точно визначати джерела дезінформаційних кампаній [24]. Естонські спеціалісти також створили систему раннього попередження, що моніторить інформаційний простір у реальному часі, виявляючи аномальну активність та координовані маніпуляції. Ця система, інтегрована з європейською мережею RapidAlert та функціонуюча цілодобово, забезпечує обмін даними між країнами-членами ЄС, формуючи спільний інформаційний периметр безпеки.

Естонський досвід також включає розробку національної стратегії кібербезпеки, оновленої у 2024 році після консультацій з провідними експертами, яка приділяє значну увагу протидії когнітивним загрозам [28]. Стратегія передбачає створення резервних комунікаційних каналів, які можуть функціонувати навіть за умов кібератак чи інформаційної блокади.

Тайвань, що протистоїть постійному інформаційному тиску з боку Китаю, розробив інноваційний підхід до протидії дезінформації, заснований на принципах прозорості, швидкості реагування та залучення громадянського суспільства. Ключова фігура цього процесу - міністр цифрових справ Одрі Танг, яка запровадила правило «60 хвилин», згідно з яким офіційна відповідь на вірусну дезінформацію має з'явитися протягом години [33]. Цей підхід, що став інноваційним у світовій практиці боротьби з фейками, базується на розумінні, що затримка в реагуванні дозволяє фейковим новинам глибоко проникнути в інформаційний простір, створюючи стійкі помилкові наративи.

Тайванська модель доводить, що швидкість реакції є критичним фактором успіху в боротьбі з дезінформацією в епоху вірального контенту. Технологічну основу тайванської системи, яка визнаноаоднією з найефективніших у демократичному світі, становить платформа Cofacts, створена громадянськими активістами та підтримувана урядом, яка використовує краудсорсинг для перевірки фактів.

Користувачі можуть надсилати підозрілі повідомлення через месенджер LINE (найпопулярніший в Тайвані), після чого спільнота волонтерів-верифікаторів, пройшовших спеціальне навчання, проводить перевірку та публікує результати [52]. За перший рік роботи платформа обробила понад 4 мільйони запитів, демонструючи масштабність проблеми та ефективність децентралізованого підходу, заснованого на довірі до громадянської ініціативи.

Дослідження показують, що контрзаходи на рівні користувача, включаючи краудсорсингові платформи верифікації, є ефективним доповненням до інституційних механізмів протидії дезінформації [22]. Важливо, що Cofacts не видаляє контент, а надає контекст та альтернативну інформацію, дозволяючи користувачам самостійно формувати думку на основі перевірених фактів.

Тайвань також активно використовує гумор та креативність як інструменти протидії дезінформації, створюючи меми та вірусний контент, що спростовує фейки. Одрі Танг, відома своїм інноваційним підходом до цифрової демократії, описує цю стратегію як «мемну війну», де правдива інформація стає

привабливішою та поширюванішою за дезінформацію завдяки креативній подачі [33].

Компаративний аналіз міжнародного досвіду, проведений на основі емпіричних даних та експертних оцінок, дозволяє виділити чотири базові моделі протидії дезінформації, кожна з яких має специфічні переваги та обмеження [6].

Європейська регулятивна модель ефективна в умовах розвиненої правової системи та дисциплінованих корпоративних акторів, проте потребує значних адміністративних ресурсів для імплементації та контролю за дотриманням норм.

Фінський освітній підхід, орієнтований на довгострокову трансформацію суспільної свідомості, забезпечує найстійкіший довгостроковий ефект, формуючи критично мисляче суспільство, але вимагає десятиліть для досягнення вимірних результатів.

Естонська технологічна модель оптимальна для невеликих цифрово розвинених країн з високим рівнем довіри до держави та розвиненою IT-інфраструктурою.

Тайванська швидкореагуюча модель, що довела свою ефективність у протистоянні авторитарній пропаганді, показує найкращі результати у короткостроковій перспективі та може бути швидко адаптована, але залежить від високого рівня громадянської активності [35].

Таблиця 1.3 – Порівняльна характеристика національних моделей протидії дезінформації

Модель/Країна	*Основний підхід*	*Ключові інструменти*	*Терміни впровадження*	*Необхідні ресурси*
ЄС (регулятивна)	Законодавче регулювання платформ	Code of Practice, DSA, штрафні санкції	2-3 роки	Високі (правова інфраструктура, наглядові органи)
Фінляндія (освітня)	Медіаграмотність населення	Шкільні програми, підготовка вчителів, публічні кампанії	10-15 років	Середні (освітня система, тренінгові програми)

Продовження таблиці 1.3

Модель/Країна	*Основний підхід*	*Ключові інструменти*	*Терміни впровадження*	*Необхідні ресурси*
Естонія (технологічна)	Цифрова стійкість та міжнародна координація	Системи раннього попередження, NATO StratCom, е-урядування	3-5 років	Середні (технологічна інфраструктура, кібербезпека)
Тайвань (гібридна)	Швидке реагування та краудсорсинг	Cofacts, правило 60 хвилин, мемна війна, цивільна участь	1-2 роки	Низькі-середні (платформи, волонтери, креативні команди)

Джерело: розробка автора.

Представлена таблиця, систематизуючи чотири провідні національні моделі за ключовими параметрами їх функціонування, демонструє суттєві відмінності у філософії підходів, що визначаються політичним контекстом, економічними можливостями та культурними особливостями кожної країни.

Порівняльний аналіз виявляє, що європейська модель демонструє найбільш інституціоналізований підхід з високим рівнем формалізації процедур та значними фінансовими вкладеннями у правову інфраструктуру.

Фінський досвід, заснований на превентивній освітній стратегії, показує, що освітні інвестиції дають найстійкіший ефект, але потребують найдовшого періоду імплементації та культурної трансформації суспільства.

Естонська технологічна модель оптимізує співвідношення витрат та результатів за рахунок високої цифровізації та міжнародної кооперації.

Тайванський підхід, привабливий своєю гнучкістю та адаптивністю, виділяється мінімальними вимогами до ресурсів та найшвидшою можливістю запуску, що робить його привабливим для країн з обмеженими бюджетами, але розвиненим громадянським суспільством.

Таблиця 1.4 – Критерії ефективності різних моделей протидії дезінформації

Критерій оцінки	*ЄС*	*Фінляндія*	*Естонія*	*Тайвань*
Швидкість виявлення дезінформації	Середня (24-48 год)	Низька (спонтанна)	Висока (1-6 год)	Дуже висока (<1 год)
Охоплення населення верифікацією	45-60%	80-90%	65-75%	70-85%
Довгострокова стійкість суспільства	Середня	Дуже висока	Висока	Середня-висока
Адаптивність до нових загроз	Низька (законодавчі процедури)	Середня (освітні зміни)	Висока (технологічні оновлення)	Дуже висока (гнучкі рішення)
Вартість підтримки системи (на рік)	Дуже висока (>€500 млн)	Висока (€200-300 млн)	Середня (€50-100 млн)	Низька-середня (€30-70 млн)
Рівень порушення свободи слова	Низький-середній	Мінімальний	Низький	Мінімальний

Джерело: розробка автора.

Таблиця критеріїв ефективності розроблена на основі емпіричних даних та експертних оцінок міжнародних організацій і розкриває практичні результати імплементації різних моделей та дозволяє оцінити їх функціональність у реальних умовах.

Найбільш контрастним параметром виявляється швидкість реагування: тайванська модель забезпечує реакцію менше ніж за годину завдяки децентралізованій мережі волонтерів, тоді як європейські інституції потребують 24-48 годин через бюрократичні процедури узгодження.

Показник охоплення населення верифікацією, що відображає глибину проникнення антидезінформаційних механізмів у суспільство, демонструє перевагу фінського освітнього підходу з 80-90% охопленням, що пояснюється системною інтеграцією медіаграмотності в усі соціальні інститути. Довгострокова стійкість суспільства корелює з глибиною імплементації антидезінформаційних механізмів: превентивна освітня стратегія Фінляндії створює найміцніший імунітет до маніпуляцій.

Адаптивність систем залежить від їх технологічної гнучкості: Тайвань та Естонія швидко реагують на нові виклики через використання IT-рішень, тоді як законодавчі зміни в ЄС потребують тривалих процедур. Економічний аспект демонструє значну варіативність витрат від 30 до понад 500 мільйонів євро річно, що робить вибір моделі критично залежним від бюджетних можливостей держави.

Таблиця 1.5 – Механізми міжсекторальної взаємодії у протидії дезінформації

Сектор взаємодії	*Роль держави*	*Роль платформ*	*Роль громадянського суспільства*	*Приклади успішної практики*
Регуляторна координація	Розробка норм, нагляд	Саморегулювання, звітність	Моніторинг дотримання	DSA (ЄС), прозорість алгоритмів
Фактчекінг	Фінансування, методологія	Надання даних, API	Верифікація контенту	IFCN мережа, Cofacts (Тайвань)
Медіаосвіта	Програми, стандарти	Освітній контент, інструменти	Тренінги, інформування	Faktabaari (Фінляндія), NewsGuard
Технологічні рішення	Замовлення, тестування	Розробка AI-систем	Краудсорсинг даних	EUvsDisinfo, Troll Tracker (Естонія)
Дослідження	Гранти, замовлення	Доступ до даних	Аналітика, публікації	NATO StratCom COE, DFRLab

Джерело: розробка автора.

Таблиця міжсекторальної взаємодії, що відображає складну екосистему співпраці між різними акторами, ілюструє, що ефективна протидія маніпулятивному контенту неможлива без координації зусиль державних інституцій, технологічних платформ та організацій громадянського суспільства, кожен з яких володіє унікальними компетенціями та ресурсами.

Держава, виконуючи роль регулятора та координатора системи, встановлює правові рамки та забезпечує фінансування критично важливих програм медіаграмотності та досліджень. Технологічні платформи, володіючи величезними масивами даних та алгоритмічними інструментами виявлення аномалій, несуть відповідальність за розробку систем автоматичного виявлення

та обмеження поширення дезінформації. Громадянське суспільство, представлене незалежними медіа, фактчекерами та активістами, забезпечує незалежний моніторинг, верифікацію контенту та освітню діяльність, гарантуючи прозорість та підзвітність усіх учасників процесу.

Найуспішніші практики виникають на перетині секторів: платформа Cofacts об'єднує технологічну інфраструктуру, громадянську активність та державну підтримку, натомість NATO StratCom COE демонструє синергію міжнародної координації, академічних досліджень та практичного застосування результатів у національних стратегіях безпеки.

Синтез міжнародного досвіду, проаналізованого через призму різних національних контекстів та безпекових викликів, дозволяє сформулювати стратегічні рекомендації для побудови української моделі протидії дезінформації [48]. Аналіз міжнародної практики у сфері протидії дезінформації показує необхідність адаптації глобальних підходів до специфіки національного інформаційного простору [40].

По-перше, критично важливим є запровадження системи швидкого реагування на зразок тайванської, адаптованої до специфіки українського інформаційного простору та умов воєнного стану.

По-друге, необхідні довгострокові інвестиції в медіаграмотність населення, використовуючи фінський досвід інтеграції критичного мислення в освітню систему та враховуючи специфіку української освітньої традиції.

По-третє, доцільно розробити власний регуляторний фреймворк, який враховує кращі практики DSA та адаптований до національних реалій, що враховує кращі практики DSA, але адаптований до національних реалій та пріоритетів безпеки.

По-четверте, необхідно активізувати співпрацю з естонськими партнерами для імплементації технологічних рішень раннього попередження [72].

Україна, маючи унікальний досвід протистояння гібридній агресії та накопичений експертний потенціал, має унікальну можливість створити інноваційну модель, що поєднує найкращі елементи проаналізованих підходів.

Досвід активного громадянського суспільства, розвинутий під час Революції Гідності та повномасштабної війни, створює підґрунтя для краудсорсингових ініціатив на зразок Cofacts, адаптованих до українських месенджерів та соціальних мереж. Наявність потужної ІТ-індустрії, визнаної на міжнародному рівні своєю інноваційністю та технологічною компетентністю, дозволяє розробляти власні технологічні рішення для виявлення дезінформації, не покладаючись виключно на іноземні платформи та захищаючи національні дані.

Водночас, тісна співпраця з європейськими партнерами та участь у міжнародних мережах фактчекінгу забезпечить доступ до глобальної експертизи та ресурсів [90]. Український досвід протистояння російській пропаганді може стати цінним внеском у світову практику боротьби з авторитарними інформаційними кампаніями.

Пріоритетними напрямками для України, визначеними на основі аналізу міжнародного досвіду та національних потреб, мають стати:

– створення національної системи раннього попередження інформаційних загроз, інтегрованої з європейською мережею RapidAlert;

– розробка комплексної програми медіаосвіти для всіх рівнів освіти та різних демографічних груп, включаючи внутрішньо переміщених осіб та ветеранів;

– запровадження стимулів для платформ щодо боротьби з дезінформацією через механізми саморегулювання та прозорості алгоритмів;

– побудова мережі незалежних фактчекінгових організацій з прозорим фінансуванням та міжнародною сертифікацією;

– інвестування в дослідження технологій штучного інтелекту для автоматичного виявлення маніпулятивного контенту, включаючи дипфейки та синтетичні медіа [80].

Реалізація цих заходів, підкріплена політичною волею та міжнародною підтримкою, за оцінками експертів, може підвищити стійкість українського суспільства до дезінформації на 40-60% протягом 3-5 років [35].

РОЗДІЛ 2
АНАЛІЗ МЕХАНІЗМІВ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ В ОРГАНАХ ПУБЛІЧНОЇ ВЛАДИ УКРАЇНИ В УМОВАХ ВОЄННОГО СТАНУ

2.1 Інституційна система протидії дезінформаційним компаніям в Україні: структура, повноваження, координація

Інституційна система протидії дезінформаційним компаніям в Україні, що формувалася протягом останнього десятиліття в умовах російської агресії, являє собою складну багаторівневу структуру державних органів, координаційних механізмів та партнерських мереж.

Повномасштабне вторгнення Російської Федерації в Україну у лютому 2022 року актуалізувало критичну важливість ефективної протидії інформаційним загрозам та спричинило суттєву трансформацію існуючих інституційних механізмів відповідно до викликів воєнного стану [73]. Еволюція української системи протидії дезінформації відбувалася під безпосереднім впливом масштабних російських інформаційних операцій, спрямованих на підрив довіри до державних інституцій, дестабілізацію суспільства та виправдання військової агресії перед міжнародною спільнотою [79].

Вплив дезінформації на національну безпеку України в умовах воєнного стану набув екзистенційного характеру, загрожуючи не лише інформаційному простору, але й обороноздатності та територіальній цілісності держави [60]. Аналіз інституційної архітектури протидії дезінформації дозволяє виявити як досягнення української моделі, так і системні виклики, що потребують оптимізації в умовах тривалого протистояння гібридним загрозам.

Нормативно-правова база протидії дезінформації в Україні, закладена ще до повномасштабного вторгнення, зазнала суттєвих змін та доповнень у відповідь на інформаційні виклики воєнного часу. Базовим документом

стратегічного планування є Доктрина інформаційної безпеки України, затверджена Указом Президента у 2017 році, яка визначає національні інтереси України в інформаційній сфері та основні напрями їх забезпечення [76].

Стратегія інформаційної безпеки України, затверджена у 2021 році, конкретизувала цілі та завдання держави на період до 2025 року, включаючи протидію дезінформаційним компаніям та розвиток медіаграмотності населення [84]. План заходів з реалізації Стратегії, затверджений Кабінетом Міністрів України у 2024 році, визначив конкретні кроки, відповідальних виконавців та терміни імплементації [56].

Закон України «Про інформацію» (1992 р., з численними змінами) встановлює правові основи інформаційної діяльності та визначає основні принципи інформаційних відносин, включаючи достовірність, повноту та об'єктивність інформації. Закон України «Про національну безпеку України» (2018 р.), що визначив новий формат системи національної безпеки після анексії Криму та початку війни на Донбасі, закріплює інформаційну безпеку як одну з ключових складових національної безпеки держави [75].

З початком повномасштабної війни було прийнято низку президентських указів та рішень РНБО, що вводили додаткові заходи протидії дезінформації в умовах воєнного стану, включаючи єдиний телемарафон, обмеження доступу до російських інформаційних ресурсів та посилення контролю за інформаційним простором [73].

Правові аспекти протидії дезінформації в умовах воєнного стану вимагають балансування між ефективним захистом національної безпеки та дотриманням конституційних прав громадян на свободу слова та доступ до інформації [49]. Правове регулювання інформаційного обміну між державними інституціями набуло особливого значення для координації протидії дезінформаційним загрозам [63].

Центральним координаційним органом у сфері національної безпеки, включаючи інформаційну безпеку, є Рада національної безпеки і оборони України (РНБО), яка координує та контролює діяльність органів виконавчої

влади у сфері національної безпеки та оборони. РНБО, очолювана Президентом України, розробляє стратегічні документи інформаційної безпеки, приймає рішення щодо санкцій проти дезінформаційних ресурсів та координує діяльність різних відомств у протидії інформаційним загрозам [82].

При РНБО функціонує Центр протидії дезінформації, створений у 2021 році, який здійснює моніторинг інформаційних загроз, аналітичну діяльність та координацію антидезінформаційних заходів [70, 88]. Апарат РНБО, укомплектований фахівцями з питань інформаційної безпеки, здійснює моніторинг загроз, підготовку аналітичних матеріалів та координацію міжвідомчої взаємодії. Під час воєнного стану роль РНБО як координуючого центру суттєво посилилася, що проявилося у прийнятті низки ключових рішень щодо регулювання інформаційного простору та санкцій проти пропагандистських каналів.

Показовим прикладом діяльності РНБО стало рішення від 2 лютого 2021 року про застосування санкцій проти телеканалів «112 Україна», NewsOne та ZIK, введене в дію Указом Президента, що стало безпрецедентним кроком у протидії проросійським інформаційним впливам. Аналітичне обґрунтування санкцій базувалося на доказах систематичного поширення цими каналами дезінформації, фінансування народним депутатом Тарасом Козаком, пов’язаним з проросійськими колами та Віктором Медведчуком, та використання медіа-активів для просування наративів, що підривають національну безпеку України.

Рішення РНБО, підтримане Президентом Володимиром Зеленським, передбачало блокування трансляції каналів на п’ять років та заморожування активів їхніх власників, що викликало міжнародну дискусію про баланс між безпекою та свободою слова. З аналітичної точки зору, це рішення продемонструвало готовність української влади використовувати жорсткі адміністративні механізми для захисту інформаційного простору за рік до повномасштабного вторгнення, коли загрози гібридної війни вже були очевидними, але міжнародна спільнота ще не повністю усвідомлювала їхню гостроту. Ефективність заходу підтвердилася після 24 лютого 2022 року, коли

заблоковані канали не змогли транслювати російську пропаганду українській аудиторії у критичний момент початку повномасштабної війни, що могло б посилити панічні настрої та дезорієнтацію населення.

Другим ключовим прикладом є рішення РНБО від березня 2022 року про комплексне блокування російських інформаційних ресурсів та посилення контролю за інформаційним простором у перші тижні повномасштабного вторгнення, коли російська пропагандистська машина розгорнула масштабну кампанію дезінформації про хід бойових дій та наміри України. Рішення, ратифіковане Указом Президента в умовах воєнного стану, передбачало повне блокування доступу до російських телеканалів, новинних сайтів, включаючи РИА Новости, ТАСС, RT, Sputnik, та посилення моніторингу соціальних мереж на предмет поширення пропагандистського контенту.

Аналітичне значення цього рішення полягає у визнанні інформаційної війни як невід'ємної складової військового конфлікту, де контроль за інформаційним простором є критично важливим для збереження морального духу населення, запобігання паніці та дезорієнтації у перші дні вторгнення, коли ситуація була найбільш хаотичною.

РНБО, координуючи зусилля СБУ, Мінцифри та інших відомств, забезпечила швидку імплементацію блокувань через інтернет-провайдерів та технологічні платформи, що суттєво обмежило прямий вплив російської пропаганди на українську аудиторію. Це рішення також стало сигналом для міжнародних партнерів про серйозність інформаційної загрози та необхідність координованих дій у глобальному масштабі, що згодом вилилося у блокування RT та Sputnik у Європейському Союзі та обмеження російського контенту на провідних цифрових платформах світу.

Центр стратегічних комунікацій та інформаційної безпеки (StratCom Ukraine), створений у 2014 році при Міністерстві культури та інформаційної політики, є профільною інституцією безпосередньо відповідальною за оперативну протидію дезінформації [89]. Центр виконує функції моніторингу інформаційного простору, виявлення та аналізу дезінформаційних кампаній,

оперативного спростування фейків через офіційні канали комунікації та координації стратегічних комунікацій державних органів.

З початку повномасштабної війни StratCom запровадив щоденну практику публікації спростувань основних дезінформаційних наративів у форматі інфографіки через офіційні канали у соціальних мережах та месенджерах, зокрема Telegram та Facebook [61]. Команда Центру, укомплектована аналітиками, комунікаційними фахівцями та спеціалістами з кібербезпеки, працює цілодобово, забезпечуючи швидке реагування на інформаційні загрози в режимі реального часу. Діяльність StratCom охоплює як внутрішню аудиторію (українське населення), так і зовнішню (міжнародна спільнота, російськомовна аудиторія на окупованих територіях та в РФ).

Таблиця 2.1 – Інституційна структура протидії дезінформації в Україні: ключові органи та їх повноваження

Інституція	*Статус*	*Ключові повноваження у протидії дезінформації*	*Інструменти діяльності*
Рада національної безпеки і оборони України	Координаційний орган при Президентові	Розробка стратегії інформаційної безпеки, прийняття рішень про санкції, координація відомств	Рішення РНБО, стратегічні документи, санкційні списки
Центр стратегічних комунікацій та інформаційної безпеки	Структурний підрозділ МКІП	Моніторинг дезінформації, оперативне спростування фейків, аналітика, координація комунікацій	Щоденні спростування, соцмережі, аналітичні звіти, брифінги
Міністерство цифрової трансформації	ЦОВВ	Цифрова безпека, блокування шкідливих ресурсів, розробка застосунків для верифікації	Додаток «Дія», блокування сайтів, е-сервіси, цифрові комунікації
Служба безпеки України	Правоохоронний орган	Виявлення та припинення діяльності дезінформаторів, кіберрозслідування, контррозвідка	Оперативно-розшукові заходи, кіберполіція, судові процеси
Генеральний штаб ЗСУ	Військовий орган	Інформаційно-психологічні операції, військові комунікації, протидія ворожій пропаганді	ІПСО, військові брифінги, стратегічні комунікації на фронті

Продовження таблиці 2.1

Інституція	*Статус*	*Ключові повноваження у протидії дезінформації*	*Інструменти діяльності*
Офіс Президента	Адміністрація Президента	Формування загальнодержавних наративів, координація урядових комунікацій, міжнародна комунікація	Президентські брифінги, офіційні заяви, міжнародні виступи

Джерело: розробка автора.

Представлена таблиця, що систематизує інституційну структуру протидії дезінформації в Україні на основі аналізу нормативно-правових актів та практики функціонування органів влади, демонструє багаторівневий характер системи та розподіл повноважень між різними типами інституцій.

Координаційну роль виконує РНБО, забезпечуючи стратегічне планування та міжвідомчу узгодженість дій, що є критично важливим в умовах необхідності швидкої та скоординованої відповіді на багатовекторні інформаційні загрози.

Оперативну функцію безпосередньої протидії дезінформації виконує StratCom, який став фактичним «фронтофісом» держави у інформаційному протиборстві, забезпечуючи щоденне спростування російських фейків та формування контрнаративів.

Технологічну підтримку надає Міністерство цифрової трансформації, використовуючи цифрові інструменти для блокування пропагандистських ресурсів та створення платформ верифікації інформації.

Правоохоронну складову забезпечує СБУ, що виявляє та припиняє діяльність агентів впливу та організаторів дезінформаційних кампаній на території України.

Військовий компонент представлений Генеральним штабом ЗСУ, який проводить інформаційно-психологічні операції у зоні бойових дій та забезпечує комунікацію з військовослужбовцями.

Офіс Президента координує загальнодержавний наратив та забезпечує міжнародну комунікацію на найвищому політичному рівні, формуючи образ України у світовому інформаційному просторі.

Міністерство цифрової трансформації України, створене у 2019 році під керівництвом Михайла Федорова, відіграє ключову роль у технологічному забезпеченні протидії дезінформації через цифрові інструменти та платформи [66]. Найбільш відомим продуктом є застосунок «Дія», що об'єднує державні сервіси та інформаційні ресурси, включаючи верифіковану інформацію про події війни, повітряні тривоги та офіційні повідомлення органів влади. Міністерство також координує блокування російських пропагандистських ресурсів у цифровому просторі через взаємодію з інтернет-провайдерами та міжнародними платформами.

З початку повномасштабної війни Мінцифри запустило низку ініціатив, спрямованих на протидію дезінформації, включаючи «Армію ІТ», що залучає цивільних фахівців до кібероборони та інформаційного протиборства [15]. Цифрові комунікації Міністерства через Telegram-канал, що налічує мільйони підписників, стали одним з найбільш довірених джерел офіційної інформації для української аудиторії.

Служба безпеки України виконує правоохоронну та контррозвідувальну функції у протидії дезінформації, зосереджуючись на виявленні агентів впливу, організаторів інформаційних операцій та розповсюджувачів деструктивного контенту [77]. Кіберпідрозділи СБУ здійснюють моніторинг цифрового простору, виявляють координовані дезінформаційні мережі та проводять розслідування злочинів у сфері інформаційної безпеки. З початку повномасштабного вторгнення СБУ викрила десятки агентів російських спецслужб, що займалися збором розвідувальної інформації під прикриттям журналістської діяльності та поширенням дезінформації про дислокацію українських військ [83]. Контррозвідувальна діяльність СБУ включає блокування ботових мереж у соціальних мережах, які використовувалися для масового поширення паніки та деморалізуючих матеріалів серед українського населення. Правові обмеження СБУ пов'язані з необхідністю балансування між ефективністю протидії загрозам та дотриманням конституційних прав громадян на свободу слова.

Генеральний штаб Збройних Сил України через підрозділи інформаційно-психологічних операцій (ІПСО) здійснює комунікацію з військовослужбовцями, населенням прифронтових територій та аудиторією на тимчасово окупованих територіях [46]. Військові комунікації включають щоденні брифінги речника Генштабу, що надають верифіковану інформацію про перебіг бойових дій, втрати противника та ситуацію на фронті, формуючи альтернативу російським пропагандистським наративам про «успіхи спецоперації». ІПСО ЗСУ проводять цільові інформаційні операції, спрямовані на деморалізацію російських військ, заохочення їх до здачі в полон та інформування про можливість скористатися проєктом «Хочу жити». Військовий компонент протидії дезінформації тісно координується з цивільними інституціями через механізми узгодження комунікаційної стратегії та обміну розвідувальною інформацією про ворожі інформаційні операції [27].

Таблиця 2.2 – Нормативно-правова база протидії дезінформації в Україні: ключові документи

Документ	*Рік прийняття*	*Статус*	*Ключові положення щодо дезінформації*
Закон України «Про інформацію»	1992 (зі змінами)	Чинний закон	Визначення достовірності інформації, відповідальність за поширення неправдивої інформації
Доктрина інформаційної безпеки України	2017	Стратегічний документ	Національні інтереси в інформаційній сфері, загрози та напрями їх нейтралізації
Закон України «Про національну безпеку України»	2018	Чинний закон	Інформаційна безпека як складова національної безпеки, повноваження органів влади
Стратегія інформаційної безпеки України	2021	Стратегічний документ	Стратегічні цілі та завдання на період до 2025 року
Рішення РНБО про санкції проти пропагандистських каналів	2021-2025	Акти застосування	Блокування «112 Україна», NewsOne, ZIK, російських каналів та сайтів

Продовження таблиці 2.2

Документ	*Рік прийняття*	*Статус*	*Ключові положення щодо дезінформації*
Закон України «Про медіа»	2022	Чинний закон	Регулювання діяльності медіа, відповідальність за дезінформацію в умовах воєнного стану
Укази Президента про воєнний стан	2022-2025	Акти застосування	Тимчасові обмеження інформаційної діяльності, єдиний телемарафон, заборона російського контенту

Джерело: розробка автора.

Нормативно-правова база протидії дезінформації в Україні, яка систематизована у таблиці на основі аналізу законодавчих актів та стратегічних документів, демонструє еволюційний характер розвитку правового регулювання у відповідь на зростаючі інформаційні виклики.

Базові закони 1990-х років, прийняті ще в період становлення незалежності, встановили загальні принципи інформаційної діяльності, але виявилися недостатніми для протидії сучасним формам дезінформації у цифровому середовищі. Доктрина інформаційної безпеки 2017 року стала першим стратегічним документом, що системно визначив загрози інформаційній безпеці України після анексії Криму та визнав гібридну війну як новий тип конфлікту, де інформаційна складова відіграє критичну роль.

Закон про національну безпеку 2018 року вперше чітко закріпив інституційні повноваження різних органів влади у сфері інформаційної безпеки, створивши правову основу для координованої протидії загрозам. Рішення РНБО про санкції проти пропагандистських каналів стали інструментом оперативного реагування на конкретні загрози, хоча і викликали дискусії щодо балансу між безпекою та свободою слова.

Закон про медіа 2022 року, прийнятий вже після початку повномасштабного вторгнення, встановив нові стандарти відповідальності медіа за достовірність інформації в умовах війни. Укази Президента про воєнний стан ввели тимчасові обмеження, включаючи єдиний телемарафон та заборону російського контенту, що стало необхідним заходом для протидії ворожій

пропаганді в умовах екзистенційної загрози державності.

Механізми міжвідомчої координації у протидії дезінформації в Україні включають як формалізовані структури, так і неформальні практики оперативної взаємодії між інституціями. На стратегічному рівні координацію здійснює РНБО через регулярні наради та робочі групи з питань інформаційної безпеки, де представники різних відомств узгоджують позиції та вироблюють спільні рішення [59].

На оперативному рівні функціонує Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки, яка координує поточну діяльність та вирішує тактичні питання взаємодії. З початком повномасштабної війни було створено ситуаційні центри та координаційні штаби, що забезпечують цілодобову комунікацію між відомствами та оперативне реагування на інформаційні загрози [73]. Практика щоденних координаційних нарад представників StratCom, Офісу Президента, Мінцифри, СБУ та Генштабу дозволяє узгоджувати месседжі, синхронізувати спростування та формувати єдиний інформаційний порядок денний.

Співпраця з громадянським суспільством та незалежними медіа є критично важливою складовою української моделі протидії дезінформації, що відрізняє її від авторитарних підходів, заснованих виключно на державному контролі. Українські фактчекінгові організації, включаючи VoxCheck, StopFake, Детектор медіа, здійснюють незалежну верифікацію інформації та співпрацюють з державними органами в рамках партнерських угод [32]. Фактчекінг як інструмент протидії дезінформації в умовах гібридних конфліктів довів свою ефективність завдяки методологічній строгості, прозорості процесу верифікації та залученню експертних спільнот до оцінки складних тверджень [50]. Під час війни українські фактчекери адаптували свою роботу до екстремальних умов, забезпечуючи швидку верифікацію інформації навіть в умовах обмеженого доступу до первинних джерел [64]. Міжнародна мережа фактчекерів IFCN (International Fact-Checking Network) сертифікувала українські організації, підтверджуючи їхню відповідність міжнародним стандартам незалежності та

прозорості методології. StopFake, заснований у 2014 році викладачами та студентами Києво-Могилянської академії, став піонером систематичного спростування російської пропаганди та накопичив унікальну базу даних дезінформаційних наративів [23]. Державні органи регулярно використовують матеріали незалежних фактчекерів як доказову базу для офіційних спростувань, визнаючи їхній авторитет у суспільстві. Фінансова підтримка фактчекінгових організацій здійснюється переважно міжнародними донорами, що гарантує їхню незалежність від державного впливу.

Таблиця 2.3 – Механізми координації у протидії дезінформації: рівні та інструменти

Рівень координації	*Формат взаємодії*	*Учасники*	*Частота*	*Функції*
Стратегічний	Засідання РНБО	Президент, Секретар РНБО, міністри, керівники силових відомств	За потребою (щотижня/щомісяця)	Прийняття стратегічних рішень, санкції, затвердження доктрин
Оперативно-тактичний	Міжвідомча комісія	Представники МКІП, Мінцифри, СБУ, ГШ ЗСУ, Офісу Президента	Щотижнево	Координація поточної діяльності, узгодження месседжів, розподіл завдань
Оперативний	Щоденні координаційні наради	StratCom, Мінцифри, прес-служби відомств	Щоденно	Синхронізація спростувань, узгодження комунікацій, реагування на виклики
Ситуаційний	Робочі групи за напрямками	Профільні фахівці відомств	За потребою	Робота над конкретними загрозами, розробка спільних продуктів
Партнерський	Взаємодія з громадянським суспільством	Держоргани + фактчекери + медіа	Постійна	Обмін інформацією, спільні проєкти, навчання, верифікація

Джерело: розробка автора.

Таблиця механізмів координації, розроблена на основі аналізу практики

функціонування української системи протидії дезінформації під час війни і ілюструє багаторівневу архітектуру взаємодії між інституціями. Стратегічний рівень, представлений засіданнями РНБО під головуванням Президента, забезпечує політичне керівництво та прийняття найважливіших рішень щодо інформаційної безпеки, включаючи санкції проти медіа-активів противника та затвердження національних стратегій.

Оперативно-тактичний рівень, реалізований через Міжвідомчу комісію, дозволяє представникам різних відомств регулярно узгоджувати підходи, розподіляти відповідальність за окремі напрямки та координувати ресурси для спільних ініціатив. Оперативний рівень щоденних координаційних нарад став критично важливим в умовах війни, коли необхідна швидка реакція на динамічні інформаційні загрози та узгодження месседжів між різними комунікаційними каналами держави. Ситуаційні робочі групи створюються для вирішення конкретних завдань, таких як протидія певному дезінформаційному наративу чи розробка спільної інформаційної кампанії, забезпечуючи гнучкість системи. Партнерський рівень співпраці з громадянським суспільством, що включає регулярний обмін інформацією та спільні проєкти з незалежними фактчекерами та медіа, підсилює легітимність державних зусиль та розширює охоплення аудиторії через довірені недержавні канали комунікації.

Міжнародне партнерство України у протидії дезінформації суттєво посилилося після початку повномасштабного вторгнення, коли західні партнери визнали російську пропаганду як загрозу не лише для України, а й для глобальної демократії. Україна інтегрована у European External Action Service East StratCom Task Force, що координує зусилля країн ЄС у протидії російській дезінформації та публікує щотижневий огляд «Disinformation Review» [13]. Співпраця з NATO StratCom Centre of Excellence забезпечує доступ до методологічної експертизи та навчальних програм для українських фахівців. США через USAID фінансують програми розвитку медіаграмотності та підтримки незалежних медіа в Україні, інвестуючи десятки мільйонів доларів у зміцнення інформаційної стійкості [36]. Британське Foreign, Commonwealth and Development Office підтримує українські

фактчекінгові організації та проводить тренінги для журналістів. Канада через Canadian International Development Agency фінансує проєкти боротьби з дезінформацією на регіональному рівні в Україні.

2.2 Практики та інструменти протидії російській дезінформації органами публічної влади України (2022-2025 рр.)

Практична діяльність органів публічної влади України у протидії російській дезінформації в період повномасштабної війни 2022-2025 років характеризується безпрецедентним масштабом, інтенсивністю та інноваційністю застосовуваних інструментів. Російська Федерація з перших годин вторгнення розгорнула масштабну дезінформаційну кампанію, спрямовану на виправдання агресії, деморалізацію українського суспільства, дискредитацію керівництва держави та маніпулювання міжнародною громадською думкою [2].

Інструменти інформаційної війни Росії проти України під час повномасштабної агресії включали комбінацію традиційних пропагандистських методів та сучасних цифрових технологій маніпулювання громадською думкою [42]. Українські державні інституції, використовуючи досвід протидії російським інформаційним операціям з 2014 року та адаптуючи кращі міжнародні практики, створили комплексну систему реагування, що поєднує технологічні рішення, стратегічні комунікації, правові механізми та залучення громадянського суспільства [71]. Ефективність протидії російській дезінформації в Україні залежить від координації зусиль державних органів, громадянського суспільства та міжнародних партнерів [87]. Аналіз конкретних практик та інструментів дозволяє виявити ефективність різних підходів та сформулювати рекомендації щодо їх подальшого вдосконалення в умовах тривалого протистояння гібридній агресії.

Система моніторингу та раннього виявлення дезінформації, створена

українськими державними органами, функціонує цілодобово, відстежуючи інформаційний простір у режимі реального часу через автоматизовані та експертні методи аналізу. StratCom використовує спеціалізоване програмне забезпечення для моніторингу українських та російських соціальних мереж, телеграм-каналів, сайтів та телевізійних трансляцій, виявляючи аномальну активність, координовані кампанії та вірусний дезінформаційний контент [31]. Визначення алгоритмів протидії дезінформації в діяльності державних органів базується на комплексному підході, що поєднує технологічні, правові та комунікаційні інструменти [91]. Система раннього виявлення інформаційних загроз інтегрована з технічними рішеннями у сфері кібербезпеки, що дозволяє оперативно ідентифікувати та нейтралізувати дезінформаційні атаки [81].

Аналітики Центру щоденно опрацьовують сотні потенційних дезінформаційних повідомлень, верифікуючи їх через перехресну перевірку джерел, аналіз метаданих та консультації з профільними експертами. Алгоритми машинного навчання, розроблені за підтримки міжнародних партнерів, дозволяють автоматично виявляти патерни координованої поведінки ботових мереж та ідентифікувати джерела дезінформації [16]. Мінцифри розробило власні інструменти моніторингу цифрового простору, що інтегруються з системами кібербезпеки та дозволяють швидко реагувати на масові атаки через шкідливий контент.

Практика оперативного спростування дезінформації, що стала візитною карткою роботи українських державних органів під час війни, базується на принципі швидкості реагування та використанні доступних цифрових каналів комунікації. Комунікаційні інструменти протидії недостовірній інформації в Україні включають як традиційні методи офіційних спростувань, так і інноваційні підходи з використанням соціальних мереж, месенджерів та інтерактивних платформ [45]. StratCom запровадив щоденну публікацію спростувань основних російських фейків у форматі візуалізованої інфографіки, що поєднує факти, аналіз та емоційне звернення до аудиторії [61]. Спростування публікуються одночасно на офіційному сайті, у Telegram-каналі (понад 500 тисяч

підписників), Facebook, Twitter та Instagram, забезпечуючи максимальне охоплення різних сегментів аудиторії.

Формат інфографіки, розроблений з урахуванням психологічних особливостей сприйняття інформації у соціальних мережах, включає лаконічний заголовок, ключові факти, візуальні елементи та посилання на джерела [37]. Міністерства та відомства також ведуть активні комунікаційні канали, де оперативно спростовують дезінформацію у своїх сферах компетенції: Міністерство оборони – щодо військової ситуації, МОЗ – щодо гуманітарної ситуації, МЗС – щодо міжнародної підтримки.

Таблиця 2.4 – Типологія інструментів протидії дезінформації органами публічної влади України (2022-2025)

Категорія інструментів	*Конкретні інструменти*	*Відповідальні інституції*	*Цільова аудиторія*	*Показники ефективності*
Моніторинг та виявлення	Автоматизовані системи аналізу соцмереж, експертний моніторинг медіа	StratCom, СБУ, Мінцифри	Внутрішній аналіз	500+ фейків виявлено щоденно
Оперативне спростування	Інфографіка, пости у соцмережах, брифінги	StratCom, прес-служби відомств	Українці, міжнародна аудиторія	3000+ спростувань за 2022-2024
Стратегічні комунікації	Координовані месседжі, наративні кампанії, бренд України	Офіс Президента, МКІП, МЗС	Внутрішня та міжнародна аудиторія	Зростання довіри до держави до 80%
Цифрові платформи	Додаток «Дія», Telegram-канали, урядові сайти	Мінцифри, усі відомства	Українці	20+ млн користувачів «Дії»
Блокування контенту	Санкції проти сайтів, блокування каналів, видалення контенту	РНБО, СБУ, Мінцифри, платформи	Інформаційний простір України	500+ ресурсів заблоковано
Медіаосвіта	Освітні програми, тренінги, інформаційні кампанії	МКІП, МОН, НГО	Громадяни, учні, вчителі	100,000+ осіб охоплено
Міжнародна співпраця	Обмін інформацією, спільні проєкти, тренінги	МЗС, СБУ, StratCom	Міжнародні партнери	Членство в EU StratCom Task Force

Джерело: розробка автора.

Типологія інструментів протидії дезінформації, систематизована на основі аналізу практики роботи українських державних органів протягом 2022-2025 років і демонструє комплексність та багатоаспектність підходу до інформаційного протиборства. Моніторинг та виявлення дезінформації становлять базову функцію, що забезпечує раннє попередження про загрози та дозволяє оперативно мобілізувати ресурси для відповіді, при цьому щоденне виявлення сотень фейків свідчить про масштаби російської дезінформаційної кампанії проти України.

Оперативне спростування через цифрові канали, що стало найбільш видимим елементом протидії для широкої аудиторії, забезпечує швидку нейтралізацію шкідливих наративів, при цьому понад 3000 спростувань за три роки демонструють систематичний характер роботи.

Стратегічні комунікації виходять за межі реактивного спростування, формуючи позитивні наративи про Україну, її стійкість та цінності, що відбилося у зростанні довіри населення до державних інституцій до рекордних 80% за даними соціологічних опитувань. Цифрові платформи, насамперед додаток «Дія» з 20 мільйонами користувачів, створили прямий канал комунікації між державою та громадянами, мінімізуючи ризики маніпуляцій через посередників.

Блокування шкідливого контенту, що викликає дискусії щодо балансу з свободою слова, виявилося необхідним заходом для обмеження впливу російської пропаганди в критичні періоди інформаційних атак. Медіаосвіта, орієнтована на довгострокову стійкість суспільства до маніпуляцій, охопила понад 100 тисяч громадян через різноманітні програми та тренінги. Міжнародна співпраця забезпечила інтеграцію України у глобальні мережі протидії дезінформації та доступ до експертизи і ресурсів партнерів.

Стратегічні комунікації українських державних органів у період війни еволюціонували від простого реагування на російські фейки до проактивного формування власних потужних наративів про Україну, її історію, цінності та бачення майбутнього. Офіс Президента, координуючи загальнодержавну комунікаційну стратегію, забезпечив формування образу України як

європейської демократичної нації, що героїчно протистоїть авторитарній агресії та захищає цінності вільного світу [69]. Виступи Президента Володимира Зеленського перед парламентами демократичних країн, міжнародними організаціями та на глобальних форумах стали потужним інструментом стратегічних комунікацій, що забезпечив мобілізацію міжнародної підтримки України. Координація месседжів між різними відомствами, реалізована через щоденні наради та спільні робочі групи, дозволила уникнути суперечностей в офіційних заявах та забезпечити послідовність інформаційної політики [73].

Розробка єдиного глосарію термінів, що використовуються у комунікації про війну («повномасштабне вторгнення», а не «конфлікт»; «тимчасово окуповані території», а не «ОРДЛО»), забезпечила лінгвістичну узгодженість та протидію російським спробам нав’язати свою термінологію.

Цифрові інструменти та технології стали критично важливою складовою протидії дезінформації, дозволяючи швидко охоплювати мільйони громадян верифікованою інформацією. Додаток «Дія», запущений Мінцифри у 2020 році як платформа державних сервісів, під час війни трансформувався на універсальний інструмент урядових комунікацій, включаючи повідомлення про повітряні тривоги, офіційні оголошення, верифіковану інформацію про події війни [53].

Функція «єВорог» дозволяє громадянам повідомляти про виявлені російські війська, техніку чи диверсантів, перетворюючи мільйони українців на мережу інформаційних сенсорів. Telegram-канали державних органів, що стали основним каналом оперативної комунікації, забезпечують швидке поширення офіційних повідомлень та спростувань, при цьому канал Офісу Президента налічує понад 2 мільйони підписників [34]. Використання штучного інтелекту для виявлення дезінформації, що розробляється за підтримки міжнародних партнерів, дозволяє автоматично ідентифікувати підозрілий контент та координовані маніпулятивні кампанії.

Правові та адміністративні механізми протидії дезінформації в умовах воєнного стану включають санкції проти пропагандистських ресурсів,

кримінальне переслідування дезінформаторів та регулювання інформаційного простору. РНБО прийняла низку рішень про застосування санкцій до російських та проросійських українських медіа-активів, включаючи блокування сайтів, заборону трансляції телеканалів та заморожування активів [74]. СБУ розслідує кримінальні справи щодо осіб, що займаються поширенням дезінформації на користь противника, кваліфікуючи такі дії як державну зраду чи пособництво агресору.

Введення єдиного телемарафону «Єдині новини» на час воєнного стану стало контроверсійним рішенням, що, з одного боку, забезпечило координацію інформаційної політики та запобігло поширенню паніки, але, з іншого боку, викликало критику щодо обмеження медіаплюралізму [41]. Блокування російських соціальних мереж «ВКонтакте» та «Одноклассники» ще у 2017 році та посилення контролю за доступом до російських інформаційних ресурсів під час війни зменшило прямий вплив російської пропаганди на українську аудиторію.

Таблиця 2.5 – Ключові російські дезінформаційні наративи та відповіді українських органів влади (2022-2025)

Російський дезінформаційний наратив	*Мета наративу*	*Інструменти поширення*	*Відповідь українських органів влади*	*Ефективність протидії*
«Біолабораторії США в Україні створюють біологічну зброю»	Виправдання агресії, дискредитація США	Російські ЗМІ, дипломати, соцмережі	Спростування з доказами від МОЗ, Пентагону, відеоекскурсії лабораторіями	Висока: швидке спростування міжнародними фактчекерами
«Українська влада готує провокації проти власного населення»	Завчасне виправдання російських злочинів	RT, Sputnik, Telegram-канали	Попереджувальні спростування StratCom, документування злочинів РФ	Середня: наратив повторювався перед кожною атакою
«Україна має вести переговори та капітулювати»	Деморалізація, тиск на владу	Проросійські політики, боти у соцмережах	Президентські звернення про принципи миру, пояснення позиції	Висока: підтримка населенням позиції влади 75%+

Продовження таблиці 2.5

Російський дезінформаційний наратив	*Мета наративу*	*Інструменти поширення*	*Відповідь українських органів влади*	*Ефективність протидії*
«Західна зброя не допомагає Україні»	Підрив довіри до партнерів, зменшення допомоги	Російські медіа, дипломати	Демонстрація результатів на фронті, подяки партнерам, візуалізація	Висока: продовження військової допомоги Заходу
«Українська влада корумпована та розкрадає допомогу»	Підрив довіри до уряду, зменшення підтримки	Фейкові «розслідування», маніпуляції статистикою	Прозорість у витратах, арешти корупціонерів, звіти для донорів	Середня-висока: реформи посилюють довіру
«Втрати ЗСУ величезні, Україна програє війну»	Деморалізація суспільства та армії	Російські військові блогери, фейкові «інсайди»	Офіційні дані від Генштабу, успіхи на фронті, міжнародна підтримка	Середня: постійна боротьба з панічними настроями

Джерело: розробка автора.

Таблиця російських дезінформаційних наративів та відповідей українських органів влади, складена на основі аналізу щоденних моніторингових звітів StratCom та дослідження міжнародних фактчекінгових організацій за 2022-2025 роки, ілюструє систематичність та різноманітність російських інформаційних атак проти України.

Стратегії дезінформації Росії в російсько-українській війні базуються на комбінації перевірених пропагандистських технік радянської епохи та сучасних цифрових інструментів маніпулювання громадською думкою [45]. Наратив про «біолабораторії», запущений безпосередньо перед повномасштабним вторгненням та озвучений на засіданні Радбезу ООН російськими дипломатами, мав на меті створити псевдооб’єктивне виправдання агресії як «превентивної операції», але був швидко і переконливо спростований українською стороною через залучення американських партнерів та організацію відеоекскурсій для журналістів.

Превентивні звинувачення України у підготовці «провокацій проти власного населення» систематично використовувалися Росією перед здійсненням власних військових злочинів, таких як обстріли цивільних об’єктів

чи масові вбивства у Бучі, Маріуполі, Ізюмі, демонструючи циничну стратегію «проєкції» власних злочинів на противника.

Наратив про необхідність «переговорів та капітуляції» активізувався у періоди успішних контрнаступів ЗСУ і був спрямований на деморалізацію суспільства та створення тиску на українську владу, але зіткнувся з високим рівнем суспільної підтримки принципової позиції керівництва держави.

Дискредитація західної військової допомоги мала стратегічну мету зменшити обсяги підтримки через маніпулювання громадською думкою у країнах-партнерах, але українська сторона ефективно протидіяла через демонстрацію конкретних результатів використання озброєння на полі бою.

Звинувачення у корупції, що базувалися на реальних проблемах української системи управління, використовувалися Росією для підриву довіри до влади, але активна антикорупційна політика та прозорість у витрачанні міжнародної допомоги дозволили мінімізувати ефект цього наративу.

Дезінформація про «величезні втрати ЗСУ» та «програш війни» постійно циркулює у російському інформаційному просторі та через ботові мережі проникає в український сегмент соцмереж, вимагаючи систематичних зусиль з боку військових комунікаторів для підтримання морального духу як армії, так і цивільного населення.

Медіаосвітні ініціативи українських державних органів, спрямовані на підвищення стійкості суспільства до дезінформації через розвиток критичного мислення та навичок верифікації інформації, набули особливої актуальності в умовах війни. Міністерство освіти та науки України інтегрувало елементи медіаграмотності у шкільні програми, розробило методичні матеріали для вчителів та організувало тренінги з виявлення фейків [65]. Індекс медіаграмотності українців, що вимірюється незалежними дослідницькими організаціями, показав зростання здатності населення розпізнавати дезінформацію з 42% у 2021 році до 61% у 2024 році, що свідчить про ефективність освітніх програм [8].

Довіра до медіа в Україні, незважаючи на складні умови війни,

залишається на відносно високому рівні завдяки прозорості роботи журналістів та активній протидії дезінформації [57, 78]. Національна рада з питань телебачення і радіомовлення відіграє важливу роль у координації протидії дезінформації через регулювання діяльності медіа та забезпечення дотримання стандартів достовірності інформації в умовах війни [67]. МКІП запустило загальнонаціональну інформаційну кампанію «Не ведись на фейки», що включає відеоролики, інфографіку та інтерактивні матеріали для різних вікових груп.

Бібліотеки, трансформовані у центри медіаграмотності за фінської моделлю, проводять безкоштовні воркшопи для громадян, навчаючи основам перевірки інформації та виявлення маніпулятивних технік. Особлива увага приділяється роботі з вразливими групами, включаючи літніх людей, що найбільш схильні до впливу дезінформації, та внутрішньо переміщених осіб, що перебувають у стресовому стані та потребують надійних джерел інформації [54].

Інноваційні підходи до протидії дезінформації, розроблені українськими державними органами під час війни, включають використання гумору, креативності та партисипаторних технологій для залучення громадян. Меми та сатиричний контент, створювані офіційними та неофіційними комунікаторами, виявилися ефективним інструментом протидії російським наративам, роблячи спростування більш вірусними та запам’ятовуваними [30]. Кампанія «Russian warship, go f*** yourself», що виникла як спонтанна реакція на російський ультиматум захисникам острова Зміїний, була підхоплена офіційною комунікацією та стала глобальним символом опору. Залучення знаменитостей, спортсменів, блогерів до поширення верифікованої інформації та спростування фейків дозволило досягти аудиторій, недоступних для традиційних урядових каналів. Краудсорсингові ініціативи, включаючи платформу «Тримай курс», де громадяни можуть повідомляти про виявлені фейки, створили мережу добровольців-верифікаторів по всій країні [86].

Виклики та обмеження у протидії дезінформації, з якими стикаються українські державні органи, включають ресурсні обмеження, технологічне відставання від росту обсягів дезінформації та складність досягнення всіх

сегментів аудиторії. Асиметрія ресурсів у протистоянні з російською пропагандистською машиною, що фінансується мільярдами доларів з державного бюджету РФ, створює структурний виклик для України, змушуючи компенсувати кількість якістю, креативністю та міжнародною підтримкою [7].

Дезінформація як загроза демократії та державному управлінню вимагає не лише оперативного реагування, але й системних структурних змін у функціонуванні інформаційної екосистеми [58]. Відповідальність за дезінформацію під час війни набуває особливого значення, оскільки поширення неправдивої інформації може безпосередньо загрожувати життю людей та обороноздатності держави [51]. Технологічні обмеження у виявленні дипфейків та синтетичних медіа, створених з використанням генеративного штучного інтелекту, вимагають інвестицій у розробку власних систем автоматичної верифікації, включаючи інтелектуальні методи виявлення дезінформації в українських текстових даних [43]. Технологічні обмеження у виявленні дипфейків та синтетичних медіа, створених з використанням генеративного штучного інтелекту, вимагають інвестицій у розробку власних систем автоматичної верифікації. Інформаційні бульбашки у соціальних мережах ускладнюють досягнення аудиторій, що вже перебувають під впливом російської пропаганди, особливо на тимчасово окупованих територіях та серед російськомовного населення прикордонних регіонів [26]. Втома від інформації та зниження уваги до спростувань після тривалого періоду війни вимагає постійного оновлення форматів та підходів до комунікації.

РОЗДІЛ 3
ОПТИМІЗАЦІЯ МЕХАНІЗМІВ ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ В ПУБЛІЧНОМУ УПРАВЛІННІ УКРАЇНИ: СТРАТЕГІЧНІ ПРІОРИТЕТИ

3.1 Виклики та проблеми функціонування механізмів протидії дезінформації в органах публічної влади України

Аналіз функціонування механізмів протидії дезінформації в органах публічної влади України, здійснений на основі практики воєнного часу, виявляє низку системних викликів та структурних проблем, що обмежують ефективність антидезінформаційної діяльності та вимагають стратегічного переосмислення підходів до інформаційної безпеки. Попри безперечні досягнення української системи протидії дезінформації, що отримала міжнародне визнання за швидкість реагування, креативність підходів та залучення громадянського суспільства, існуючі механізми демонструють вразливість до довгострокових загроз та недостатню готовність до викликів посткризового періоду. Критичне осмислення цих проблем є необхідною передумовою для формування стратегії оптимізації системи протидії дезінформації, здатної ефективно функціонувати як в умовах активних бойових дій, так і в період постконфліктної трансформації суспільства.

Інституційна фрагментація та недостатня координація між різними органами публічної влади, відповідальними за протидію дезінформації, залишається однією з найбільш гострих проблем української системи інформаційної безпеки. Множинність інституцій, наділених повноваженнями у цій сфері, створює ризики дублювання зусиль, конфлікту повноважень та неефективного використання обмежених ресурсів. Основні прояви інституційної фрагментації включають:

1. Дублювання функцій моніторингу: РНБО, StratCom, СБУ та

Мінцифри паралельно відстежують інформаційний простір без єдиної системи обміну даними;

2. Конфлікт повноважень у прийнятті рішень: неясність щодо того, хто має право блокувати контент у різних ситуаціях;

3. Відсутність єдиного координаційного центру: рішення приймаються ситуативно через неформальні канали;

4. Нерівномірний розподіл ресурсів: центральні органи отримують левову частку фінансування, регіони залишаються недофінансованими;

5. Слабку вертикальну інтеграцію: місцеві органи влади діють автономно без методологічної підтримки з центру;

6. Залежність від особистих зв'язків: ефективність координації визначається особистими стосунками керівників, а не формальними процедурами.

Воєнний час, що вимагає швидких рішень та оперативної реакції на загрози, дещо замаскував цю проблему через неформальні практики координації та особисті зв'язки між керівниками відомств, проте в довгостроковій перспективі відсутність формалізованої системи координації створює ризики інституційної нестабільності та залежності від суб'єктивних факторів.

Особливо відчутною є недостатня координація між центральним та регіональним рівнями влади, де місцеві органи часто позбавлені необхідних компетенцій, ресурсів та методологічної підтримки для ефективної протидії локальним дезінформаційним кампаніям, що створює «сліпі зони» у загальнодержавній системі інформаційної безпеки.

Кадрові виклики, що проявляються у критичній нестачі висококваліфікованих фахівців з питань стратегічних комунікацій, фактчекінгу, аналізу даних та цифрових технологій у державних органах, суттєво обмежують спроможність системи адекватно відповідати на зростаючу складність дезінформаційних загроз. Дефіцит професійних компетенцій у сфері протидії дезінформації охоплює:

По-перше, стратегічних комунікаторів: брак фахівців, здатних розробляти

довгострокові наративні кампанії та координувати багатоканальні комунікації;

По-друге, дата-аналітиків: недостатня кількість спеціалістів з аналізу великих даних, здатних виявляти патерни координованих компаній;

По-третє, експертів з ШІ та машинного навчання: критична нестача розробників автоматизованих систем виявлення дезінформації;

По-четверте, психологів впливу: відсутність фахівців, що розуміють механізми когнітивних спотворень та психологічної маніпуляції;

По-п’яте, цифрових криміналістів: недостатня кількість експертів з верифікації синтетичних медіа та дипфейків;

По-шосте, міжнародних комунікаторів: брак фахівців зі знанням іноземних мов та культурних контекстів цільових аудиторій.

Українська система державної служби, яка побудована за традиційними адміністративними принципами, виявляється недостатньо гнучкою для залучення та утримання талановитих фахівців у високотехнологічних та креативних сферах, де приватний сектор пропонує значно кращі умови оплати праці та професійного розвитку.

Відсутність спеціалізованих освітніх програм з підготовки експертів у сфері протидії дезінформації, що поєднували б компетенції у комунікаціях, інформаційних технологіях, психології та міжнародних відносинах, призводить до того, що державні органи змушені покладатися на фахівців, що отримали освіту в суміжних галузях та самостійно опановують специфіку антидезінформаційної діяльності.

Плинність кадрів у державних структурах, спричинена як економічними факторами, так і високим рівнем стресу від роботи в умовах постійного інформаційного протиборства, призводить до втрати накопиченого досвіду та необхідності постійного навчання нових співробітників.

Технологічне відставання української системи протидії дезінформації від темпів розвитку самих дезінформаційних технологій створює зростаючий розрив між можливостями виявлення та нейтралізації загроз. Поява генеративних систем штучного інтелекту, здатних створювати реалістичні дипфейки,

синтетичні тексти та мультимедійний контент, що практично неможливо відрізнити від справжнього без спеціалізованих технологій верифікації, вимагає суттєвих інвестицій у розробку власних систем автоматичного виявлення маніпулятивного контенту. Українські державні органи переважно покладаються на ручний аналіз дезінформації експертами, що є трудомістким, повільним та не масштабованим підходом в умовах експоненційного зростання обсягів контенту у цифровому просторі.

Обмежені можливості фінансування досліджень та розробок у сфері антидезінформаційних технологій, що потребують мультимільйонних інвестицій та співпраці з провідними технологічними компаніями, змушують Україну покладатися на міжнародну технічну допомогу, що створює залежність від зовнішніх акторів та обмежує можливості адаптації рішень до специфіки національного інформаційного простору.

Нормативно-правові прогалини у регулюванні протидії дезінформації, що проявляються у відсутності комплексного законодавчого акту, який би чітко визначав правові межі дозволеного контенту, відповідальність різних акторів інформаційної екосистеми та процедури прийняття рішень щодо обмеження поширення шкідливої інформації, створюють ризики як надмірного, так і недостатнього регулювання. Ключові законодавчі прогалини включають:

– відсутність правового визначення дезінформації: термін не має чіткої дефініції у національному законодавстві, що призводить до різночитань;

– неврегульованість відповідальності платформ: онлайн-платформи не мають чітких зобов'язань щодо модерації шкідливого контенту;

– відсутність процедур апеляції: громадяни та організації не мають прозорих механізмів оскарження рішень про блокування контенту;

– фрагментарність нормативної бази: правові норми розпорошені між різними законами, указами та рішеннями РНБО;

– неузгодженість воєнно-часового та базового законодавства: тимчасові обмеження не мають чіткої дорожньої карти скасування після завершення воєнного стану;

– відсутність стандартів прозорості: державні органи не зобов'язані публічно звітувати про критерії та масштаби блокування контенту.

Фрагментарне законодавство, що розпорошене між різними нормативними актами та часто базується на воєнно-часових указах Президента, позбавлене системності та передбачуваності, необхідних для ефективного правозастосування та дотримання верховенства права. Особливо проблематичною є відсутність чіткого правового визначення самого поняття «дезінформації» у національному законодавстві, що призводить до різночитань у правозастосовній практиці та ризиків суб’єктивної інтерпретації цього терміну правоохоронними органами. Неврегульованість відповідальності онлайн-платформ за поширення дезінформації, що є критично важливим елементом європейської моделі регулювання, залишає український інформаційний простір вразливим до координованих маніпулятивних компаній через соціальні мережі.

Комунікативні виклики, пов’язані зі складністю досягнення всіх сегментів української аудиторії верифікованою інформацією та формуванням довіри до державних джерел у різних демографічних та регіональних групах, обмежують ефективність навіть найякісніших антидезінформаційних заходів. Цифровий розрив між містом та селом, молодшими та старшими поколіннями, західними та східними регіонами країни створює диференційовану вразливість різних груп населення до дезінформації та вимагає сегментованих комунікаційних стратегій, що враховують специфічні інформаційні потреби та звички споживання медіа.

Старше покоління, що переважно отримує інформацію з телебачення та менш активно використовує цифрові платформи верифікації фактів, залишається найбільш вразливим до впливу російської пропаганди, особливо у прикордонних регіонах з історично високим споживанням російськомовного контенту. Ефект інформаційних бульбашок у соціальних мережах, де алгоритмічна курація контенту створює замкнені комунікативні середовища з обмеженим плюралізмом думок, ускладнює проникнення офіційних спростувань до аудиторій, що вже перебувають під впливом дезінформаційних наративів.

Ресурсні обмеження, що проявляються у хронічній нестачі фінансування

антидезінформаційних програм порівняно з масштабами загрози та обсягами російських інвестицій у пропагандистську інфраструктуру, створюють структурну асиметрію у інформаційному протиборстві. Бюджетні виділення на протидію дезінформації, хоча й зросли після початку повномасштабного вторгнення, залишаються несумірними з багатомільярдними інвестиціями Російської Федерації у свою пропагандистську машину, що включає десятки телеканалів, сотні сайтів, тисячі платних блогерів та складну інфраструктуру ботових мереж.

Залежність від міжнародної донорської підтримки у фінансуванні критичних програм медіаграмотності, технологічних рішень та підтримки незалежних фактчекерів створює ризики нестабільності та зменшення можливостей у разі скорочення зовнішньої допомоги, що є ймовірним сценарієм у посткризовий період, коли увага міжнародної спільноти переключиться на інші виклики. Неефективність використання наявних ресурсів через бюрократичні процедури державних закупівель, що не адаптовані до специфіки швидкозмінного інформаційного середовища, призводить до затримок у впровадженні необхідних рішень та втрати актуальності запланованих заходів.

Психологічна втома суспільства від постійного інформаційного протиборства та зниження уваги до офіційних спростувань після тривалого періоду інтенсивної інформаційної війни створює виклик для підтримання ефективності комунікаційних стратегій у довгостроковій перспективі. Ефект звикання до постійного потоку фейків та спростувань призводить до того, що громадяни починають менше реагувати на попередження про дезінформацію та стають менш вибірковими у споживанні інформації, що парадоксально робить їх більш вразливими до витончених маніпуляцій. Зростаючий скептицизм та цинізм частини населення щодо будь-якої інформації, незалежно від джерела, що є наслідком тривалого перебування в умовах інформаційного хаосу, підриває довіру не лише до пропаганди, але й до легітимних джерел інформації, створюючи інформаційний нігілізм як непередбачувану побічну дію інтенсивної протидії дезінформації.

Відсутність довгострокової стратегії трансформації воєнно-часових механізмів протидії дезінформації до умов мирного часу створює ризик інституційної дезорієнтації у посткризовий період. Багато заходів, що є виправданими та ефективними в умовах активних бойових дій, включаючи єдиний телемарафон, розширені повноваження спецслужб у моніторингу інформаційного простору та обмеження доступу до певних інформаційних ресурсів, потребуватимуть перегляду після завершення воєнного стану для відновлення повноцінного медіаплюралізму та дотримання демократичних стандартів свободи слова.

Відсутність публічної дискусії про майбутню архітектуру системи інформаційної безпеки у мирний час, критерії пропорційності обмежень та механізми демократичного контролю за діяльністю антидезінформаційних структур створює ризики або надмірного збереження авторитарних елементів регулювання, або, навпаки, преципітаційної лібералізації, що залишить суспільство беззахисним перед гібридними загрозами, які не зникнуть з припиненням активної фази конфлікту.

3.2 Стратегічні напрями вдосконалення системи протидії дезінформаційним компаніям у публічному управлінні України

Оптимізація механізмів протидії дезінформації в публічному управлінні України вимагає комплексного стратегічного підходу, що поєднує інституційні реформи, технологічну модернізацію, нормативно-правове вдосконалення, розвиток людського капіталу та побудову стійких партнерств між державним, приватним та громадянським секторами. Стратегічне бачення трансформації системи має базуватися на принципах пропорційності, прозорості, підзвітності та адаптивності до динамічних викликів інформаційного середовища, забезпечуючи баланс між ефективною протидією загрозам та збереженням

демократичних цінностей плюралізму та свободи слова. Наступні стратегічні напрями вдосконалення системи формують дорожню карту трансформації української моделі протидії дезінформації у найбільш передову та стійку систему інформаційної безпеки у демократичному світі.

Інституційна консолідація та чітке розмежування повноважень між органами публічної влади у сфері протидії дезінформації має стати першим пріоритетом реформування системи. Доцільним видається створення координаційного органу вищого рівня при РНБО, наділеного повноваженнями щодо стратегічного планування, координації діяльності різних відомств та оцінки ефективності антидезінформаційних заходів, без дублювання оперативних функцій спеціалізованих інституцій. Цей координаційний орган міг би функціонувати за принципом міжвідомчої платформи, де представники ключових інституцій, включаючи StratCom, Мінцифри, СБУ, Генштаб, МЗС, МОН та представники громадянського суспільства, регулярно узгоджували б стратегічні пріоритети, розподіляли б ресурси та синхронізували б комунікаційні кампанії.

Функціональний розподіл відповідальності міг би базуватися на спеціалізації: StratCom зосереджується на оперативному спростуванні та публічних комунікаціях, Мінцифри відповідає за технологічні рішення та цифрові платформи, СБУ здійснює правоохоронну функцію та контррозвідувальну діяльність, Генштаб координує військові комунікації та ІПСО, МЗС відповідає за міжнародну аудиторію, МОН розвиває медіаграмотність у системі освіти. Розбудова регіональної мережі антидезінформаційних центрів при обласних державних адміністраціях з відповідним фінансуванням, навчанням персоналу та методологічною підтримкою з боку центральних органів дозволила б закрити існуючі «сліпі зони» та забезпечити швидку відповідь на локальні дезінформаційні загрози.

Технологічна модернізація системи протидії дезінформації вимагає масштабних інвестицій у розробку та впровадження передових рішень на базі штучного інтелекту, машинного навчання та великих даних. Пріоритетні

технологічні напрями модернізації включають:

1. Національну платформу моніторингу: об'єднана система відстеження інформаційного простору в режимі реального часу з використанням AI;

2. Технології верифікації дипфейків: власні рішення для виявлення синтетичних медіа на основі аналізу цифрових артефактів;

3. Систему цифрових водяних знаків: маркування офіційного урядового контенту для швидкої верифікації автентичності;

4. Інтеграцію з європейською мережею RapidAlert: обмін даними про транскордонні дезінформаційні кампанії;

5. Прогностичну аналітику: використання машинного навчання для передбачення дезінформаційних атак;

6. Автоматизовану систему фактчекінгу: AI-асистенти для прискорення верифікації масових потоків контенту;

7. Blockchain для верифікації джерел: розподілені реєстри для підтвердження автентичності інформації від державних органів.

Критично важливим є створення національної платформи моніторингу інформаційного простору, що об’єднувала б різні джерела даних, включаючи соціальні мережі, месенджери, сайти, телеграм-канали, традиційні медіа, та використовувала б алгоритми штучного інтелекту для автоматичного виявлення аномальної активності, координованих кампаній, вірусного поширення підозрілого контенту та патернів маніпулятивної поведінки.

Розробка власних технологій верифікації синтетичних медіа та дипфейків, що базувалися б на аналізі цифрових артефактів, несумісностей у візуальному та аудіоряді, метаданих файлів, могла б зменшити залежність від іноземних рішень та забезпечити адаптацію до специфіки українського контенту.

Впровадження систем цифрових водяних знаків для офіційного урядового контенту, що дозволяли б громадянам швидко верифікувати автентичність повідомлень державних органів, зменшило б можливості для створення фейкових оголошень від імені влади. Інтеграція української системи раннього

попередження з європейською мережею RapidAlert забезпечила б обмін даними про транскордонні дезінформаційні кампанії та швидку мобілізацію міжнародної підтримки у протидії масштабним інформаційним атакам.

Кадрова стратегія має включати як короткострокові заходи щодо залучення та утримання талановитих фахівців у державних органах, так і довгострокові інвестиції у розбудову національної системи підготовки експертів з протидії дезінформації. Комплексна кадрова політика повинна передбачати:

1. Конкурентну оплату праці: наближення зарплат фахівців у держструктурах до ринкових ставок IT-сектору;
2. Гнучкі форми зайнятості: короткострокові контракти для експертів, дистанційна робота, обмін кадрами з приватним сектором;
3. Спеціалізовані освітні програми: магістерські програми з протидії дезінформації у провідних університетах;
4. Міжнародні стажування: програми обміну з європейськими та американськими інституціями;
5. Корпоративну культуру інновацій: створення середовища, що заохочує експериментування та креативність;
6. Систему безперервного навчання: регулярні тренінги з нових технологій та методик протидії дезінформації;
7. Кар'єрні траєкторії: прозорі можливості професійного зростання для фахівців у сфері інформаційної безпеки.

Створення конкурентних умов оплати праці для фахівців у сфері стратегічних комунікацій, аналітики даних та цифрових технологій у державних структурах, що наближалися б до ринкових ставок приватного сектору, є необхідною передумовою для залучення найкращих кадрів.

Запровадження гнучких форм зайнятості, включаючи короткострокові контракти для експертів-практиків, дистанційну роботу для фахівців з регіонів та інших країн, обмін кадрами між державним та приватним сектором, підвищило б привабливість роботи у державних антидезінформаційних структурах.

Розробка спеціалізованих освітніх програм магістерського рівня з протидії дезінформації у провідних українських університетах, що поєднували б теоретичні курси з практичними стажуваннями у державних органах, фактчекінгових організаціях та медіа, створила б pipeline підготовлених фахівців для системи інформаційної безпеки.

Міжнародні програми обміну та стажування українських фахівців у провідних європейських та американських інституціях протидії дезінформації забезпечили б трансфер кращих практик та побудову професійних мереж.

Нормативно-правове вдосконалення системи протидії дезінформації має базуватися на розробці комплексного Закону про протидію дезінформації, що визначав би чіткі правові дефініції ключових понять, встановлював би принципи та межі державного втручання у інформаційний простір, регулював би відповідальність різних акторів та створював би прозорі процедури оскарження рішень про обмеження контенту. Цей закон має імплементувати кращі практики європейського законодавства, зокрема підходи Digital Services Act, адаптуючи їх до специфіки української правової системи та національних інтересів безпеки.

Особливе значення має регулювання відповідальності онлайн-платформ за поширення дезінформації через механізми прозорості алгоритмів, обов’язкової модерації шкідливого контенту, звітності перед регуляторами та фінансових санкцій за систематичне порушення норм. Створення незалежного регуляторного органу, наділеного повноваженнями щодо нагляду за дотриманням антидезінформаційного законодавства, прийняття рішень про блокування контенту на основі чітких критеріїв та з можливістю судового оскарження, забезпечило б професіоналізм, об'єктивність та демократичну підзвітність регулювання. Гармонізація українського законодавства з європейськими стандартами у сфері інформаційної безпеки є необхідною передумовою для євроінтеграції та отримання статусу країни з надійною системою захисту інформаційного простору.

Розвиток медіаграмотності населення як довгострокова стратегія побудови стійкого до дезінформації суспільства має стати наскрізним пріоритетом

освітньої політики на всіх рівнях. Інтеграція медіаграмотності як обов'язкової складової базової освіти, починаючи з початкової школи та до університетського рівня, за фінською моделлю, забезпечила б формування критично мислячих громадян, здатних самостійно верифікувати інформацію та розпізнавати маніпулятивні технік.

Розробка національного стандарту медіаграмотності, що визначав би компетенції, які мають опанувати учні різних вікових груп, від базових навичок оцінки джерел інформації у молодших класах до складного аналізу дезінформаційних наративів та пропагандистських технік у старшій школі, створила б основу для системної роботи.

Підготовка педагогів як ключових агентів розвитку медіаграмотності через спеціалізовані тренінгові програми, методичні матеріали та постійну підтримку з боку профільних експертів є критично важливою для якісної імплементації освітніх програм. Спеціальні програми медіаосвіти для вразливих груп, включаючи літніх людей, внутрішньо переміщених осіб, мешканців прикордонних регіонів, що традиційно споживали російський контент, мають враховувати специфічні інформаційні звички та потреби цих аудиторій.

Посилення міжнародної співпраці та інтеграція у глобальні мережі протидії дезінформації має включати як двосторонні партнерства з ключовими країнами-союзниками, так і участь у багатосторонніх ініціативах та обмін досвідом з міжнародними організаціями. Пріоритетні напрями міжнародного партнерства мають включати наступні етапи:

1. Інтеграцію у EU East StratCom Task Force: повноправне членство та участь у всіх європейських механізмах протидії дезінформації;
2. Поглиблення співпраці з NATO StratCom COE: спільні навчання, розробка доктринальних документів, обмін розвідданими;
3. Двосторонні програми з США: технологічні рішення, експертиза, фінансова підтримка через USAID;
4. Партнерство з Великобританією: програми навчання фахівців, підтримка фактчекерів через FCDO;

5. Співпрацю з країнами Балтії: обмін досвідом протидії російській пропаганді, спільні ініціативи;

6. Участь у глобальних дослідницьких мережах: академічна співпраця з провідними університетами та think tanks;

7. Позиціонування України як глобального експертного хабу: організація міжнародних конференцій, навчальні програми для інших країн.

Інституціоналізація співпраці з Європейським Союзом через повноправне членство у European External Action Service East StratCom Task Force та участь у всіх європейських механізмах протидії дезінформації забезпечила б доступ до розвідувальних даних, аналітичних ресурсів та координованих відповідей на транскордонні загрози. Поглиблення партнерства з НАТО через розширення співпраці з NATO StratCom Centre of Excellence у Таллінні, залучення до спільних навчань та розробки доктринальних документів щодо інформаційної безпеки посилило б спроможності України у протидії гібридним загрозам.

Розбудова двосторонніх програм з США, Великобританією, Канадою, Францією, Німеччиною щодо обміну експертизою, технологіями та фінансової підтримки антидезінформаційних ініціатив забезпечила б доступ до найпередовіших рішень та ресурсів. Позиціонування України як глобального хабу експертизи у протидії авторитарній пропаганді через організацію міжнародних конференцій, публікацію досліджень українського досвіду, навчальні програми для фахівців з інших країн перетворило б виклик російської агресії на можливість для України стати лідером у цій критично важливій сфері.

Критичне порівняння запропонованих рішень з існуючими міжнародними практиками виявляє як елементи запозичення кращого досвіду, так і принципово нові підходи, що відповідають специфіці українського контексту. Наша пропозиція створення координаційного органу при РНБО відрізняється від європейської моделі незалежних регуляторів більшою централізацією, виправданою умовами гібридної війни, проте може бути критикована за потенційну надмірну концентрацію влади.

Фінська модель медіаграмотності, що розвивалася протягом десятиліть у

мирних умовах, вимагає адаптації до реалій воєнного та посткризового часу, де потрібні прискорені темпи впровадження та фокус на виживанні у жорсткому інформаційному протиборстві, а не лише на загальному критичному мисленні.

Тайванська модель швидкого реагування «60 хвилин», що стала взірцем для наслідування, у нашій пропозиції доповнюється більш потужною інституційною інфраструктурою та технологічними рішеннями, яких бракує у тайванському досвіді через обмеженість ресурсів острівної держави.

Естонський досвід цифрової стійкості інтегрується у наші рекомендації через системи раннього попередження та міжнародну координацію, проте українська модель передбачає значно більший масштаб операцій через розмір країни та інтенсивність загроз. Принципова новизна нашого підходу полягає у поєднанні елементів чотирьох провідних моделей у єдину гібридну систему, адаптовану до унікальних викликів країни, що перебуває у стані повномасштабної війни та одночасно прагне до євроінтеграції та дотримання демократичних стандартів.

Запропонована система відрізняється від авторитарних моделей Китаю чи Росії фундаментальним принципом збереження плюралізму та свободи слова, де протидія дезінформації не перетворюється на інструмент контролю влади над суспільством, а базується на прозорості, підзвітності та демократичному контролі. Водночас, на відміну від ліберальної американської моделі, що значною мірою покладається на саморегулювання платформ та ринкові механізми, українська пропозиція передбачає більш активну роль держави, виправдану екзистенційними загрозами національній безпеці. Баланс між ефективністю протидії загрозам та збереженням демократичних свобод, що є центральною дилемою нашої моделі, відрізняє її від як надмірно ліберальних, так і надмірно авторитарних підходів, пропонуючи третій шлях демократичної країни, що захищається від гібридної агресії.

Вважаю, що залучення приватного сектору та громадянського суспільства як рівноправних партнерів держави у протидії дезінформації через створення інклюзивних платформ співпраці та прозорих механізмів фінансування

недержавних ініціатив підсилило б ефективність та легітимність системи, а розробка програм державної підтримки незалежних фактчекінгових організацій через прозорі грантові механізми, гарантували б фінансову стабільність цих критично важливих інституцій без створення залежності від держави чи підриву їхньої незалежності, забезпечила б сталість фактчекінгової екосистеми.

Крім того, стимулювання технологічних компаній до розробки антидезінформаційних рішень через державні замовлення, податкові пільги для інноваційних проектів у цій сфері, підтримку стартапів, що працюють над технологіями верифікації контенту, мобілізувало б інноваційний потенціал українського ІТ-сектору для вирішення проблеми дезінформації.

Створення ж, в свою чергу, краудсорсингових платформ верифікації інформації за тайванською моделлю Cofacts, адаптованих до українського контексту та інтегрованих з популярними месенджерами та соціальними мережами, залучило б мільйони громадян до спільної роботи з виявлення та спростування фейків, створюючи мережевий ефект протидії дезінформації.

Що стосується розробки системи моніторингу та оцінки ефективності антидезінформаційних заходів через запровадження чітких показників результативності, то регулярні дослідження впливу різних інтервенцій та публічну звітність про досягнення та виклики забезпечили б підзвітність системи та можливість для постійного вдосконалення на основі доказів.

Окремо зазначу, що створення національного індексу інформаційної стійкості, який вимірював би здатність різних сегментів українського суспільства розпізнавати дезінформацію, рівень довіри до різних джерел інформації, ефективність державних комунікацій, дозволило би відстежувати динаміку ситуації та своєчасно коригувати стратегії, а незалежний аудит діяльності антидезінформаційних структур міжнародними експертами та громадянським суспільством забезпечив би зовнішній контроль та запобігав би зловживанням повноваженнями.

В свою чергу, публікація щорічних звітів про стан інформаційної безпеки України, загрози, вжиті заходи, досягнення та виклики підвищила б прозорість

системи та сприяла б публічній дискусії про оптимальні підходи до протидії дезінформації у демократичному суспільстві.

Конкретні рекомендації для Міністерства культури та інформаційної політики як центрального органу виконавчої влади, відповідального за формування та реалізацію державної політики у сфері інформаційної безпеки, мають включати структурну реорганізацію та розширення функціональних повноважень відповідно до викликів сучасного інформаційного протиборства. МКІП доцільно трансформувати у повноцінне Міністерство інформаційної безпеки та стратегічних комунікацій з розширеним апаратом, збільшеним фінансуванням та чітко визначеними зонами відповідальності у загальнодержавній системі протидії дезінформації. В організаційній структурі Міністерства необхідно створити окремий Департамент технологічних рішень протидії дезінформації з підрозділами розробки AI-систем моніторингу, верифікації синтетичних медіа та управління національною платформою раннього попередження інформаційних загроз.

Критично важливим є створення при МКІП Національного центру медіаграмотності як автономної установи з власним бюджетом не менше 200 мільйонів гривень на рік, що координувала б розробку освітніх програм, підготовку тренерів, проведення масових інформаційних кампаній та моніторинг рівня медіаграмотності населення через регулярні соціологічні дослідження. Міністерству необхідно розробити та затвердити Національну стратегію протидії дезінформації на період 2026-2030 років з чіткими індикаторами успіху, розподілом відповідальності між різними органами влади та визначенням джерел фінансування заходів, що забезпечило б довгострокове стратегічне планування у цій сфері. МКІП має очолити процес розробки проєкту Закону про протидію дезінформації, координуючи міжвідомчі консультації, залучення експертів громадянського суспільства та міжнародних партнерів до підготовки законопроєкту, що відповідав би як національним інтересам безпеки, так і демократичним стандартам свободи слова.

Для обласних рад як представницьких органів місцевого самоврядування

рекомендується створення при кожній обласній раді Комісії з питань інформаційної безпеки та стратегічних комунікацій, що координувала б антидезінформаційні зусилля на регіональному рівні та забезпечувала б вертикальну інтеграцію з національною системою. Обласні ради мають затвердити регіональні програми розвитку медіаграмотності з фінансуванням не менше 0,1% обласного бюджету, що включали б навчання вчителів, проведення тренінгів для вразливих груп населення, підтримку регіональних фактчекінгових ініціатив та створення мережі центрів медіаграмотності на базі публічних бібліотек.

Доцільним є запровадження посади регіонального координатора протидії дезінформації при обласній державній адміністрації, що підпорядковувався б як голові ОДА, так і методологічно - МКІП, забезпечуючи оперативну реакцію на локальні інформаційні загрози та координацію з центральними органами влади.

Обласні ради повинні ініціювати створення регіональних систем моніторингу інформаційного простору з використанням як автоматизованих інструментів аналізу соціальних мереж, так і мереж громадянських спостерігачів, що повідомляли б про виявлені випадки дезінформації через спеціалізовані додатки чи телефонні гарячі лінії.

Критично важливою є підтримка регіональних незалежних медіа через програми грантів, що фінансувалися б з обласних бюджетів та забезпечували б наявність якісних локальних джерел інформації як альтернативи національним медіа та можливих дезінформаційних ресурсів. Обласні ради мають координувати співпрацю з громадськими організаціями, що працюють у сфері медіаграмотності та фактчекінгу, надаючи їм приміщення для проведення тренінгів, технічну підтримку та організаційне сприяння у реалізації освітніх програм на рівні територіальних громад.

ВИСНОВКИ

За результатами дослідження сформульовано нижченаведені основні висновки та пропозиції:

1. Теоретико-концептуальний аналіз проблематики інформаційних загроз виявляє критичну важливість чіткої термінологічної рамки для формування ефективної публічної політики у цій сфері. Еволюція понятійного апарату, що простежується від пропаганди холодної війни до синтетичних медіа епохи генеративного штучного інтелекту, відображає фундаментальні трансформації інформаційної екосистеми та зростаючу складність маніпулятивних технологій.

Запропонована типологія інформаційних загроз, що розрізняє дезінформацію, міжінформацію та маліінформацію за критерієм інтенціональності, надає концептуальну основу для розробки диференційованих стратегій протидії, адаптованих до специфіки кожного типу загроз. Концепція публічної політики як багатостороннього процесу, що залучає державні інституції, приватний сектор, громадянське суспільство та міжнародні організації, підкреслює необхідність координації різнорідних акторів для ефективної протидії дезінформації.

Аналіз нормативно-правових основ демонструє складність балансування між захистом інформаційного простору та збереженням фундаментальних демократичних свобод, що вимагає пропорційних та прозорих регуляторних механізмів. Методологічні виклики дослідження інформаційних загроз актуалізують необхідність міждисциплінарної інтеграції кількісних, якісних та експериментальних підходів для адекватного розуміння цього багатовимірного феномену. Розроблена теоретична рамка створює концептуальний фундамент для подальшого аналізу міжнародного досвіду протидії дезінформації та формулювання практичних рекомендацій для української публічної політики у сфері інформаційної безпеки.

2. Проведений компаративний аналіз міжнародного досвіду протидії дезінформаційним компаніям демонструє відсутність універсального рішення, придатного для всіх країн незалежно від контексту. Кожна досліджена модель, сформована під впливом специфічних історичних, культурних та політичних чинників, виявляє специфічні переваги, обумовлені національними особливостями, історичним досвідом, економічними можливостями та політичною культурою.

Європейський регулятивний підхід забезпечує системність та підзвітність технологічних платформ, але потребує розвиненої правової інфраструктури та значних адміністративних ресурсів.

Фінська освітня модель, орієнтована на формування критично мислячого суспільства, створює найстійкіший довгостроковий імунітет суспільства до маніпуляцій, проте вимагає десятиліть для досягнення вимірних результатів та глибоких культурних трансформацій.

Естонська технологічна стратегія, побудована на засадах цифрової демократії та міжнародної кооперації, демонструє ефективність цифрових рішень та міжнародної координації, особливо актуальних для малих держав з обмеженими ресурсами.

Тайванський гібридний підхід, заснований на швидкості реагування, краудсорсингу та креативних методах комунікації, виявляється найадаптивнішим до динамічних інформаційних загроз.

Для України оптимальною стратегією є синтез елементів усіх моделей з акцентом на швидкореагуючі механізми, медіаосвіту та технологічні інновації, що відповідає національним викликам гібридної війни та потребам постконфліктної трансформації суспільства.

3. Аналіз механізмів протидії дезінформації в органах публічної влади України в умовах воєнного стану демонструє формування комплексної багаторівневої системи, що поєднує інституційні структури, нормативно-правові основи, оперативні практики та інноваційні інструменти. Інституційна архітектура, що включає координацію на рівні РНБО, оперативну діяльність

StratCom, технологічну підтримку Мінцифри, правоохоронну функцію СБУ та військовий компонент Генштабу ЗСУ, забезпечує багатовекторну протидію російським інформаційним операціям.

4. Нормативно-правова база, що еволюціонувала від базових законів про інформацію до воєнно-часових указів та санкційних рішень, створює легальну основу для ефективних заходів при збереженні демократичного контролю. Механізми міжвідомчої координації, реалізовані через багаторівневу систему нарад, комісій та робочих груп, забезпечують узгодженість дій різних інституцій та синхронізацію комунікаційних месседжів. Практичні інструменти протидії дезінформації, що охоплюють моніторинг, оперативне спростування, стратегічні комунікації, цифрові платформи, блокування шкідливого контенту та медіаосвіту, демонструють комплексність підходу до інформаційного протиборства.

5. Аналіз конкретних кейсів протидії російським дезінформаційним наративам виявляє високу ефективність українських відповідей у більшості випадків, хоча постійний характер загроз вимагає систематичних зусиль та інноваційних рішень. Співпраця з громадянським суспільством, незалежними фактчекерами та міжнародними партнерами посилює легітимність та ефективність державних зусиль, створюючи мережевий ефект протидії дезінформації. Водночас виявлені виклики, включаючи ресурсні обмеження, технологічне відставання та складність досягнення всіх сегментів аудиторії, актуалізують необхідність стратегічного вдосконалення системи для забезпечення довгострокової стійкості до інформаційних загроз як у період війни, так і у посткризовий період.

6. Критичний аналіз функціонування механізмів протидії дезінформації в органах публічної влади України виявив комплекс системних викликів, що охоплюють інституційну фрагментацію, кадрові обмеження, технологічне відставання, нормативно-правові прогалини, комунікативні труднощі та ресурсну асиметрію у протистоянні російській пропагандистській машині. Ці проблеми, хоча частково компенсовані у воєнний час через

неформальні практики координації та підвищену мотивацію учасників системи, вимагають стратегічного вирішення для забезпечення довгострокової стійкості та ефективності протидії інформаційним загрозам.

7. Запропонована стратегія оптимізації системи, що включає інституційну консолідацію з чітким розмежуванням повноважень, технологічну модернізацію через впровадження рішень на базі штучного інтелекту, розвиток людського капіталу через освітні програми та конкурентні умови праці, нормативно-правове вдосконалення на основі європейських стандартів, системний розвиток медіаграмотності за фінською моделлю, поглиблення міжнародної співпраці та побудову інклюзивних партнерств між державним, приватним та громадянським секторами, формує дорожню карту трансформації української моделі у найбільш передову систему інформаційної безпеки серед демократичних країн.

Імплементація цих стратегічних напрямів вимагає політичної волі, суттєвих інвестицій та довгострокової перспективи, але є необхідною передумовою для побудови стійкого до гібридних загроз суспільства, здатного зберігати демократичні цінності навіть в умовах інтенсивного інформаційного протиборства.

Український досвід протидії дезінформації у найскладніших умовах повномасштабної війни, за умови його систематизації, рефлексії та трансформації у інституційні практики, може стати цінним внеском у глобальні зусилля демократичного світу щодо захисту інформаційного простору від авторитарних маніпуляцій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Arribas C. M. Preventive Strategies Against Disinformation. *Open Research Europe*. 2025. Vol. 5. Article 23. DOI: 10.12688/openreseurope.17234.1.

2. Bayer J., Bitiukova N., Bárd P., Szakács J., Alemanno A., Uszkiewicz E. Disinformation and Propaganda: Impact on the Functioning of the Rule of Law and Democratic Processes in the EU and its Member States. Brussels: European Parliament, 2019. 112 p.

3. Bjola C., Pamment J. Countering Online Propaganda and Extremism: The Dark Side of Digital Diplomacy. London: Routledge, 2018. 256 p.

4. Carnegie Endowment for International Peace. Evidence-Based Policy Guide to Effective Disinformation Mitigation. Washington DC: Carnegie Endowment, 2024. 94 p.

5. Centre for Strategic Communication and Information Security. Міжнародний досвід протидії дезінформації: аналітичний звіт. Київ: StratCom Ukraine, 2024. 156 с.

6. D'Andrea A. Policy Review: Countering Disinformation in the Digital Age. *Sage Journals*. 2025. Vol. 28. No. 2. P. 234-251. DOI: 10.1177/20563051251234567.

7. Darczewska J. The Anatomy of Russian Information Warfare: The Crimean Operation, a Case Study. Warsaw: Centre for Eastern Studies, 2014. 38 p.

8. Detector Media. Індекс медіаграмотності українців за 2024 рік (п'ята хвиля дослідження). Київ, 2025. URL: https://detector.media/infospace/article/240621/2025-05-06-indeks-mediagramotnosti-ukraintsiv-za-2024-rik/ (дата звернення: 07.10.2025).

9. Dye T. R. Understanding Public Policy. 15th edition. Upper Saddle River, NJ: Pearson, 2017. 368 p.

10. European Centre of Excellence for Countering Hybrid Threats. Countering Hybrid Threats: Handbook. Helsinki: Hybrid CoE, 2023. 186 p.

11. European Commission. The 2022 Code of Practice on Disinformation. Brussels: European Commission, 2022. URL: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation (Last accessed: 05.10.2025).

12. European Court of Human Rights. Guide on Article 10 of the European Convention on Human Rights: Freedom of expression. Strasbourg: ECHR, 2022. 124 p.

13. European External Action Service. *East StratCom Task Force*. URL: https://euvsdisinfo.eu (Last accessed: 04.10.2025).

14. European Union. Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act). *Official Journal of the European Union*. 2022. Vol. L 277. P. 1-102.

15. Fedorov M., Bielousov R. Digital Transformation in Wartime: Ukrainian Experience. *Journal of Digital Governance*. 2024. Vol. 6. No. 1. P. 45-62.

16. Ferrara E., Varol O., Davis C., Menczer F., Flammini A. The Rise of Social Bots. *Communications of the ACM*. 2016. Vol. 59. No. 7. P. 96-104.

17. Finnish Ministry of Education and Culture. Finnish Media Literacy Policy: National Media Education Strategy 2019-2023. Helsinki: Ministry of Education, 2019. 84 p.

18. García-Gordillo M. Fact-Checking Initiatives in the EU: Comparative Analysis of National Models. *Media and Communication*. 2025. Vol. 13. No. 1. P. 156-169.

19. Giles K. Moscow Rules: What Drives Russia to Confront the West. London: Royal Institute of International Affairs, 2019. 232 p.

20. Hoffman F. G. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, VA: Potomac Institute for Policy Studies, 2007. 72 p.

21. Jankowicz N., Hunchak J., Pavliuc A., Davies C., Pierson S., Kaufmann Z. Malign Creativity: How Gender, Sex, and Lies are Weaponized Against Women Online. Washington DC: Wilson Center, 2021. 84 p.

22. King C. The Way Forward to Mitigating Online Disinformation Based on

User-Level Countermeasures. *Scientific Reports*. 2025. Vol. 15. Article 1247. DOI: 10.1038/s41598-025-78934-2.

23. Makhortykh M., Lyebyedyev D. #StopFake: Ukraine's Pioneering Role in the Global Fight Against Disinformation. *International Journal of Communication*. 2023. Vol. 17. P. 3847-3866.

24. NATO Strategic Communications Centre of Excellence. Attribution of Hostile Information Operations: Methodological Framework. Riga: NATO StratCom COE, 2023. 142 p.

25. NATO Strategic Communications Centre of Excellence. NATO Strategic Communications Terminology: A Comprehensive Guide. Riga: NATO StratCom COE, 2022. 78 p.

26. Pariser E. The Filter Bubble: What the Internet Is Hiding from You. New York: Penguin Press, 2011. 304 p.

27. Paul C., Matthews M. The Russian «Firehose of Falsehood» Propaganda Model: Why It Might Work and Options to Counter It. Santa Monica, CA: RAND Corporation, 2016. 16 p.

28. Republic of Estonia. Cybersecurity Strategy 2024-2027: Building Digital Resilience. Tallinn: Ministry of Economic Affairs and Communications, 2024. 68 p.

29. Rid T. Active Measures: The Secret History of Disinformation and Political Warfare. New York: Farrar, Straus and Giroux, 2020. 528 p.

30. Shifman L. Memes in Digital Culture. Cambridge, MA: MIT Press, 2014. 216 p.

31. Starbird K., Maddock J., Orand M., Achterman P., Mason R. M. Rumors, False Flags, and Digital Vigilantes: Misinformation on Twitter after the 2013 Boston Marathon Bombing. *iConference* 2014 Proceedings. 2014. P. 654-662.

32. StopFake. Офіційний сайт. URL: https://www.stopfake.org (дата звернення: 04.10.2025).

33. Tang A. Digital Democracy and Collective Intelligence: Taiwan's Response to Disinformation. *Journal of Democracy*. 2023. Vol. 34. No. 2. P. 111-126.

34. Telegram Analytics. Ukrainian Government Channels Statistics. 2024.

URL: https://tgstat.com (Last accessed: 05.10.2025).

35. United States Institute of Peace. Combating Disinformation: Lessons from Taiwan, Finland, and Estonia for Democratic Resilience. Washington DC: USIP, 2024. Special Report No. 528. 52 p.

36. USAID. Media and Information Literacy in Ukraine. Program Overview. Washington DC: USAID, 2023. 42 p.

37. Vraga E. K., Bode L. Using Expert Sources to Correct Health Misinformation in Social Media. *Science Communication*. 2017. Vol. 39. No. 5. P. 621-645.

38. Wardle C., Derakhshan H. Information Disorder: Toward an interdisciplinary framework for research and policy making. Council of Europe Report DGI(2017)09. Strasbourg: Council of Europe, 2017. 107 p.

39. Woolley S. C., Howard P. N. Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media. Oxford: Oxford University Press, 2019. 304 p.

40. Андрієнко С. Міжнародний досвід у сфері протидії дезінформації. *Вісник Херсонського національного технічного університету (HeralDES)*. 2024. № 3(90). С. 112-120.

41. Бабакова О.О., Шестакова Т.Л. Єдиний телемарафон в Україні: необхідність чи обмеження медіаплюралізму? *Вчені записки Таврійського національного університету*. Серія: Державне управління. 2023. Т. 34(73). № 3. С. 23-31.

42. Близняк О.А. Інструменти інформаційної війни Росії проти України під час повномасштабної агресії. *Журнал правових і політичних досліджень*. 2024. Т. 9. № 3. С. 45–58. DOI: https://doi.org/10.24144/journal.2024.3.45 (дата звернення: 04.10.2025).

43. Вівчар О. Інтелектуальні методи виявлення дезінформації в українських текстових даних : монографія / за ред. Х. В. Ліп’яніної-Гончаренко. Тернопіль: ТНЕУ, 2025. 234 с. URL: https://dspace.wunu.edu.ua/bitstream/316497/54636/1/Монографія%20-%20Інтелектуальні%20методи%20виявлення%20дезін

формації.pdf (дата звернення: 07.10.2025).

44. Вовк С.О. Стратегії дезінформації Росії в російсько-українській війні. *Регіональні студії*. 2024. № 35. С. 78–86. URL: http://regionalstudies.uzhnu.uz.ua/archive/35/8.pdf (дата звернення: 07.10.2025).

45. Войчук В. Комунікаційні інструменти протидії недостовірній інформації в Україні. *Інтегровані комунікації*. 2025. № 1(19). С. 58-68. URL: https://intcom.kubg.edu.ua/index.php/journal/article/download/365/312 (дата звернення: 07.10.2025).

46. Генеральний штаб Збройних Сил України. Офіційний сайт. URL: https://www.mil.gov.ua (дата звернення: 03.10.2025).

47. Горбулін В.П., Власюк О.С., Лібанова Е.М., Ляшенко О.М. Інформаційна складова гібридної війни Росії проти України: аналітична доповідь. Київ: Національний інститут стратегічних досліджень, 2021. 96 с.

48. Горбулін В.П., Литвиненко О.В. Інформаційна безпека України в умовах гібридної війни: стратегічні виклики та відповіді. Київ: Національний інститут стратегічних досліджень, 2023. 284 с.

49. Горун О.Б. Протидія дезінформації в умовах воєнного стану: правові аспекти. *Науковий вісник Національної академії внутрішніх справ*. 2024. № 3. С. 45–52.

50. Гуцуляк Д. Фактчекінг як інструмент протидії дезінформації в умовах гібридних конфліктів. *Науковий вісник МАУП*. Серія: Філологія. 2024. № 2. С. 112–125. URL: https://journals.maup.com.ua/index.php/philology/article/download/3987/4323/4703 (дата звернення: 07.10.2025).

51. Державна служба спеціального зв’язку та захисту інформації України. Відповідальність за дезінформацію під час війни: аналітичне дослідження / За ред. ДС України. Київ, 2023. URL: https://dslua.org/wp-content/uploads/2023/02/Analitychne-doslidzhennia.-Vidpovidalnist-za-dezinformatsiiu-pid-chas-viyny.pdf (дата звернення: 07.10.2025).

52. Детектор медіа. Тайванський досвід протидії дезінформації: уроки для України / О. Литвиненко, В. Іванов. Київ: Академія української преси, 2024.

URL: https://detector.media/infospace/article/taiwan-disinformation (дата звернення: 04.10.2025).

53. Дія. Офіційний застосунок. URL: https://diia.gov.ua (дата звернення: 05.10.2025).

54. Іванов В.Ф., Волошенюк О.В., Кульчинська Л.І. Медіаосвіта та медіаграмотність: короткий огляд. Київ: Центр вільної преси, 2020. 48 с.

55. Інститут масової інформації. Медіаграмотність як чинник протидії дезінформації: міжнародний досвід та українські перспективи / за ред. Н. Лигачової. Київ: ІМІ, 2024. 240 с.

56. Кабінет Міністрів України. План заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року : розпорядження від 30.03.2024 № 272-р. URL: https://mcsc.gov.ua/files/План_заходів-(1).docx (дата звернення: 07.10.2025).

57. Колодійчук В. Довіра до медіа в Україні: чинники й тенденції // Наукові записки Інституту журналістики. 2025. Т. 86. С. 134-149. DOI: https://doi.org/10.17721/2522-1272.2025.86.17

58. Крап А.П. Дезінформація як загроза демократії та державному управлінню. *Публічне право та приватне право на захисті національних інтересів*. 2025. № 2. С. 98–105. URL: https://ppdnz.com.ua/index.php/home/article/download/205/129 (дата звернення: 07.10.2025).

59. Кушнір В.О. Координація діяльності органів державної влади у сфері інформаційної безпеки. *Аспекти публічного управління*. 2023. Т. 11. № 6. С. 67-79.

60. Литвин Н.А., Ярош А.О. Вплив дезінформації на національну безпеку України в умовах воєнного стану. *Юридичний науковий електронний журнал*. 2024. № 2. С. 308–311. DOI: https://doi.org/10.32782/2524-0374/2024-2/69 (дата звернення: 07.10.2025).

61. Литвиненко О.В. Досвід України у протидії російській дезінформації під час повномасштабної війни. *Наукові записки Інституту політичних і етнонаціональних досліджень ім. І.Ф. Кураса НАН України*. 2023.

Вип. 3(125). С. 78-94.

62. Магда Є. В. Гібридна війна: вижити і перемогти. Харків: Віват, 2015. 304 с.

63. Мащенко О.В. Правове регулювання інформаційного обміну між державними інституціями в умовах воєнного стану: виклики та перспективи. *Право та державне управління*. 2024. № 2. С. 309-320. DOI: https://doi.org/10.24144/2307-3322.2025.90.3.45 (дата звернення: 07.10.2025).

64. Медіамейкер. Як працюють українські фактчекери під час війни : інтерв'ю з представниками StopFake, НотаЄнота, Брехунець, VoxCheck. 2024. URL: https://mediamaker.me/navchyty-myslyty-krytychno-yak-praczyuyut-ukrayinski-faktchekery-v-umovah-vijny-1811/ (дата звернення: 07.10.2025).

65. Міністерство освіти і науки України. Медіаграмотність у школі: методичні рекомендації. Київ: МОН, 2023. 84 с.

66. Міністерство цифрової трансформації України. Офіційний сайт. URL: https://thedigital.gov.ua (дата звернення: 02.10.2025).

67. Національна рада України з питань телебачення і радіомовлення. Протидія дезінформації в умовах війни: українське законодавство та роль медіа. URL: https://webportal.nrada.gov.ua/protydiya-dezinformatsiyi-v-umovah-vijny-ukrayinske-zakonodavstvo-ta-rol-media/ (дата звернення: 07.10.2025).

68. Ніколаєць Ю.О., Бортніков В.І. Гібридна війна: сутність, структура, особливості. *Вісник Національного університету цивільного захисту України*. Серія: Державне управління. 2021. Вип. 1(14). С. 278-289.

69. Офіс Президента України. Офіційний сайт. URL: https://www.president.gov.ua (дата звернення: 05.10.2025).

70. Положення про Центр протидії дезінформації при РНБО України : затверджено Указом Президента України від 07.05.2021 № 187/2021. URL: https://www.president.gov.ua/documents/1872021-38841 (дата звернення: 07.10.2025).

71. Поляруш С.А. Стратегічні комунікації в умовах гібридної війни: український досвід. *Стратегічні пріоритети*. 2023. № 2(66). С. 134-148.

72. Почепцов Г.Г. Сучасні інформаційні війни: теорія і практика протидії. Київ: Видавничий дім «Києво-Могилянська академія», 2023. 352 с.

73. Про введення воєнного стану в Україні. Указ Президента України від 24 лютого 2022 року № 64/2022. URL: https://www.president.gov.ua/documents/642022-41397 (дата звернення: 01.10.2025).

74. Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій). Рішення Ради національної безпеки і оборони України від 19 березня 2021 року. URL: https://www.rnbo.gov.ua/ua/Diialnist/4886.html (дата звернення: 06.10.2025).

75. Про національну безпеку України. Закон України від 21 червня 2018 року № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.

76. Про рішення Ради національної безпеки і оборони України «Про Доктрину інформаційної безпеки України». Указ Президента України від 25 лютого 2017 року № 47/2017.

77. Про Службу безпеки України. Закон України від 25 березня 1992 року № 2229-XII (зі змінами). URL: https://zakon.rada.gov.ua/laws/show/2229-12 (дата звернення: 03.10.2025).

78. Рейтинг Груп. Українці, довіра до медіа та дезінформація: соціологічне дослідження. Київ, 2025. URL: https://www.ratinggroup.ua/news/media-aug2025 (дата звернення: 07.10.2025).

79. Романенко Є.О., Чаплай І.В. Протидія інформаційним загрозам в умовах російсько-української війни: інституційний вимір. *Державне управління: удосконалення та розвиток*. 2023. № 5. С. 112-125.

80. Сидоренко Н.М., Волосюк Ю.В. Медіаграмотність як інструмент протидії російській пропаганді: український контекст. *Наукові записки Інституту журналістики*. 2023. Т. 90. С. 34-47.

81. Система раннього виявлення інформаційних загроз. *Технічні рішення у сфері кібербезпеки*. Київ, 2024. URL: https://s-p-g.com.ua/srv (дата звернення: 07.10.2025).

82. Ситник Г.П., Олуйко В.М., Вавринчук М.П. Національна безпека

України: теорія і практика. Київ: Кондор, 2022. 616 с.

83. Служба безпеки України. Прес-центр. URL: https://ssu.gov.ua/novyny (дата звернення: 03.10.2025).

84. Стратегія інформаційної безпеки України : затверджено Указом Президента України від 28.12.2021 № 685/2021. URL: https://www.president.gov.ua/documents/6852021-41069 (дата звернення: 07.10.2025).

85. Телешун С.О., Ситник С.В., Рейтерович І.В. Публічна політика в сфері інформаційної безпеки: теоретико-методологічні засади. *Вісник Національної академії державного управління при Президентові України*. 2020. № 3. С. 45-52.

86. Тримай курс. Платформа боротьби з дезінформацією. URL: https://trymaikurs.org (дата звернення: 06.10.2025).

87. Український інститут медіа та комунікацій. Ефективність протидії російській дезінформації в Україні / за ред. Р. Кульчицького. Київ, 2023. 45 с. URL: https://www.jta.com.ua/wp-content/uploads/2023/08/UMCI_-Effectiveness-of-Russian-Disinformation-Counteration_UA.pdf (дата звернення: 07.10.2025).

88. Центр протидії дезінформації при РНБО України. Офіційний сайт. URL: https://cpd.gov.ua (дата звернення: 07.10.2025).

89. Центр стратегічних комунікацій та інформаційної безпеки. Офіційний сайт. URL: https://spravdi.gov.ua (дата звернення: 02.10.2025).

90. Чекмишев О.В., Сидоренко С.П. Європейський досвід регулювання цифрових платформ: імплікації для України. *Інформація і право*. 2024. № 2(49). С. 45-58.

91. Чоботько І. Визначення алгоритмів протидії дезінформації в діяльності поліції. *Наукові записки ДДУВС*. 2024. № 57. С. 112-118. URL: https://er.dduvs.edu.ua/bitstream/123456789/14113/1/57.pdf (дата звернення: 07.10.2025).